



No One  
Behind

# Training manual for a digital competent citizen



Co-funded by the  
Erasmus+ Programme  
of the European Union

*This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project n. 2020-1-RO01-KA204-079988)*

# Training manual for a “digital competent” citizen

Erasmus Plus Programme – KA2 Strategic Partnership for Adult Education

COPYRIGHT

© Copyright 2020 NO ONE BEHIND Consortium

Consisting of:

P1 – Agentia Nationala pentru Programe Comunitare in Domeiul Educariei si Formarii Profesionale - NERDA - RO  
P2 - EUROCREA MERCHANT SRL – EUROCREA - IT  
P3 - INOVA+ - INNOVATION SERVICES, SA – INOVA+ - PT  
P4 - Asociatia de Dezvoltare Locala ECO LAND - ADL “ECO LAND” - RO  
P5 - AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSY ANONYMI ETAIREIA IDEC – GR  
P6 - European E-learning Institute - EUEI – DK  
P7 - ATERMON B.V. – ATERMON - NL

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the NO ONE BEHIND Consortium. In addition, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

All rights reserved.

**AUTHORS | No One behind | August 2021**

## Partnership



**North-East Regional Development Agency - NERDA, Romania**  
**Lucian Alexa and Olivian Secara**  
Website: <https://www.adnordest.ro/en/homepage/>



**Eurocrea Merchant, SRL, Italy**  
**Beatrice Del Nero**  
Website: <http://www.eurocreamerchant.it/>



**INOVA+ - Innovation Services S.A., Portugal**  
**Andreia Monteiro and Sara Correia**  
Website: <https://inova.business/>



**ECO LAND, Romania**  
**Ciprian Barsan**  
Facebook: <https://www.facebook.com/AdlEcoLand/>



**IDEC, Greece**  
**Rafaella Paspatis and Lila Anthopoulou**  
Website: <https://idec.gr/>



**European E-learning Institute – EUEI, Denmark**  
**Canice Hamill & Catherine Neill**  
Website: <https://www.euei.dk/>



**ATERMON, Netherlands**  
**Anna Stamouli**  
Website: <https://www.atermon.nl/>



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

## Digital Competent Citizen Training Manual

No One Behind | Erasmus+ Strategic Partnership - 2020-1-RO01-KA204-079988

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	9
INTRODUCTION .....	11
1. Introduction to the <i>No One Behind</i> training manual.....	9
2. Profile of the "digital competent" citizen.....	11
DIGITAL COMPETENT CITIZEN CURRICULUM .....	13
1. Module 1: Information and data literacy .....	17
1.1. Browsing, searching and filtering data .....	18
1.1.1. Main concepts: IT, ICT and Internet .....	19
1.1.2. Introduction to searching online .....	20
1.1.3. Protection when using ICT .....	22
1.1.4. Practical activities .....	23
1.2. Evaluating data, information and digital content .....	28
1.2.1. How to assess sources and information online?.....	28
1.2.2. Evaluating your Sources.....	30
1.2.3. Evaluating websites .....	30
1.2.4. Fact-checking websites .....	32
1.2.5. Practical Activities.....	32
1.3. Managing data, information and digital content.....	35
1.3.1. Devices to save and retrieve information .....	35
1.3.2. Copyrighting and data protection .....	37
1.3.3. Practical activities .....	39
2. Module 2: Communication and collaboration and collaboration .....	42
2.1. Interacting through digital technologies .....	43
2.2. Sharing through digital technologies .....	49
2.3. Engaging in citizenship through digital technologies.....	53
2.4. Collaborating through digital technologies.....	60
2.5. Netiquette.....	64
2.6. Managing digital identity.....	71
3. Module 3: Content creation .....	75
3.1. Developing digital content .....	76
3.2. Integrating and re-elaborating digital content .....	79



3.3.	Copyright and licences .....	81
3.4.	Programming .....	83
4.	Module 4: Safety .....	87
4.1.	Protecting devices.....	88
4.1.1.	Protecting devices.....	88
4.1.2.	Software updates.....	91
4.1.3.	Security and passwords .....	93
4.1.4.	Increasing security .....	96
4.1.5.	What is malicious code? .....	103
4.1.6.	Practical activities .....	106
4.2.	Protecting personal data and privacy .....	109
4.2.1.	Protecting yourself online .....	109
4.2.2.	Guidelines for sharing personal information .....	111
4.2.3.	Practical Activities.....	114
4.3.	Protecting health and well-being .....	117
4.3.1.	Negative effects of technology: what to know .....	117
4.3.2.	Have you heard of cyberbullying? .....	121
4.3.3.	Practical activities .....	123
4.4.	Protecting the environment .....	125
4.4.1.	Proper Disposal of Electronic Devices .....	125
4.4.2.	Practical activities .....	128
5.	Module 5: Problem solving .....	131
5.1.	Solving technical problems.....	132
5.1.1.	Computers and its systems.....	132
5.1.2.	Most common technical problems.....	Error! Bookmark not defined.
5.1.3.	Practical Activities.....	137
5.2.	Identifying needs and technological responses .....	139
5.2.1.	Identifying needs and technological responses .....	139
5.2.2	Practical Activities .....	142
5.3.	Creatively using digital technologies.....	149
5.4.	Identifying digital competence gaps .....	154
	EVALUATION OF THE TRAINING .....	158

1. Evaluation of the learning .....	159
2. Evaluation of the training.....	162
ANNEXES.....	163
Annex I – Additional resources .....	164
Annex II – Evaluation sheet Module 1. Information and Data Literacy .....	168
Annex III – Evaluation sheet Module 2 .....	170
Annex IV – Evaluation sheet Module 3 .....	172
Annex IV – Evaluation sheet Module 4 .....	173
Annex V – Evaluation sheet Module 5 .....	174
Annex VI – Evaluation of the training .....	175
REFERENCES .....	177

## TABLE OF FIGURES

Figure 1 – Overview and global structure of the Digital Competent Citizen profile, as defined by the consortium and in accordance with the ECVET. ....	11
Figure 2 – Identification of the units of competences correspondent to the modules of the profile for a digital competent citizen. ....	12
Figure 3 – Icons of some browsers. ....	20
Figure 4 – Google homepage. ....	21
Figure 5 – Chrome homepage. ....	21
Figure 6 – Identification of the lock icon. ....	22
Figure 8 – identification and short description of memory and storage devices. ....	36
Figure 9 – Guidelines related to personal data protection as established on the Directive 95/46/EC. ....	38
Figure 10 – Identification of possible situations to be considered in this activity. ....	39
Figure 11 – Division of learners into two groups. ....	40
Figure 12 – Profiles to be considered to prepare passwords. ....	74
Figure 13 – Data for the calculation of the power consumption. ....	128

## TABLE OF TABLES

Table 1 – Curriculum of the Digital Competent Citizen training course. ....	14
Table 2 – Brief description and identification of the units of competences of each module of the training course. ....	15
Table 3 – Identification and brief description of the methods considered in this manual. ....	16
Table 4 – Global structure of the Module 1 – Information and data literacy. ....	17
Table 5 – Structure of the unit of competence 1.1. - Browsing, searching and filtering data of the Module 1 – Information and data literacy. ....	18

### *Digital Competent Citizen Training Manual*

Table 6 - Structure of the unit of competence 1.2. Evaluating data, information and digital content of the Module 1 – Information and data literacy.....	28
Table 7 – List of affirmations and correct answer. ....	32
Table 8 - Structure of the unit of competence 1.3. Managing data, information and digital content of the Module 1 – Information and data literacy.....	35
Table 9 - Global structure of the Module 2 – Communication and collaboration. ....	42
Table 10 - Structure of the unit of competence 2.1. – Interacting through digital technologies of the Module 2 – Communication and collaboration. ....	43
Table 11 - Structure of the unit of competence 2.2. – Sharing through digital technologies of the Module 2 – Communication and collaboration. ....	49
Table 12 - Structure of the unit of competence 2.2. – Engaging in citizenship through digital technologies of the Module 2 – Communication and collaboration. ....	53
Table 13 - Structure of the unit of competence 2.5. – Collaborating through digital technologies of the Module 2 – Communication and collaboration. ....	60
Table 14 - Structure of the unit of competence 2.6. – Netiquete of the Module 2 – Communication and collaboration.....	64
Table 15 - Structure of the unit of competence 2.7. – Managing digital identity of the Module 2 – Communication and collaboration....	71
Table 16 - Global structure of the Module 3 – Content Creation. ....	76
Table 17 - Structure of the unit of competence 3.1.- Developing digital content of the Module 3 – Content Creation. ....	76
Table 18 Structure of the unit of competence 3.2. – Integrating and re-elaborating digital content of the Module 3 – Content Creation.....	79
Table 19 - Structure of the unit of competence 3.3.- Copyright and licences of the Module 3 – Content Creation. ....	81
Table 20 - Structure of the unit of competence 3.4. - Programming of the Module 3 – Content Creation.....	83
Table 21 - Global structure of the Module 4 – Safety.....	87
Table 22 - Structure of the unit of competence 4.1. – Protecting devices of the Module 4 – Safety.....	88
Table 23 - Structure of the unit of competence 4.2. – Protecting personal data and privacy of the Module 4 – Security.....	109
Table 24 - Structure of the unit of competence 4.3. – Protecting health and well-being of the Module 4 – Security. ....	117
Table 25 - Structure of the unit of competence 4.4. – Protecting the environment of the Module 4 – Security.....	125
Table 26 - Global structure of the Module 5 – Problem solving. ....	131
Table 27 - Structure of the unit of competence 5.1. – Solving technical problems of the Module 5 – Problem Solving.....	132
Table 28 - Structure of the unit of competence 5.2. – Identifying needs and technological responses of the Module 5 – Problem Solving. ....	139
Table 29 - Structure of the unit of competence 5.3. – Creatively using digital technologies of the Module 5 – Problem Solving. ....	149
Table 30 - Structure of the unit of competence 5.4. – Identifying digital competences gaps of the Module 5 – Problem Solving.....	154
Table 31 – Identification of the criteria of evidence of each unit of competence, for the assessment of the domain of the competence by adult learners. ....	161

## ABBREVIATIONS

EQF	European Qualification Framework
ECVET	European credit system for vocational education and training



# EXECUTIVE SUMMARY








The **training manual for a digital competent citizen** was developed in the framework of the [No One Behind](#) project to guide trainers and learners through an easy pathway to promote digital skills of adults from rural areas.

The manual provides a training curriculum and materials to support adult educators (and other stakeholders) in the development of digital skills of adults from rural areas, allowing them to become “digitally competent citizens”.

The training curriculum was structured based on the profile of the **digital competent citizen**, also designed by the consortium in accordance with the principles of the European credit system for vocational education and training (ECVET)<sup>1</sup> and the European Qualification Framework (EQF)<sup>2</sup>. The profile is briefly presented in the beginning of this manual.

In terms of structure and contents, the curriculum and materials are related with [the DigComp – European Digital Competence Framework for citizens](#) and thus contains 5 training modules, covering 21 digital competences of the framework:

-  Information and data literacy
-  Communication and collaboration
-  Digital Content Creation
-  Safety
-  Problem Solving

For each one of these modules, this manual provides:

- an overview of the objectives, contents and structure to be followed by adult educators and learners;
- specific plans, activities and resources related to the units of competence identified in each module and fostering the development and reinforcement of adults’ digital skills.

Is also part of this document a set of grids to support the assessment of the level of development of digital competences of adults from rural areas, to be done before and after the training take place.

<sup>1</sup> European Qualification Framework: more information about this can be found [here](#).

<sup>2</sup> European credit system for vocational education and training: more information about this can be found [here](#).

# INTRODUCTION



## 1. Introduction to the *No One Behind* training manual

This training manual is the result of the joint work of diverse organizations thinking of producing a step-by-step guide to promote digital skills within groups of people living in rural areas and promote social inclusion by increasing their digital competency. The units and contents are organized in a way that the manual can be used for self-learning but also as a tool/ guidance for trainers wishing to deliver a training on digital skills for people who have very little digital competencies.





### Who is this manual for?

Adult educators: social workers, teachers, mentors, professors and other professionals who work with adults;




Adults from rural zone willing to improve their daily life, to change their job or to find new opportunities by developing useful digital skills.

The aim of this manual is to guide trainers and learners through an easy and innovative pathway to promote digital skills, following the guidelines of the DigComp framework.

The manual is organized in four main sections as follows:

-  **Executive Summary** – With a synthesis of the content of the training manual, that can be used to introduce it to the target groups and social media.
-  **Introduction** – Starting with a brief introduction to the training manual and with including a short overview of the profile of the "digital competent" citizen presented in the methodology<sup>3</sup>.
-  **Digital competent citizen curriculum** – It comprises five chapters corresponding to the five modules of the training. Each chapter provides information about the structure of the module and the correspondent units of competence. It also provides guidelines and materials to support the implementation of the training and the acquisition/reinforcement of learners' digital competences.
-  **Evaluation of the training** – This section provides directives related with the evaluation of the digital competences and learning of learners, providing the supports to assure it. It also provides supports for the evaluation of the training by learners.

A set of annexes to support the implementation of the training are also provided in this document, including:

-  **Annex I – Additional resources** – With links related to the modules and units of competences included in this training manual, that trainers and learners can access to know more.
-  **Annex II – Evaluation sheet Module 1** – An evaluation grid to be used to measure the level of development of the learners' digital competences related to *Information and data literacy*.
-  **Annex III – Evaluation sheet Module 2** – An evaluation grid to be used to measure the level of development of the learners' digital competences related to *Communication and Collaboration*.

<sup>3</sup> The full presentation of the profile is available in the document *Innovative methodology for educating and training adults from rural zone to improve their digital and ICT skills*. Accessible [here](#).



[Annex IV – Evaluation sheet Module 3](#)– An evaluation grid to be used to measure the level of development of the learners’ digital competences related to *Content Creation*.



[Annex IV – Evaluation sheet Module 4](#)– An evaluation grid to be used to measure the level of development of the learners’ digital competences related to *Safety*.



[Annex V – Evaluation sheet Module 5](#)– An evaluation grid to be used to measure the level of development of the learners’ digital competences related to *Problem Solving*.



[Annex VI – Evaluation of the training](#) - Evaluation grid for the evaluation of the quality and relevance of the training by learners.



## 2. Profile of the "digital competent" citizen

Behind the training course introduced in this manual is the profile of the “digital competent” citizen, defined as shown in the scheme below (Figure 1.):

### Digital competent citizen

#### OVERVIEW

EQF<sup>4</sup> Level

3

EQF credits: 5

**Description:** The "digital competent" citizen will be able to:

- understand the usefulness of digital competences
- use in everyday life the main digital systems
- understand the risks and possible threats connected to the Internet environment
- understand how to interact with others and use technologies to access services

#### GLOBAL STRUCTURE

Nr.	Module	Duration	Credit
1	Information and data literacy	25h	1
2	Communication and collaboration	25h	1
3	Digital content creation	25h	1
4	Safety	25h	1
5	Problem solving	25h	1

Figure 1 – Overview and global structure of the Digital Competent Citizen profile, as defined by the consortium and in accordance with the ECVET<sup>5</sup>.

Each module is structured in units of competences, essential to guide adult educators and learners in the acquisition, development and consolidation of digital competences (Figure 2.).

<sup>4</sup> European Qualification Framework: more information about this can be found [here](#).

<sup>5</sup> European credit system for vocational education and training: more information about this can be found [here](#).



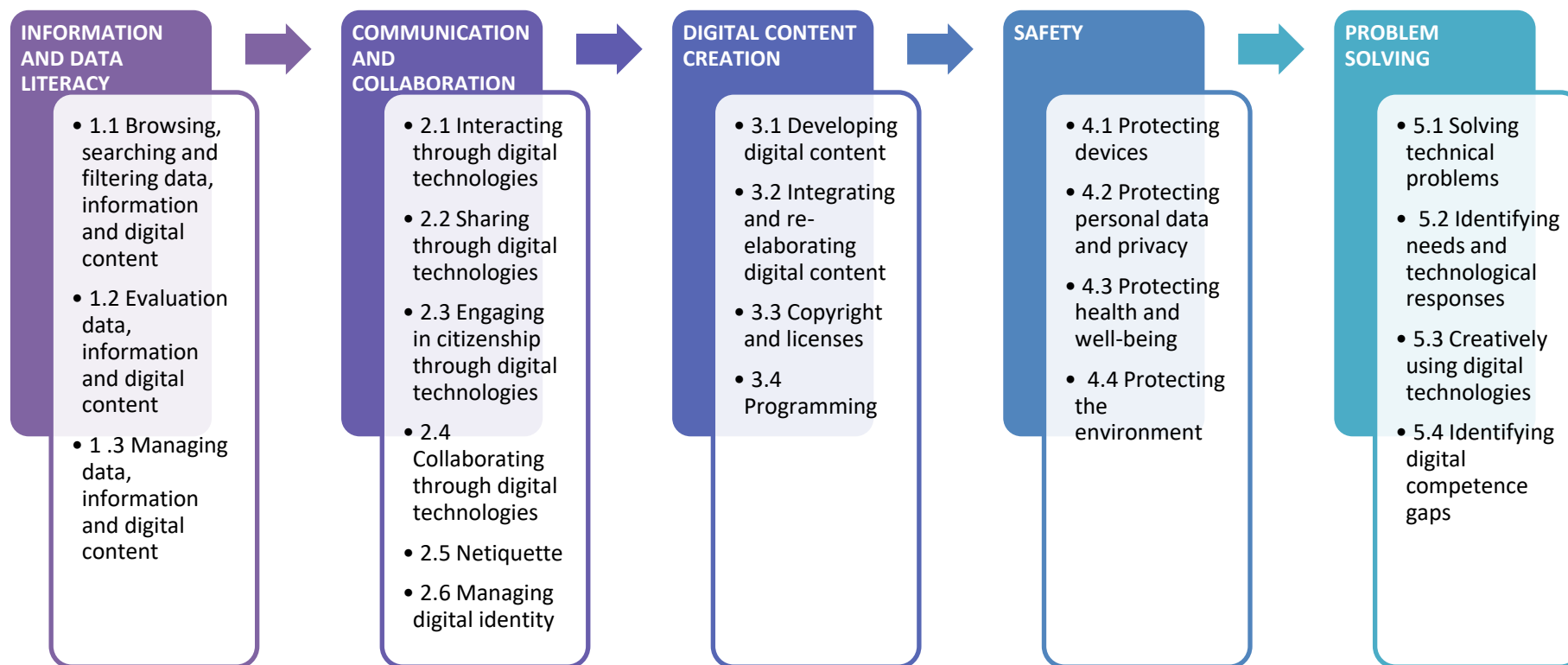


Figure 2 – Identification of the units of competences correspondent to the modules of the profile for a digital competent citizen.

These units of competence are described in the document *Innovative methodology for educating and training adults from rural zone to improve their digital and ICT skills*<sup>6</sup> in terms of knowledge, skills and competences.

<sup>6</sup> Accessible [here](#).

# DIGITAL COMPETENT CITIZEN CURRICULUM



This section is dedicated to the **Digital Competent Citizen** curriculum where you have access to:

- a global overview of the structure of the curriculum;
- brief presentation of the 5 modules comprising the curriculum;
- specific plans, activities and resources related to the units of competence identified in each module and fostering the development and reinforcement of adults' digital skills.

The Table 1. Presents the global structure of the **Digital Competent Citizen** curriculum as structured in the scope of No One Behind project:



Training course	Digital Competent Citizen
Duration	125h
Targets	Combination of face-to-face session with online sessions and self-study.
Training organization	Blended learning, combining face-to-face training with online sessions.
Main goal	 This manual aims at becoming a reference for trainers when working with adults with low digital skills. To achieve this goal, the manual comprises theoretical content and practical activities to elicit learning.  This manual aims to support trainees and adults to enhance their digital skills, by providing step-by-step activities.
Training Plan	The course is structured in five modules: <ul style="list-style-type: none"> <li>• Module 1 - Information and data literacy (25h)</li> <li>• Module 2 - Communication and collaboration (25h)</li> <li>• Module 3 - Digital content creation (25h)</li> <li>• Module 4 – Safety (25h)</li> <li>• Module 5 - Problem solving (25h)</li> </ul>
Learning assessment	Assessment sheets for each module and unit ( <i>provided at the end of the manual</i> )
Training assessment	Assessment sheets ( <i>provided at the end of the manual</i> )

Table 1 – Curriculum of the Digital Competent Citizen training course.

As it can be seen, the curriculum is organised in 5 modules, each one with a specific propose and divided into units of competence as shown in Table 2.:

<a href="#">Module 1</a> <a href="#">Information and data literacy</a>	
<p>This module introduces the tools and competencies needed to perform online searching, while presenting different strategies and techniques available to find reliable information. By the end of this module, it is expected that learners know how to manage information, being able to save it in technological devices, retrieve it though being aware of copyrighting laws and data protection.</p>	1.1. Browsing, searching and filtering data
	1.2. Evaluating data, information and digital content
	1.3. Managing data, information and digital content
<a href="#">Module 2</a> <a href="#">Communication and collaboration</a>	
<p>In this module, learners will develop skills and abilities to engage with others using digital technology. They will be able to interact and share information, being aware of netiquette and personal identity online.</p>	2.1. Interacting through digital technologies
	2.2. Sharing through digital technologies
	2.3. Engaging in citizenship through digital technologies
	2.4. Collaborating through digital technologies
	2.5. Netiquette
	2.6. Managing digital identity
<a href="#">Module 3</a> <a href="#">Digital content creation</a>	
<p>The objective of this module is to promote competencies at creating digital content and programming, so learners feel confident at, for instance, promote their own business online.</p>	3.1. Developing digital content
	3.2. Integrating and re-elaborating digital content
	3.3. Copyright and licenses
	3.4. Programming
<a href="#">Module 4</a> <a href="#">Safety</a>	
<p>When completing this module, learners must become aware of actions they can take to protect devices, their health and the environment when using technology. This module also aims at raising awareness to privacy and personal data.</p>	4.1. Protecting devices
	4.2. Protecting personal data and privacy
	4.3. Protecting health and wellbeing
	4.4. Protecting the environment
<a href="#">Module 5</a> <a href="#">Problem solving</a>	
<p>This module highlights technical problems and strategies to deal with the most current issues when operating a computer. Additionally, learners will have the chance to think of creative methodologies when using digital tools.</p>	5.1. Solving technical problems
	5.2. Identifying needs and technological responses
	5.3. Creatively using digital technologies
	5.4. Identifying digital competence gaps

*Table 2 – Brief description and identification of the units of competences of each module of the training course.*

Following this structure, you can find in this section five chapters, each correspondent to one of the modules of the curriculum. At the beginning of each chapter, you will have a table with an overview of the duration, objectives and units covered in the module. It follows the presentation to the units of competences in terms of duration, objectives, content, resources and training methodologies and how the units could be delivered. For each unit you will find both theoretical information and practical activities, so the learning experience flows easily and hopefully enables a “hands-on” approach.

Therefore, many activities are suggested throughout the manual, making use of diverse learning methodologies such as:

Method	Description
Presentation by trainer	Participation of the learners on lessons based on <i>PowerPoint</i> presentations, videos visualization, demonstration, research studies, books, papers or other resources and supports displayed by the trainers in a training session or e-learning platform. Additional supports - case studies, assignments and quizzes – can be used, enabling their expertise consolidation and knowledge increment.
Group exercise Discussion / Debate	It can be made in large or smaller groups and the idea is to promote the discussion or debate between learners related to a specific topic launched by the trainer. The discussion or debate should be monitored to allow the participation of all learners and the focus on the relevant topics. At the end of the discussion or debate is important to draft and share some conclusions.
Working in pairs / Small groups	The trainer must provide each small group with exact information about the topic, the expected outcomes of the group work (also the method of presentation of the outcomes – the group should be clear about who is going to present these outcomes at the beginning of the work) and the duration of the group work. Before starting the exercise, the trainer and all learners check the time, and the trainer tells the learners when to meet again in the large group to avoid any misunderstandings. During the group work the trainer assists all groups and keeps an eye on the timetable.
Presentation by participants	Trainers can challenge learners to prepare a presentation on a certain topic and moderate a learning session. Learners can choose the format of presentation (e. g. PowerPoints, activities, videos,...) and engage other learners in the different moments of the presentation.
Simulation / Role plays	Role playing is a learning method in which learners assume roles of characters and collaboratively create stories. This technique is an excellent tool for engaging learners and allowing them to interact with their peers as they try to complete the task assigned to them in their specific role. This work can be done in cooperative groups and/or learners can maintain the persona of their role throughout the class period. Students are more engaged as they try to respond to the material from the perspective of their character.
Project based Learning (PBL)	PBL is a teaching based on projects or integrated tasks. Starting from a concrete problem, learners are challenged to develop projects that respond to real-life problems allowing them to actively be involved in their learning, learn by doing and acquire/reinforce their skills.
Cooperative Learning	It is a discussion-based methodology, where a small group of learners discusses a topic launched by the trainer. Three main roles must be distributed among learners: 1) the scribe takes notes on the debate so that all the other learners can be fully engaged in the conversation; 2) the little map drawer monitors who is speaking and when and draws the conversation's evolution; 3) the moderator makes sure that the conversation does not stay on one topic for too long or move too quickly, and that everybody talks. The trainers only intervenes when necessary.
Flipped Classroom	It is a pedagogical approach in which the traditional elements of the lesson taught by the trainer are reversed: the primary educational materials are studied by the learners at home and, then, worked on in the session.
Station Learning	With help of the station learning method content is processed individually and needs-oriented. The trainer prepares a learning station for each application component, at which work assignments and working materials are available. The learners can choose the stations that interest them in terms of content and that they rate as important for their individual application. The trainer is always available for questions. The learners take notes and later will also have access to the materials / samples etc. of all stations. They can choose their own learning path from station to station.

*Table 3 – Identification and brief description of the methods considered in this manual.*

## Module 1: Information and data literacy

The first module will introduce you to the online searching procedures, focusing also in how to evaluate the information, how to store, retrieve it and use it responsibly.

Please note that practical activities described in each unit might entail the support of an experienced trainer. Although the information presented in the manual is written in a way that is easy to understand, some actions, adjacent to the information presented, may require the supervision and support of experienced people.





Module 1	Information and data literacy		
Duration	25h		
Objectives	 To search reliable information online using different browsers and search engines  Perform online searching in a safety and secure manner  Identify possible fake news and misleading information on websites  Organize, store and retrieve information		
Units	1.1 Browsing, searching and filtering data, information and digital content	1.2 Evaluating data, information and digital content	1.3 Managing data, information and digital content
Training organization	Face-to-face E-learning	Face-to-face E-learning	Face-to-face E-learning
Duration	9h	8h	8h

Table 4 – Global structure of the Module 1 – Information and data literacy.



## 1.1. Browsing, searching and filtering data










Unit 1.1	Browsing, searching and filtering data, information and digital content	
Duration	9 hours	
Objectives	 To use different browsers and search engines for online searching;  To perform an online search on a specific subject, selecting reliable sources of information;  To identify suspicious websites and misinformation;  To save and retrieve data such as documents, images, websites;  To manage the digital environment taking into account privacy settings and confidentiality	
Content	1.1.1 Main concepts: IT, ICT and Internet 1.1.2 Introduction to searching online 1.1.3 Protection when using ICT 1.1.4 Practical activities	
Resources	Training manual Computer with internet access Flipchart papers Markers Case study 1 and 2	
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Working in pairs / Small groups  Presentation by participants	

Table 5 – Structure of the unit of competence 1.1. - Browsing, searching and filtering data of the Module 1 – Information and data literacy.

### 1.1.1. Main concepts: IT, ICT and Internet

In order to introduce you to this module, we would like to present two main concepts that you probably hear a lot when talking about computers technology. These are:

**IT (Information Technology)** - encompasses all of the technology that we use to collect, process, protect and store information. It refers to hardware, software (computer programs), and computer networks.






**ICT (Information and Communication Technology)** - this concept involves transfer and use of all kinds of information. ICT is the foundation of economy and a driving force of social changes in the 21st century. Distance is no longer an issue when it comes to accessing information; for example, working-from-home, distance learning, e-banking, and e-government are now possible from any place with an Internet connection and a computing device.

#### Take note:

ICT includes all technical means that are used for handling information and facilitating communication, including computers, network hardware, communication lines and all the necessary software. In other words, ICT is comprised of information technology, telephony, electronic media, and all types of process and transfer of audio and video signals, and all control and managing functions based on network technologies.

#### Internet

Internet ("network of all networks") is a global system comprised of interconnected computers and computer networks, which communicate by means of using TCP/IP protocols. Although, in its beginnings, it emerged from the need for simple data exchange, today it affects all domains of society, for example:

-  **Economy:** Internet banking (paying bills, transferring funds, access to account, access to credit debt, etc.), electronic trading (stocks, various goods, intellectual services, etc), etc.
-  **Socializing:** social networks, forums...
-  **Information:** news portals, blogs etc.
-  **Healthcare:** diagnosing disease, medical examinations (for people living on an island or in other remote places, some examinations, that require a specialist, can be done remotely), making appointments for medical examinations, the exchange of medical data between hospitals and institutes, surgery and remote surgery monitoring
-  **Education:** online universities with webinars (web + seminar), websites with tutorials, expert advice, online training, etc.

Internet really does have many applications and a huge social impact. Perhaps the most important trait is information exchange, because information exchange among people enables collaboration, collaboration of like-minded people leads to ideas and actions in real life and coordinated actions of people results in social change.

**Now that you learnt more about technology and the potential of the internet at changing the world, take a moment to think about how it may affect you and your personal life.**

You might be wondering right now... ok, this idea of connecting with others in such an easy way sounds amazing, but how do I use these tools? That's the first topic on this manual: searching online and learning to browse, search and filtering information.

### 1.1.2. Introduction to searching online

The ability to search for information online is one of the most important digital literacy skills you can possess. It allows you to quickly find what you are looking for without having to sift through pages of irrelevant results. The most important tool in this process is the search engine, which is a specialized website that searches for information across the Internet. You have probably heard of the most popular ones, including Google, Yahoo!, and Bing, and while each of them are useful, they can also yield different results. Overall, Google is the most popular search engine. It is so popular, in fact, that it is even become a common verb, like when someone says, "I'm googling the address right now".

#### How to start searching

In order to start a search you will need to click on a **browser**. A browser is a software that allows a computer user to find and view information on the Internet and there are different ones available to users. Internet Explorer, Mozilla's Firefox and Chrome are just some of them and you usually find them at the bottom line of your computer's desktop.



*Figure 3 – Icons of some browsers.*

Then go to the search engine's homepage, for example [google.com](https://www.google.com), and type your search terms into the text box. To see your results, you can press the Enter key, or you can click an icon, such as the Google Search button or a magnifying glass.



Figure 4 – Google homepage.

Depending on your browser, you may be able to conduct a search right from the browser's interface. For example, in Chrome, you can enter your search term directly into the address bar. In Internet Explorer (pictured below), you can use either the address bar or the built-in search bar to start a search.



Figure 5 – Chrome homepage.

## Search Strategies

With a few basic search strategies, you can usually find almost anything you want. It does not matter if you are using Google or any other search engine because these techniques are effective no matter where you search.



**Keep it simple:** Make your searches brief by focusing on keywords, then keep the number of these keywords to a minimum. This way, you are more likely to get relevant results.



**Consider suggestions:** As you enter your term, search engines will suggest the most popular results involving the term so do not be afraid to select one, as they can often give you plenty of new ideas.



**Use natural language:** You do not have to use complicated words or phrases to get results. Search engines can recognize the language you naturally use in your everyday life, so feel free to try whatever comes to your mind.

Depending on your search, the format of your results may vary based on what the search engine thinks will be most useful. This means your results could include maps, a portion of a Wikipedia article, lists, and more. Search engines can find many other types of content in addition to webpages. With only a click or two, you can also search for images, videos, news, and more.

Before you start your online experience, we would like to draw your attention for something of utmost importance: **online security and privacy settings**.




### 1.1.3. Protection when using ICT

Information security is defined as preservation of information confidentiality, integrity and availability.

**Information security measures** are the rules of data protection on physical, technical and organizational level. User authentication involves user identification, so individuals can gain access to a certain content (data). For example, to check your e-mail via browser, i.e., access an account, it is necessary to enter a username and password. If the required information is entered correctly, access is granted. Passwords should, for security reasons, be kept confidential. A password is a key (like a key to access your home or a car) that allows access. As you would not share your apartment or car keys with just anyone, you should not share your password either. Nowadays, many people have home security doors with locks whose keys are difficult to copy, with the aim of blocking unauthorized home intrusion. Passwords should be created with the same caution. The more complex your password is, the harder it will be to break through (crack it), therefore it is less likely that someone will gain unauthorized access to your data.

When choosing a password, it is advisable to use punctuation, numbers and a mix of uppercase and lowercase letters. A minimum length of 8 characters is recommended (shorter passwords are easier break through). From time to time, it is necessary to change the password. That way, the possibility of its detection decreases.

Some of the most common mistakes when choosing passwords are:

-  using words from a dictionary
-  passwords based on personal information, such as name or birth date, employment place etc.
-  characters that follow the order given on a keyboard: 123, qwert, etc.

**Website's safety:** to see whether a website is safe to visit, you can check for security information about the site. Check to the left of the web address for the security status:

-  If you see a lock icon next to a website's address it means the traffic to and from the website is encrypted.

It is also verified, which means the company running the site has a certificate proving they own it. Selecting the lock icon, you can see more information about the site, such as who owns it and who verified it.

If you do not see a lock icon, your connection is not private and any traffic could be intercepted.









Figure 6 – Identification of the lock icon.

### Personal information – a few things to bear in mind!

You need to be careful with how much personal information you reveal online. Sharing your address, phone number, birthday and other personal information can mean you are at a greater risk of identity theft, stalking and harassment. This includes information you post on social media.

Cybercriminals can piece together your identity from information that is publicly available about you, so think about what information you are sharing online.

Therefore, here are a few things to consider when using the internet:

-  Use a separate email address for shopping, discussion groups and newsletters. If you need to, you can then change this address without disrupting online business activities.
-  Only share your primary email address with people you know.
-  If you use social media, adjust your privacy settings to control the amount and type of information you share.
-  When creating an account take the time to familiarise yourself with social media privacy policies.
-  Only make online purchases from companies that have a clear privacy policy and secure payment options
-  Think before you fill out online forms and be careful with who and how you share your information. Ask yourself, do I really need to give my information to this site?

### 1.1.4. Practical activities

After each theoretical description of the contents, we suggest you some group dynamics to enhance learning. These activities are described step-by-step.

When delivering training, it is important that trainers and learners feel comfortable within the group so they feel happy to share experiences, questions and so on. The more people feel at ease with their colleagues, the better is the learning experience. Therefore, we suggest that each activity starts with an icebreaker, if possible something fun which allows people to present themselves to the group without feeling intimidated.

At the presentation stage, the trainer might want to invite people to share what they would like to learn, what animal they would like to be, what is their favourite dish, what colour is their toothbrush and any other subject, considering it is something not too personal.

#### Step 1: Icebreaker “I’m the only one”

Everyone spreads around the room making a closed circle. Trainer explains that a ball will go around stopping on each person in the circle. Whoever has the ball must say their name and one thing they are the only ones at knowing or doing in the group. They may also talk about an exquisite interest or taste. If another member of the group shares the same skill, the person who spoke must find something else which is different.



The ball does not have to follow an order, so people might toss it to anyone in the group, just making sure each person has a chance to speak.

You can adjust this icebreaker to an online format by instructing people to nominate a colleague to speak instead of tossing a ball.

## Step 2: Brainstorming kick off

In order to introduce the subject of online searching but also to gather an idea of where people are in terms of common knowledge, start this unit with a brainstorming.

Make sure you have a whiteboard ready to register everyone's inputs. If the activity is run online, you can use an online platform to support with registering (ex. <https://padlet.com>) or even share a word document with the group where you can just type their answers.

Inform participants that there are no right/ wrong answers because the idea is to share with the group what we already know/ may not know. Possible questions:



What is an online search?



How may this knowledge be helpful on our daily lives?



How does information end up on the internet?



What kind of risks may one encounter while searching online?

## Step 3: Online searching – hands on!

Show participants different web browsers: Google Chrome, Safari, Mozilla Firefox, Edge, Internet Explorer, explaining these are software programmes to access the World Wide Web and navigate through different pages; show participants where they can find the browsers in a computer; (10 minutes)

You can also use the following tutorial in order to introduce the topic of how to use a search engine: <https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/>

The trainer shows how to search for “organic fertilizer” (this is an example, but it is advisable that you choose a meaningful subject for your group); Show the group how to look on different pages and how to use different “search expressions”; (10 minutes)

Now, invite each participant to search online for information about the dangers of fake news and write down three main facts they have found; (20 minutes)

Group discussion: each participant presents the results of their search. (20 minutes)

#### Step 4: Analysing, storing and presenting information

Have a list of different topics ready for participants to explore online. Ex: mental health during the pandemic, the best recipes in the world, extreme sports, the importance of the bees, trees diseases, industrial revolution, robots in technology, healthy lifestyle, etc.

Ask the group to organize in pairs and choose a topic to work on. The main goal in this activity is 1) to compile reliable information on the topic chosen, 2) select and store the information in the desktop (in a folder created by the student) and 3) set up a short presentation (10 minutes long) ensuring they have used trustworthy sources. Learners must register the websites and references used as this will be assessed at the end.

For those learners who might not be able to use software to work on the presentation, trainer must provide flip chart paper and markers. Even if not using the computer to present information, they must be able to search images, graphics or videos to illustrate their search and store them in their desktop's folder. (4 hours)

Once this task is finished, each group must present the work to colleagues. (90 minutes)

#### Step 5: Privacy settings online

Provide learners with Cases Study 1 and 2. Additionally, you might want to invite them to watch a quick tutorial on privacy and security on Chrome: <https://www.youtube.com/watch?v=zMXl6waGFp4>



Split up learners into two groups to work on each case. They must read and answer the questions, supported by online information on cyber security. (30 minutes).



Each group will produce a factsheet<sup>7</sup>, pointing out ten steps to avoid privacy breaches while using the internet (20 minutes)



Group debate (40 minutes)

<sup>7</sup> Trainees may do this on the computer or a flipchart paper, depending on their pre-existent digital skills.

## Case study 1 - Jane

Read the following situation and discuss within your group what happened and answer the questions below to guide the debate. Then, write down the main conclusions so you can present your ideas to the group.

*“Jane signs onto the Internet, preparing for what most would deem a typical, innocuous Web browsing experience. Jane purchases some clothing for herself and her two- and five-year-old children on an up-scale department store’s Web site. She then follows with an extended review of a Web site featuring weight loss plans. Although most would consider this browsing experience a litany of mundane transactions, a savvy direct marketer with the ability to covertly monitor these activities considers the information obtained priceless. As surprising as it may be too many Web surfers, assembling an alarmingly detailed profile of Jane, without her knowledge or consent, is quite possible with a single browsing activity such as the one previously outlined. Although this scenario requires some inferences, a marketing profile of Jane’s transactions might develop as follows: Jane is a mother with two young children, purchases some up-scale goods, and is seriously concerned about her weight and health. Based on her, a merchant or vendor might want to send Jane advertisements, e-mails, banner, advertisements, or pop-up advertisements that offer expensive home exercise equipment. The equipment would allow her to stay at home with her children, aid with her fitness goals, and be affordable based on her observed consumer spending pattern. An advertisement for exercise equipment may not bother Jane at all. In fact, she may actually be interested in home exercise equipment instead of a different ad that would have been randomly posted on her computer screen as she browsed the Web. However, Jane might be very disturbed by the covert means employed by the merchants to collect, aggregate, use, and/or sell her personal information without asking her for permission or notifying her of their intent to use the information in that manner.*

Groemminger, B. K. (2003). *Personal privacy on the internet: should it be a cyberspace entitlement*<sup>8</sup>.

**1) What privacy settings or actions could Jane take to avoid her information to be spread through commercial companies?** (Possible answers below)

- She should pay attention to cookies permissions, by only allowing necessary ones
- She could delete the search history once finished or sign in as anonymous – this is particularly relevant if using a public computer
- She must log out of her email or other accounts she might have signed in.

**2) What kind of safety measures would you take into account when shopping online?** (Possible answers below)

- Check the safety of the website - see if it is a safe connection
- Create a virtual card with a specific amount of money
- Use credible platforms for payments like PayPal
- Ensure you run a virus scan and your computer is secure
- Avoid using a public network connection while shopping

<sup>8</sup> Accessible [here](#).

## Case study 2 - Mary

**Read the following situation and discuss within your group what happened and answer the questions below to guide the debate. Then, write down the main conclusions so you can present your ideas to the group.**

*Mary is 22 years old and she is very knowledgeable on social networking as she calls herself “an influencer”. She believes that regular exercise and good nutrition are the pillars for a healthy living and she writes many posts and suggestions on Instagram about it. She has reached just over 10000 followers and she is very proud about it. Recently some people wrote to her, complaining they had fallen on a cyber-attack due to messages sent in her name. At the beginning she does not know how to explain this, but then she realises she has been hacked. Two days ago, she received a message informing she had won an online competition. At the beginning she found the message a little suspicious, as she could not recognize the sender, but then she clicked the link and completed a form with personal details. As there was no prize, she then found out it was a scam. Being aware of that, she posted an alert on social media informing everyone to not open messages from her.*

- 1) What else could Mary do once she realised what happened?** (Possible answers below)
  - reset the passwords (email, phone, social media, banking, etc.) and ensure those passwords are strong (minimum 8 characters with capitals, numbers, etc.)
  - ensure the anti-virus is up to date / run a virus scan
  - back up her data
  - take the device to an IT professional
- 2) What could Mary do to avoid this situation?** (Possible answers below)
  - She should have checked twice the sender and never open the message/ link if suspicious
  - She should have checked the website address and see if it was marked as dangerous
  - She should not give personal details while not sure of what that was

## 1.2. Evaluating data, information and digital content

The unit 2 is related with the evaluation of information, assess its credibility and sources.










Unit 1.2	Evaluating data, information and digital content
Duration	8 hours
Objectives	 To analyze and assess the credibility of information online  To take steps to evaluate different sources of information  To understand each one's responsibility when sharing misinformation online  To be aware of how personal values and judgements influence understanding of information
Content	1.2.1 How to assess sources and information online 1.2.2 Evaluating your sources 1.2.3 Evaluating websites 1.2.4 Fact-checking websites 1.2.5 Practical activities
Resources	Training manual, computers with internet access, True or False cards
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Working in pairs / Small groups  Presentation by participants  Media selection

Table 6 - Structure of the unit of competence 1.2. Evaluating data, information and digital content of the Module 1 – Information and data literacy

### 1.2.1. How to assess sources and information online?

By the time you reached this part of the manual you already have a clear idea of what information you can find online: pretty much everything! This affirmation introduces the next unit, where you will learn how to evaluate data, so you are able to look for reliable sources and therefore contribute to sharing factual information online.

Unlike similar information found in newspapers or television broadcasts, information available on the Internet is not regulated for quality or accuracy. Therefore, it is particularly important for the individual Internet user to evaluate the resource or information. Keep in mind that almost anyone can publish anything they wish on the Web. It is often difficult to determine authorship of Web sources, so **it is really your responsibility to judge the accuracy of your sources**. Despite the main resources to do so is your judgement and reasoning, there are a few actions that can help you to increase the odds in favour of reliable information.

### Ask yourself these questions before using resources from the internet:

1. Who is the author? Is the author qualified to write on the topic? In case it is an organization, is it credible? Did I hear about it?
2. What is the purpose of the site? Who is the intended audience?
3. Is the information and language objective, impartial and free of emotion-rousing expressions?
4. Are the factual sources listed so information can be verified?
5. Is information supported by evidence?
6. How old is this information? When was the site last updated?

### Last but not least... **Check your emotions!**

Be mindful of when a tittle has the power to change your emotional state. This is not only a very old technique to draw your attention, but it has been used as a clickbait for fake news spreading. Our normal inclination is to ignore verification needs when we react strongly to content, and researchers have found that content that causes strong emotions spreads the fastest through our social networks (Matthew Shaer, 2014). So, **read beyond the headlines!**



### 1.2.2. Evaluating your Sources

In your search for information, you eventually face the challenge of evaluating the resources you have located and selecting those you judge to be most appropriate for your needs. Examine each information source you locate and assess sources using the following criteria, also known as the **TAARP method**:

#### **T – Timeliness**

Your resources need to be recent enough for your topic. If your paper is on a topic like cancer research, you would want the most recent information, but a topic such as World War II could use information written in a broader time range.

#### **A – Authority**

Does the information come from an author or organization that has authority to speak on your topic? Has the information been peer-reviewed? (You can use Ulrichsweb to determine if a journal is peer-reviewed). Do they cite their credentials? Be sure there is sufficient documentation to help you determine whether the publication is reliable including footnotes, bibliographies, credits, or quotations.

#### **A – Audience**

Who are the intended readers and what is the publication's purpose? There is a difference between a magazine written for the general public and a journal written for professors and experts in the field.

#### **R – Relevance**

Does this article relate to your topic? What connection can be made between the information that is presented and your thesis? An easy way to check for relevance is by reviewing the Abstract or Summary of the article before downloading the entire article.

#### **P – Perspective**

Biased sources can be helpful in creating and developing an argument, but make sure you find sources to help you understand the other side as well. Extremely biased sources will often misrepresent information and that can be ineffective to use in your paper.

### 1.2.3. Evaluating websites

Websites create an interesting challenge in evaluating credibility and usefulness because no two websites are created the same way. The TAARP method described above can be used, but there are additional things you want to consider when looking at a website:

**The look and feel of the website** - Reliable websites usually have a more professional look and feel than personal Web sites.

**The URL of your results** - The .com, .edu, .gov, .net, and .org all actually mean something and can help you to evaluate the website!

**Informational Resources** are those which present factual information. These are usually sponsored by educational institutions or governmental agencies. (These resources often include **.edu** or **.gov**.)

**Advocacy Resources** are those sponsored by an organization that is trying to sell ideas or influence public opinion. (These resources may include **.org** within the URL.)

**Business or Marketing Resources** are those sponsored by a commercial entity that is trying to sell products. These pages are often very biased, but can provide useful information. (You will usually find **.com** within the URL of these resources.)

**News Resources** are those which provide extremely current information on hot topics. Most of the time news sources are not as credible as academic journals, and newspapers range in credibility from paper to paper. (The URL will usually include **.com**.)

**Personal Web Pages/Resources** are sites such as social media sites: blogs, Twitter pages, Facebook, etc. These sources can be helpful to determine what people are saying on a topic and what discussions are taking place. Exercise great caution if trying to incorporate these sources directly into an academic paper. Very rarely, if ever, will they hold any weight in the scholarly community.

**Are there advertisements on the site?** - Advertisements can indicate that the information may be less reliable.

**Check the links on the page** - Broken or incorrect links can mean that no one is taking care of the site and that other information on it may be out-of-date or unreliable.

**Check when the page was last updated** - Dates when pages were last updated are valuable clues to its currency and accuracy.

### 1.2.4. Fact-checking websites

Fortunately, you may also use a **fact-checking website**, where you can check further if the information you found has been flagged as fake. Additionally, you can ask a **librarian**. Here is a list of some fact-checking sites (depending on your home country, it may be interesting to look for fact-checking sites on national news. Those we present are mostly American):



FactCheck.org - <https://www.factcheck.org/>



PolitiFact: sorting out the truth in politics - <https://www.politifact.com/truth-o-meter/>



Urban Legends: Politics - <https://www.snopes.com/fact-check/category/politics/>



Truth or Fiction - <https://www.truthorfiction.com/>



Observador Fact-Check (Portugal) - <https://observador.pt/seccao/observador/fact-check/>

### 1.2.5. Practical Activities

#### Step 1: True or False?

In order to introduce the subject of how to assess the veracity of information we come across online, start with a quick True or False game. You will need to prepare some True/False cards previously and split learners into groups of three. You will present some affirmations related to the topic and each group will have to show the True or the False card, according to their answer. You may correct the answers and give out some information on the topics as you go along.

List of affirmations:

	Affirmation	T/F
1	All the information posted online is reliable.	False
2	Anyone can add information online, even on encyclopaedias	True
3	There are ways to check the credibility of information.	True
4	There is a phenomenon of “fake news” around the world.	True
5	To spot fake news, one could check the web domain.	True
6	The more something is shared, more likely is to be truth.	False
7	Checking the date of the news is not something worth considering.	False
8	Personal values may influence one’s perception of the truth.	True
9	It is usually very easy to identify a fake new.	False
10	There are fact-checking sites available.	True

Table 7 – List of affirmations and correct answer.

## Step 2: How do misinformation spread?

In order to support the learning of how to evaluate data online, you can present a quick video showing how fake news spread.

**Suggestion:** [https://www.youtube.com/watch?v=cSKGa\\_7XJkg](https://www.youtube.com/watch?v=cSKGa_7XJkg)

Upon this, each trainee may entail their own search in order to find **two news likely to be true and two news likely to be false**. Taking into account the information given by the trainer on how to evaluate data's reliability, learners will now have to use some of those strategies in order to select information and be able to explain to colleagues what strategies they have used.

## Step 3: Storytelling activity

The following story talks about two farmers striving to manage their business in a small village. One of them is very literate on digital tools but the other is not very skilled on that. The story highlights the potential of using the internet to spread rumours and fake news. The main goal of the story is to elicit personal thoughts on what is a fake new and how easily someone can do it but also thinking of the impact they may have on our daily life and worldwide.

Also, we aim to promote a debate on the advantages of the internet and how it can be useful to help us reaching information quickly, support us connecting to others who might be able to help, etc. We suggest the trainer to present the following story:

*There were two men in a little village: Robert and Peter. Both were very hard-working people who run big farms and their own business. They used to talk very proudly about the products they sell to the markets as they have always followed procedures to guarantee high quality standards.*

*Peter and Robert have always been neighbours and know each other for over 10 years now. However, we can't say their relationship has always been good, as they have always competed for the regular clients of the village and the small city nearby. They believe there is no place for both in the business of such a small area.*

*In one of his morning walks, Robert finds Peter very worried about his plantations as the lettuces are ruined by what looks to be a plague. He is upset he did not notice this earlier and complains that this week there will be no lettuce to sell in the city's market. He is also worried that, if clients find out what happened, they might see him as incompetent and loose trust in the quality of his products. Also, he does not know how to deal with this plague as it seems to be a completely new virus he has never seen before.*

*Meanwhile, Robert is thinking that actually this unfortunate event might be a chance for him to take down his neighbour's business once and for all! So, he decides to create a Facebook profile of someone who allegedly bought Peter's products and is very unsatisfied. In order to cover the lie even better, Robert found*

*some pictures online and added them in the profile as if they were pictures of Peter's bad products. Then, he starts to send friendship requests to people in the village and quickly the message is spread around.*

*A few days later, Peter realises that his profit has significantly gone down, even in the selling of other products which were not affected by the plague. However, he has no idea of what Robert has been doing on the internet behind his back...*

**Suggested questions for group debate:**

- Why do you think Peter's profit started to go down?
- If you were Peter's client, how do you think you may feel watching pictures of rotten lettuces? Would you still buy his products?
- How easy to you think it is to spread a rumour and misinformation online?
- Considering the impact fake news had on Peter's business, how do you think it may impact politics for example or public health issues related to covid-19? Can you think of any news on covid-19 you may have heard and might not be true?
- Now imagine you were in Peter's shoes... would you have used the internet to help you with the plague? How?

### 1.3. Managing data, information and digital content












Unit 1.3	Managing data, information and digital content
Duration	8 hours
Objectives	 To save and store information using different devices  To manage, locate and retrieve data  To understand copyrighting and licensing rules  To be aware of data protection laws
Content	1.3.1 Devices to save and retrieve information 1.3.2 Copyright and data protection 1.3.3 Practical activities
Resources	 Training manual, computers with internet access, a hat, pieces of paper, 1 to 5 scale (you can use 5 papers numbered 1 to 5), flipchart papers, <i>blu-tack</i> or any material to stick papers on the wall, coloured markers, chairs, table, spoon, horn or any object to make an alarm sound  Access to collaborative learning platform if done online (ex: LAMS, Padle)
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Working in pairs / Small groups  Presentation by participants  Cooperative Learning

Table 8 - Structure of the unit of competence 1.3. Managing data, information and digital content of the Module 1 – Information and data literacy.

#### 1.3.1. Devices to save and retrieve information

Throughout the last units, you learnt how to use computer tools in order to navigate online, while taking into account your safety and privacy. We also covered a very important topic which enables you to be a responsible digital citizen when sharing information, by evaluating data's veracity.

Now it is our aim to take you through the tools available to save your information, store and retrieve it whenever you wish.

In the same way you keep your clothing organized into drawers, you have many resources in your computer to store information. Below we introduce you to some of them.



## Memory and Storage Devices

**ROM (Read Only Memory)** is a type of permanent, internal memory that is used solely for reading.

**RAM (Random Access Memory)** is a working memory in which analysed data and programs are stored, while a computer runs. It allows reading and writing data, and is deleted/cleared when the computer shuts down.

**CD (Compact Disc)** is an optical disc used for data storage. The standard capacity of a CD is 700MB. CD-R is used for reading and writing data one time-only, while CD-RW for reading and writing data multiple times.

**DVD (Digital Versatile Disc)** is an optical disc which is, due to the larger capacity (about 4.7 GB), mostly used for video storage. Blu-ray disc (BD)- the successor to DVD, is an optical disk storage, it comes in different capacities, depending on how many layers it has and the capacity of each layer.

**Memory card** is a type of flash memory used to store data in digital cameras, cell phones, MP3 players etc.

**USB Stick** is a data storage device. It features small dimensions, relatively high capacity, reliability and speed. It belongs to the type of flash memory that remembers data, even when not under voltage i.e. they do not need electric power to maintain data integrity.

*Figure 7 – identification and short description of memory and storage devices.*

To store information, there is also a device called **internal hard disk drive**, which is embedded in the computer case, and an **external hard disk drive**, which is connected to a computer by using an appropriate cable or USB port, and is usually used to transfer data from one computer to another or for backup.

When downloading information from the Internet, it is important to remember that we are using other people's work like articles, books, images, videos, compositions, video games, etc. Therefore, we must understand the concepts of **copyrighting, licensing, and data protection**. However, in the digital era, it has been difficult to establish copyright laws regarding the information posted online. For instance, social media like Facebook does not own work posted on their website, however you must agree to a license where Facebook may use your work for other purposes.

### 1.3.2. Copyrighting and data protection

**Copyright** is a right which is used to protect the author's intellectual property. If someone wants to use such copyrighted work, they must respect the conditions under which the author, as the owner, has allowed the use of his/her work (payment of fees, referencing the original, etc.).

#### Personal data protection

The EU Charter of Fundamental Rights stipulates that EU citizens have the right to protection of their personal data.

**“Everyone has the right to the protection of personal data concerning him or her” and to “access data which has been collected concerning him or her, and the right to have it rectified”<sup>9</sup>**

The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age. More than 90% of Europeans say they want the same data protection rights across the EU – and regardless of where their data is processed.

**Directive 95/46/EC** is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of these data. The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down guidelines determining when this processing is lawful. The guidelines relate to:

---

<sup>9</sup> Source: [https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data\\_en](https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en)

### The quality of the data

- personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be accurate and, where necessary, kept up to date

### The legitimacy of data processing

- personal data may be processed only if the data subject has unambiguously given his/her consent or processing is necessary

### Special categories of processing

- it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis

### Information to be given to the data subject

- the controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.)

### The data subject's right of access to data

Every data subject should have the right to obtain from the controller:

- 1.confirmation as to whether or not data relating to him/her are being processed and communication of the data undergoing processing;
- 2.the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive in particular, either because of the incomplete or inaccurate nature of the data, and the notification of these changes to third parties to whom the data have been disclosed.

### Exemptions and restrictions

- the scope of the principles relating to the quality of the data, information to be given to the data subject, right of access and the publicising of processing may be restricted in order to safeguard aspects such as national security, defence, public security or the prosecution of criminal offences.

Figure 8 – Guidelines related to personal data protection as established on the Directive 95/46/EC.

### 1.3.3. Practical activities

#### Step 1: Pass the hat

Everyone seats in a circle. In the middle of the circle, the trainer places a scale from 1 to 5. It can be a piece of paper with the numbers written or 5 papers, each with a number. Then, trainer explains that a hat will pass around with sentences. The sentences describe personal information from real people that were posted online. Each person must take a piece of paper from inside the hat, reading it out and placing it near a number from 1 to 5, where 1 means “not a serious issue” and 5 means “very serious issue”.

Possible situations:

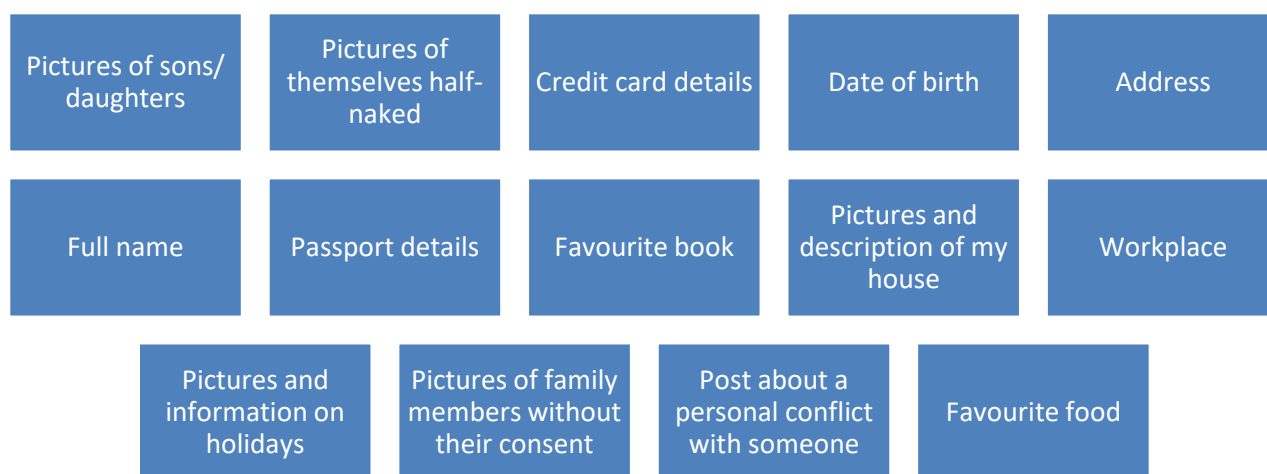


Figure 9 – Identification of possible situations to be considered in this activity.

These are just a few examples you can use to start a conversation around personal information everyone shares online, sometimes without giving it a second thought.

At the end of the activity, when all the sentences are under the numbers 1 to 5, it would be interesting to discuss how people judged each of them. For instance, why sharing a favourite food is not as serious as sharing pictures of family members without their consent?

#### Step 2: Walking brainstorming

This activity is an introduction to the subject of copyrighting, licensing and data protection rules. The trainer will stick three flipchart papers up on the wall (we suggest you stick the papers with *blu-tack*) naming them with “copyrighting”, “licensing” and “data protection”.

Learners are given markers of different colours and they must walk around the room and write a word or more in each paper, according to what comes to mind when thinking of each subject. It is important to highlight that there are no right/wrong answers.

Once everyone has written at least one word, you may start a discussion and then present information on the subjects. You can adapt this activity to an online format by using collaborative learning platforms. We suggest LAMS (Learning Activities Management System) which is a free and open source to develop these sorts of activities online.

### Step 3: Test your knowledge

This activity builds up on the knowledge acquired by learners following the presentation of the subjects in this unit.

Trainer instructs the class that they will have 30 min to review everything that has been taught in the unit. When the time is up, the class is divided into two groups. The trainer places a spoon on a table and the two groups will place themselves in two rows facing each other, in the direction of the table (see Figure 10).

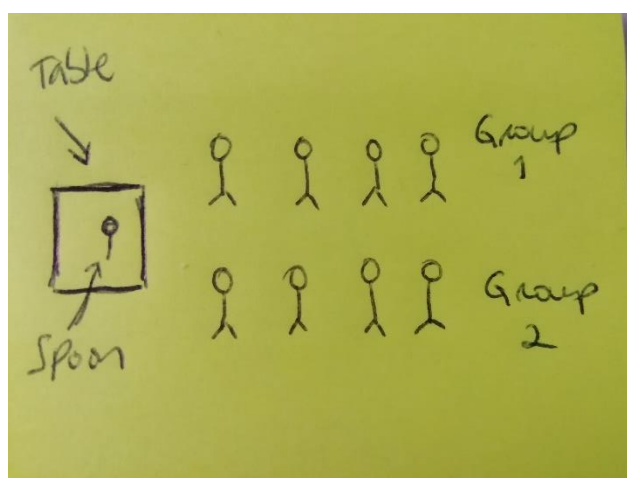


Figure 10 – Division of learners into two groups.



The two learners closest to the table (they must be at the same distance) will be responsible for picking the spoon when they hear an alarm (the trainer will make a sound). The team picking the spoon first have the right to answer a question.



Trainers must prepare a set of questions regarding the subjects taught.



Each correct answer wins 1 point.



Each wrong answer gets -1 point.



Time for answers is 1 minute (trainer may increase it).



In each round, the team swaps the member who is picking the spoon, so everyone has a chance to do it. If running this activity online, you may need to adapt it to a sort of “who wants to be a millionaire?” game.

**Congratulations, you have now completed Module 1.**

**Do not forget to check the Annexes for additional resources and documents provided to support self-study!**



## Module 2: Communication and collaboration

The second module contains information on collaborative platforms and describes subjects related to communication and interaction online.

Please note that practical activities described in each unit might entail the support of an experienced trainer. Although the information presented in the manual is written in a way that is easy to understand, some actions, adjacent to the information presented, may require the support of experienced people.




Module 2	Communication					
Duration	25h					
Objectives	 Being able to use online technologies to collaborate with other people, such as exchanging data and information or organising work in teams.  Being able to behave appropriately in the online environment.  Being aware of the risks and benefits of having an online identity.					
Units	2.1 Interacting through digital technologies	2.2 Sharing through digital technologies	2.3 Engaging in citizenship through digital technologies	2.4 Collaborating through digital technologies	2.5 Netiquette	2.6 Managing digital identity
Training organization <sup>10</sup>	Face-to-face E-Learning	Face-to-face E-Learning	Face-to-face E-Learning	Face-to-face E-Learning	Face-to-face E-Learning	Face-to-face E-Learning
Duration	4h	4h	5h	3h	5h	4h

Table 9 - Global structure of the Module 2 – Communication and collaboration.

<sup>10</sup> It can be: Face-to-face, E-Learning. Blended learning or Self-study.

## 2.1. Interacting through digital technologies












Unit 2.1 Interacting through digital technologies	
Duration	4 hours
Objectives	 Communication Fundamentals (How to Communicate Better)  Learners will consider the importance of email, internet search and digital documents  Learners will use digital tools for everyday tasks in different platforms  Learners will get familiar with social media
Content	2.1.1 The process of Communication and Communication Styles 2.1.2 Effective Email Communication 2.1.3 Social Media Training for Beginners 2.1.4 Practical Activities
Resources	Projector for Power-point presentation (download presentation from the website) Mobile devices/ Computer stations/tablets Headphones Example projects
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Working in pairs / Small groups  Presentation by participants  Media selection  Project based Learning (PBL)  Flipped Classroom

Table 10 - Structure of the unit of competence 2.1. – Interacting through digital technologies of the Module 2 – Communication and collaboration.

## 2.1.1 The process of Communication and Communication Styles

### Communication fundamentals



### Digital Channels and Mediums

A digital **CHANNEL** can be defined as an interface connected to the world wide web through which communication can be made.

- On the Web – websites
- For Search - Search engine results
- Communication – Email and Messaging apps
- Online events – webinar
- Digital Media - Video streaming and Music sites
- Games – Virtual games

A digital **MEDIUM** is a physical way of storing media or archiving it and can hold

- Data
- Graphics
- Audio and video

Digital mediums are well known as digital media, i.e the form of media that can be created, viewed, modified and distributed by electronic devices.

## Communication Styles



**Passive:** Passive communicators often act indifferently and fail to express their feelings or needs allowing others to express themselves.

*“It really doesn’t matter that much.”*



**Aggressive:** Aggressive communicators often express themselves in a “loud” way and tend to issue commands, ask questions in a rude manner and fail to listen to others.

*“I’m right and you’re wrong.”*



**Passive – Aggressive:** These communicators most likely communicate with body language and appear to be aware of their needs, but at times they struggle to voice them.

*“That’s fine with me, but don’t be surprised if someone else gets mad.”*

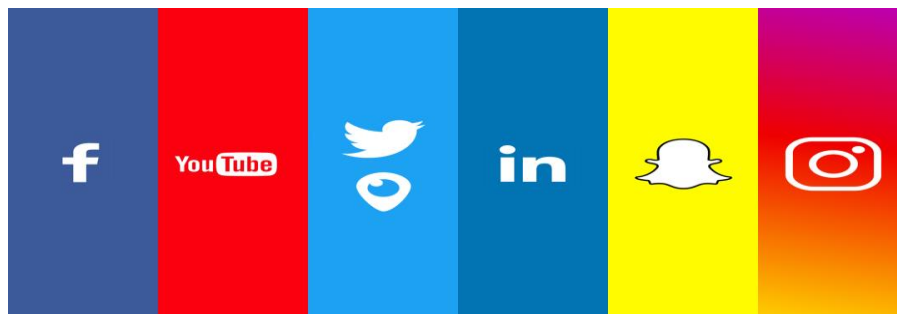


**Assertive:** Assertive communicators can express their own needs, desires, ideas and feelings while also considering the needs of others.

*“I respect the rights of others.”*

## Social Media





Social Media refers to the means of interactions amongst people in which they create, share and exchange information and ideas in virtual communities and networks. The top social media apps **Facebook, Instagram, Twitter, LinkedIn, YouTube.**



## Practical Activities

<b>Module</b>	2
<b>Unit</b>	2.1
<b>Duration</b>	3-4 hours
<b>Type of activity</b>	Practical Activity
<b>Objectives</b>	<p>At the end of the activity learners will be able to:</p> <ul style="list-style-type: none"> <li>◆ Communicate and Interact better through digital tools</li> <li>◆ Using the online platforms depending on the receiver and the content the user wishes to communicate</li> <li>◆ Understanding how to use all digital tools and get familiar with social media</li> </ul>
<b>Setting</b>	<p>For the development of this activity is needed:</p> <ul style="list-style-type: none"> <li>◆ A Projector</li> <li>◆ Powerpoint slides (download from the website)</li> <li>◆ Paper and pens</li> <li>◆ Mobile devices</li> <li>◆ Computers</li> <li>◆ A blackboard</li> <li>◆ Chalk</li> </ul>
<b>Debriefing activity</b>	<p>At the end of the activity learners need to think about:</p> <ul style="list-style-type: none"> <li>◆ What it means to communicate and interact through digital technologies.</li> <li>◆ What advantages does it bring? What disadvantages?</li> <li>◆ How have these tools changed personal and group communication in the past years?</li> </ul>

### Step 1: 40-50 min

-  The educator after getting to know all learners, starts by introducing the module in PowerPoint slides, giving a general definition of what is communication and interaction, and what is defined as digital tools.
-  The educator will assign to each learner a partner and then to each couple a computer station.
-  The educator will ask from each couple of learners to pick an app such as word to write a short letter or a paragraph.
-  Discuss with learners what type of communication or what of interaction is a letter.

### Step 2: 30-40 min

The educator will introduce through PowerPoint slides the Communication Fundamentals.

The educator will ask from all learners for the letter or paragraph they wrote to identify who is




- a. The sender
- b. The receiver
- c. The message
- d. The code

### Debriefing activity

- The educator will discuss with all learners and ask them what do they consider as communication channels, and ask them to provide some examples
- The educator will list all examples for communication channels and mediums provided by the learners on the blackboard.
- The educator will present through PowerPoint slides communication channels and mediums
- The educator will ask how would they categorize the channels, formal, informal, unofficial.

### Step 3: 60 min

This activity is more practical than the first two activities but it will also combine some theory as the educator will introduce the digital tools and will emphasize the use of an online account

-  The educator will introduce the term username, password and online account
-  The educator will guide learners to google.com on their computer stations to create their online account
-  The learners through this activity will work in pairs and each couple will share an account





Once learners have created their Google account, the educator will guide and show them to Gmail and explain the format and the layout of this tool



Ask learners to compose a small letter or a small paragraph in the new message window

## Debriefing Activity

The educator will propose some debriefing questions

- Who would you email? What tone would they use and why?
- What type of communications is email best for?
- What sort of media or files can one attach to an email?

## Step 4: 30-40 min



The educator based on the previous debriefing activity will present through PowerPoint slides the communication styles and communication styles used through digital tools



The educator will introduce and name all Social media



The educator will guide learners step by step to create a Facebook account using their Gmail email address and sign in



The educator will guide learners to check all features on Facebook and send instant messages to the other colleagues.



The educator will also guide them step-by step in creating a small post

## 2.2. Sharing through digital technologies










Unit 2.2 Sharing through digital technologies	
Duration	4 hours
Objectives	 Connecting with others through digital tools  Setting up shared folders on a specific platform  Using and editing a shared file
Content	2.2.1 Use online account on a digital platform 2.2.2 Set up a shared file on a platform 2.2.3 Use comments or make adjustments on a shared file 2.2.4 Practical Activities
Resources <sup>11</sup>	Computer stations / Tablets with internet access Power point presentation (download from the website) PowerPoint projector Headphones
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Working in pairs / Small groups  Media selection  Project based Learning (PBL)  Station Learning

Table 11 - Structure of the unit of competence 2.2. – Sharing through digital technologies of the Module 2 – Communication and collaboration.

### Sharing through Digital Technologies

Digital technologies are tools, systems, devices and resources that generate, store or process data. Some of the most common Digital Technologies include social media, online games, multimedia and mobile devices.

What is sharing with digital technologies?

According to the Digital competence Framework 2.0 it means to share data, information and digital contents with others through appropriate digital technologies as mentioned above.

<sup>11</sup> Materials and equipments.

## Digital Tools



**Programs:** Word, Paint , Notes



**Websites:** Google.com (Google drive)



**Online sources:** Podcasts, Videos, Social media

Let's see how someone can share a file on Google Drive...

### ***What is Google Drive?***

Google Drive is a file storage location developed by Google. It is an internet-based service available as a website and an app and allows to store files in the “cloud” and synchronize files across devices.

Now let's check it out!!

1. On your computer station go to drive.google.com
2. Sign in with your Google username and password
3. Upload the file we created earlier on Google Drive
4. Click the uploaded file and click share
5. Under “People” type the email address of your colleague
6. Click send

## Practical Activities

<b>Module</b>	2
<b>Unit</b>	2.2
<b>Duration</b>	2 – 3 hours
<b>Type of activity</b>	Practical Activity
<b>Objectives</b>	At the end of the activity learners will be able: <ul style="list-style-type: none"> <li>◆ Connecting with others through digital tools</li> <li>◆ Setting up shared folders on a specific platform</li> <li>◆ Using and editing a shared file</li> </ul>
<b>Setting<sup>12</sup></b>	For the development of this activity is needed: <ul style="list-style-type: none"> <li>◆ A Projector</li> <li>◆ Powerpoint slides (download presentation from the website)</li> <li>◆ Paper and pens</li> <li>◆ Mobile devices</li> <li>◆ Computers</li> </ul>
<b>Debriefing activity</b>	At the end of the activity learners need to think about: <ul style="list-style-type: none"> <li>◆ What it means to share through digital technologies.</li> <li>◆ What advantages does it bring? What disadvantages?</li> <li>◆ How have these tools changed information sharing in the past years?</li> </ul>

### Step 1: 10 min

The educator will introduce to learners the concept of sharing and will also provide them with its definition.

#### Debriefing activity

The educator will propose some debriefing questions:



What type of information do you usually share?

<sup>12</sup> Please identify the equipment, materials, documents and any support needed to perform this activity. In case you create a supporting document you can add it here as well.



How do you share this information?



Which digital tools or platforms could be used to share this information?

## Step 2: 30-40 min



The educator will introduce through PowerPoint slides simple digital tools such as Word, Notes or Paint to create content



The educator will ask learners on each of their computer stations to select one of the demonstrated apps to create specific content, either word based or picture based.



Once all learners have created their files, the educator will ask them to save locally on their computer station.



The educator will present the most common platforms to share content, Facebook, Instagram, mail, YouTube, Google Drive, Dropbox

## Step 3: 20 min



The educator will ask learners to open a specific digital tool such as Dropbox and guide them step by step in order to locate the file they created before and share through Dropbox with the rest of the learners



The educator will then ask learners to open a social media app such as Facebook and will ask learners to share their created file as a post

## Step 4: 10-20 min





The educator will present through slides simple steps on how to edit a shared file on Dropbox.



The educator will then ask learners to edit all files that were shared in the common folder of the Dropbox platform

## 2.3. Engaging in citizenship through digital technologies

This unit will introduce you to two main concepts:

-  Digital Citizenship
-  Cyber Security Awareness

We will focus on understanding how to identify cyber security risks, how to prevent them and resolve them.











Unit 2.3	Engaging in citizenship through digital technologies
Duration	5 hours
Objectives	 Understand the Digital Citizenship as well as Cyber Security Awareness concept  Identify cyber security risks  How to prevent cyber attacks
Content	2.3.1 Digital Citizenship 2.3.2 Basic concepts 2.3.3 Security and Privacy 2.3.4 Practical Activities
Resources	Computer stations and mobile devices with internet access Headphones Powerpoint Projector Power point presentation ( <b>download from the website</b> ) Black Board
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Simulation / Role plays  Media selection  Project based Learning (PBL)  Cooperative Learning  Flipped Classroom

Table 12 - Structure of the unit of competence 2.2. – Engaging in citizenship through digital technologies of the Module 2 – Communication and collaboration.



### 2.3.1 Digital Citizenship

Digital Citizenship refers to the behavior, the positive engagement individuals impose when entering the digital world. In more detail, a **Digital Citizen** is a person who has the knowledge and skills to effectively use digital technologies to communicate with others, participate in society and create and consume content through digital tools.

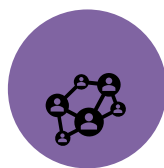
### 2.3.2 Basic Concepts



SAFETY



REPUTATION



RELATIONSHIPS



ETHICS

#### E-Safety

This concept has become a fundamental topic in the digital world and includes an individual's knowledge about Internet privacy and how an individual's behavior can contribute towards a healthy interaction with the use of the internet.

Common Dangers: Phishing, Malware, cyberbullying, accessing and posting private information.

#### Reputation



Moving along from  
the Age of  
Information to the  
Age of Reputation



Our digital reputation  
is how we are  
perceived online and  
is shaped and figured  
by the way an  
individual presents  
him/her self and the  
information other  
individuals post about  
them.



Digital Reputation is a  
concept that has  
shaped in such a way  
that has become more  
permanent than ever  
before since we as  
individuals have  
placed more trust in  
search results than  
any other source.

## Relationships

Digital relationships involve using technologies to develop a more interactive and relevant interaction between individuals.

These technologies can contribute both positively and negatively specifically in personal relationships depending on how individuals use technology and might create problems between partners potentially stirring conflict and dissatisfaction in the relationship.



OR



## Ethics

Digital Ethics is the study of how to manage oneself ethically professionally and in a manner via online and digital mediums.

Some examples of an Ethical behavior is when an individual:

1. Asks for permission to collect and store data about users
2. Asks for permission to sell any personal data that has been stored
3. Has been provided with the right to request that data about them to be deleted.
4. Has been provided with access to personal data that has been collected and stored

## Digital Footprints

Digital Footprints or Digital Trails are records of what an individual searches, visits, creates, shares, posts, installs through digital tools on a mobile device or on a computer station.

### *A good Citizen*

- Advocates for equal human rights
- Treats others with respect
- Does not steal or damage others' property
- Communicates clearly respectfully and with empathy
- Speaks honestly and does not repeat unsubstantiated rumors
- Protects self and others from harm
- Projects a positive self-image

### *A good Digital Citizen*

- Advocates for equal digital rights for all
- Seeks to understand all perspectives
- Respects digital privacy, intellectual property and other rights of people online
- Communicates and acts with empathy for others' humanity via digital channels
- Applies critical thinking to all online sources including fake news
- Is mindful of physical, emotional and mental health while using digital tools.
- Understands the permanence of the digital world and proactively manages digital identity.

## 2.3.3 Security and Privacy

**Security** - Numerous processes which protect an individual's personal information from other people. This can be achieved through different ways:

- VPN, Virtual Private Networks
- Antivirus programs
- Strong Passwords

**Privacy** – A person’s right to preserve and protect his/her identity and maintain a safe and protected space around one's integrity, physical presence, thoughts, feelings and intimate activities.




In the digital world Privacy must be seen as a crucially important right for individuals as a society and as a collective.

### 2.3.4 Practical Activities



<b>Module</b>	2
<b>Unit</b>	2.3
<b>Duration</b>	5 hours
<b>Type of activity</b>	Practical Activity
<b>Objectives</b>	At the end of the activity learners will be able: <ul style="list-style-type: none"> <li>◆ Understand the Digital Citizenship as well as Cyber Security Awareness concept</li> <li>◆ Identify cyber security risks</li> <li>◆ How to prevent cyber attacks</li> </ul>
<b>Setting<sup>13</sup></b>	For the development of this activity is needed: <ul style="list-style-type: none"> <li>◆ Computer stations and mobile devices with internet access</li> <li>◆ Headphones</li> <li>◆ Powerpoint Projector</li> <li>◆ Black Board</li> <li>◆ Chalk</li> </ul>
<b>Debriefing activity</b>	At the end of the activity learners need to think about: <ul style="list-style-type: none"> <li>◆ How people interact online.</li> <li>◆ As online, you have to be very careful how you communicate with others.</li> <li>◆ How to prevent cyber attacks</li> <li>◆ How to protect a computer station or a mobile device while surfing on the internet</li> <li>◆ How to filter information on the internet and shared content</li> </ul>

<sup>13</sup> Please identify the equipment, materials, documents and any support needed to perform this activity. In case you create a supporting document you can add it here as well.








## Step 1: 30-40 min

-  The educator will have an agenda slide to help keep the lesson on track and ensure learners will know and understand what to expect during the training
-  The educator will introduce the module to all learners through the PowerPoint slides and explain the concept of Digital Citizenship.
-  Ask learners using their stations to watch two issue-based videos that focus on why Digital Citizenship is important.




## Debriefing Activity

-  The educator will discuss with the learners what have they understood so far by the term Digital Citizenship
-  The educator will also discuss with the learners the threats and risks one comes across when not searching secure websites and how to manage social media related issues.

## Step 2: 60 min

-  The educator will introduce the basic concepts of Digital Citizenship
-  The educator will provide examples to learners and help them become internet alert
-  The educator will encourage learners to exchange ideas amongst them and demonstrate awareness of the dangers by providing case scenarios
-  The educator will illustrate the two case scenarios and will discuss the key points of each scenario
-  Once the two scenarios are elaborated the educator will then create on the blackboard a three-column chart with the terms “Safe”, “Responsible” and “Respectful” written at the top of each column.
-  Invite learners to provide words or phrases that describe how people can act safely, responsibly and respectful online and write them in the appropriate column
-  Have each of the learners use a piece of plastic and shred into pieces, explain what will this cause to the environment and link it to the digital footprint when ones is not acting in a safe, responsible and respectful manner.

## Step 3: 50 min

-  The educator will introduce the concept and definition of Digital trail and footprint
-  The educator will provide to all learners handouts to write down what they already know, what they want to know and what they have learned
-  The educator will ask two volunteers to take part in a role playing  
Say: “Imagine you are walking down a crowded street and a complete stranger approaches you and says you have just won a free trip—all you need to give him is your name, age, address, phone number, and passwords to your social network accounts (Google+, Facebook etc). Would you believe him?”

### Debriefing Activity

The educator will handout a post assessment which will be discussed amongst learners

#### Step 4: 45 min



The educator will begin by asking how important their privacy is to them or rate it from 1 to 5 and record information on the blackboard



The educator will then ask the learners who say it is unimportant to have their privacy and encourage the other learners to debate on the topic.



Using some examples provided from the debate discuss with all learners what do they understand by the term Security and Privacy



The educator will provide the definition of Privacy and Security and provide examples used on digital tools

At the end the educator will over cap what has been discussed in the unit and explain the rights everyone has as a digital citizen and ask the security and privacy settings of their social media accounts on their computer stations.

## 2.4. Collaborating through digital technologies





Unit 2.4	Collaborating through digital technologies
Duration	3 hours
Objectives	Teaching learners how to use digital tools to collaborate online with others.
Content	2.4.1 Collaborating through digital technologies – main concepts 2.4.2 Practical Activities
Resources	Blackboard Pieces of paper Pens Jar Computers
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Working in pairs / Small groups  Media selection

Table 13 - Structure of the unit of competence 2.5. – Collaborating through digital technologies of the Module 2 – Communication and collaboration.

### 2.4.1 Collaborating through digital technologies – main concepts

The aim of this unit is to teach students what it means to collaborate through digital technologies, to know the most common tools to collaborate online and to be able to identify the right tool for a particular need.

#### Definition of Collaborating through digital technologies:

According to the definition in the Digital Competence Framework 2.0, *collaborating through digital technologies* means: "to use digital tools and technologies for collaborative processes and for co-construction and co-creation of resources and knowledge".

#### Why is collaboration through digital technologies so important?

Nowadays we are more and more used to using digital technologies, in our private and working lives to interacting with others.

Exchanging documents, photos, information or using the online environment to organise work or study has become increasingly important, especially since the Covid 19 pandemic forced us to live, work and study at home. There are a number of tools that allow us to exchange information in the online environment, in a quick and easy way.



Especially in a work environment, it has become essential to be able to interact with colleagues or other people online, exchange documents and information and to be able to manage tasks, organise meetings etc. Digital tools will help us to manage work (not only remotely), speed up the exchange of information and increase team productivity.

### What are the most useful tools for collaborating in an online environment?

As already mentioned, there are many tools that help us to collaborate online with others. Below we would like to share and recommend some of them:

**Skype; GoToMeeting; Zoom Meetings; Google Meet; Microsoft Teams:** All these tools are Web Conferencing and Online Meeting Tools that allow people to organise meetings remotely or easily see each other when people are far away. You can also share your screen and show presentations and files to other participants.

**Google Drive; Dropbox:** With these apps, you can save files and store them in an online space, separate from your devices. This is useful because you can recover the file even if your devices have some problems, assuming you have archived them here. Furthermore, thanks to these tools you will be able to work and collaborate with other people by having the possibility to share your space or documents with colleagues, friends or family members or whoever you want.

**Google Calendar; Teamup:** These are apps designed as an agenda. They look like a calendar that you can organise and personalise. The interface is very simple in both and you can decide to display a single day, a week or even longer time intervals. You can mark your appointments, schedules meeting and even share them with other people.

**Trello; Redbooth; Asana:** These are project management tools that help in work activities. You can create lists, assign tasks to other members of your team who share the same space, set deadlines and customise everything as efficiently as possible.

**Google Form:** The google application allows you to create surveys freely and very easily. You can customise your surveys and use different ways of asking questions: multiple answers, open answers, satisfaction scores etc.

## 2.4.2 Practical Activities

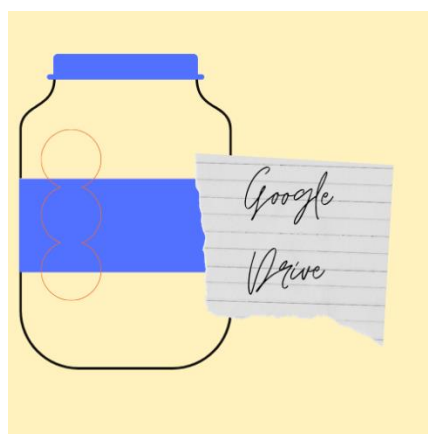
### Step 1: The jar of tools

The educator lists several tools that could be proposed to the learners.

All the tools we suggest are open-source digital tools. The educator can insert as many tools as he/she wants (at least one per student).






We suggest the following: Google Drive, Trello, Dropbox, Google Calendar Google Form etc.).

The educator writes the name of the tool on a piece of paper and inserts it in the jar.



At this point, it is the learners' turn: one at a time learners take a piece of paper in the jar and say aloud the name of the tool that they have found.

The educator proposes some questions to the student and the class:

-  What is this tool used for?
-  Have you ever used this tool?
-  Do you know how it works?
-  Do you know other tools that work in the same way?
-  Do you think this tool is useful to foster collaboration?

The educator will lead the discussion but will try to stimulate the conversation among the learners.

When all the notes in the jar are finished, the educator will write down on a blackboard all the names of the tools that have come out and explain better to the learners how they work.

At the end of the activity, the educator will propose some debriefing questions:



Do you know what it means to collaborate through digital technologies?



How can the tools we have seen help people collaborate faster and easier?

## Step 2: Let's try it!

This activity is more practical than the first one and serves to put into practice the more theoretical knowledge acquired during the first part.

The learners work in pairs.

The educator assigns them a tool to be tested among those mentioned in the first activity.

At this point, depending on the tool "received", the educator will ask learners to carry out small tasks.

The tasks can be many and different, and it depends on the tools the educator decides to present to his/her learners.

Creating a shared folder, sending a heavy file, setting up an online meeting and inviting some contacts etc.

The learners will try for 30 minutes a tool and they can rotate with others to allow everyone to try as many tools as possible.

At the end of the activity, the educator will propose some debriefing questions:



Did you find the tools you tried useful?



Did you already know them?



Do you think they are useful in the work context and beyond?



What would you use them for?

## 2.5. Netiquette



Unit 2.5	Netiquette
Duration	5 hours
Objectives	Teaching learners the correct behaviour that should be kept in an online environment.
Content	2.5.1 What does it mean <i>Netiquette</i> ? 2.5.2 Practical Activities
Resources	A blackboard; Chalk; Post it; Paper and pens Case study 1 Case study 2
Training methodologies	 Group exercise Discussion / Debate  Working in pairs / Small groups

Table 14 - Structure of the unit of competence 2.6. – Netiquette of the Module 2 – Communication and collaboration.

### 2.5.1 What does it mean *Netiquette*?

The aim of this unit is to teach learners to keep correct behaviour in the online environment. Respecting others and the places where we are is as important in the physical environment as in the online one. Teach these topics is very important, especially because online people become more aggressive or mean towards other people. There are many examples of phenomena linked to bad online behaviour, cyberbullying, body-shaming are just a few examples of behaviours that we witness on a daily basis on the web, not to mention episodes of racism and hate towards minorities in general. Education to respect others is essential to prevent such behaviour.

#### Definition of Netiquette

According to the definition in the Digital Competence Framework 2.0, *netiquette* means: “To be aware of behavioural norms and know-how while using digital technologies and interacting in digital environments. To adapt communication strategies to the specific audience and to be aware of cultural and generational diversity in digital environments”.

#### Which behaviours are considered a bad example of netiquette?

In general, we can consider as a bad example of netiquette all those online behaviours that are disrespectful towards others. These attitudes can be of various characters.

**Disrespecting intellectual property:** sharing content, photos, materials of others without citing the source is considered wrong and an example of bad netiquette (In addition to implying legal duties which we will not discuss here).

We should always check where we are getting this content and see if it is open source or if we have to cite the source when we use it.

**Not respecting other people's opinions:** not respecting other people's opinions and therefore adopting hostile and insulting attitudes towards these people is an example of bad netiquette. We should always try to establish a dialogue with others without using words or tones that are inappropriate or that may offend others.

**Expressing ourselves in a disrespectful way:** When writing a message, an email or a post we have to be aware of how we write and how we express ourselves and our ideas. Always remember that people on the other side do not see our expressions or hear our tone of voice and this can lead to misunderstandings. That is why it is important to be careful when expressing yourself online. Using ambiguous or hostile language, using capital letters, not signing, not contextualising the content of your message are just a few examples of bad netiquette. Remember also to use formal or informal language depending on the person you are dealing with, whether they are a friend, an acquaintance, a colleague or a stranger.

**Disrespecting the privacy of others:** Many people share a lot of photos or private information about themselves on social networks but be careful to always respect the privacy of others and never share sensitive data without the other person's permission.

## 2.5.2 Practical Activities

### Step 1: Which one doesn't belong?

The educator writes on a board different online behaviors having to do with netiquette, some positive examples, and some negative examples.

In this first activity, learners should find out which elements have nothing to do with the others in a group of good and bad examples of netiquette.

The purpose of the exercise is to identify the bad behaviors inside good ones.

Call one student at a time to the blackboard and ask them to circle bad examples of netiquette.

In the end, the educator will correct the answers given by the learners.

At the end of this activity, the educator invites learners to reflect on the behavior that people keep online. The educator will propose some debriefing questions:



What are the behaviors that make you uncomfortable online?



In the online environment, have you ever noticed the use of bad behavior by users?



Have you ever tried to explain to others what netiquette is?

#### Tips:

- This activity can also be done using post-it notes to hang on a wall.
- This activity can also be done online using a tool such as *jamboard* (<https://jamboard.google.com/>).



## Step 2: Keyboard warrior

For this exercise, the educator proposes to learners different texts in which people interact with each other online (i. e., chat, email, faq, comments etc.).

Two case studies can be used in this activity.



### Case study 1

#### An email exchange between two colleagues

Anna and Elisabeth are two colleagues who work in the same company. Anna works in the administrative sales department while Elisabeth manages the relationship with the client and the organization of events. Elisabeth ordered some flyers and posters to publicize the event, but there were delays in delivery.

**Object:** Summer Festival\_delivery delays

**Anna:**

Dear Elisabeth, I am writing to you with reference to the order of flyers and posters for the summer party you asked for. Unfortunately, due to the Covid 19 pandemic, our printmaker has informed us that there will be a delay in delivery.

I will let you know as soon as we receive the materials.

Sincerely,

Anna

**Elisabeth:**

Hi Anna. I understand that Covid has caused a lot of problems, but this is a very serious problem for the organisation of the festival. I'm the one who has to talk to the client, what should I tell him?

HOW DO I PROMOTE THE EVENT NOW?

The client wants the materials by the end of the week. NO EXCUSES.

CHANGE PRINTMAKER if necessary! DO YOU UNDERSTAND ME?

**Anna:**

Dear Elisabeth,

I am very sorry that this delay is causing problems with your work.



Unfortunately, we have already paid for the material in advance and we cannot get the money back at this point. Please try to explain the situation to your client, I am sure he will understand.

Confident of your cooperation,

I wish you a good day.

Sincerely,

Anna

---

**Elisabeth:**

I'll try to explain to him the situation and ask for more time, but I do not want to take responsibility for this problem, if necessary, I will give the number of the director of services.

THAT'S HOW I WILL MANAGE THIS PROBLEM.

Elisabeth

---

The educator invites learners to reflect on the text:



How does Anna appear? Does she have a nice attitude towards Elisabeth or not?



And Elisabeth to Anna?



What is Elisabeth's attitude towards the problem? Is she comprehensive to her colleague or not?




In the text, there are some examples of bad netiquette. Can you find out what they are?

After answering the educator's questions, the participants should try to rewrite the text transforming the behaviors from negative to positive.


## Case study 2

A girl (Lily) posts on her Facebook profile a photo after receiving her first dose of the vaccine against Covid 19:



**Lily88**  
Today at 11.00

I GOT MY COVID-19 VACCINE!  
#vaccinated #bye #corona #happy #staysafe



12

Adrien: Congratulations!  
Rose: That's awesome! ☺  
Ben: I'm scared of getting my vaccine😬  
Jessica: I will do it soon too! ☺☺

**Olly:** Maybe the vaccine will make your brain grow too!

R: Emily: People who don't want to be vaccinated are very intelligent... ☺☺

R: Olly: MY BODY, MY CHOICE!

R: Emily: Your choice not to take the vaccine is selfish! If everyone decided not to vaccinate, the situation would still be terrible.

R: Steven: People who don't vaccinate deserve to get sick!

**Billy:** I think everyone is free to choose for themselves ☺

R: Emily: Yes, but they should not attack people who have decided to be vaccinated!

R: Olly: I didn't attack anyone, I just expressed MY OPINION.









R: Emily: It is impossible to talk to a DONKEY!

R: Olly: Fxxk off Emily!

R: Billy: Please, I don't think we should argue about this. There are many people who have different opinions. Let's try to respect each other!

R: Thank you Billy. I agree with you. I am very happy to have received my dose of vaccine, but I don't expect everyone to understand. Everyone is free to do as they want ☺  
Peace & Love ☺

The educator invites learners to reflect on the text:

-  What do you think is bad netiquette in these comments?
-  How would you have reacted to Olly's comment?
-  Do you think Emily answered to Billy properly?
-  Who do you think acted appropriately in these comments?
-  Can you find bad and good examples of netiquette in the text?
-  Why do you think it is easier to be mean online?
-  Have you ever been a keyboard warrior?
-  What do you do when you recognize that someone is using mean behavior online?

After answering the educator's questions, the participants should try to rewrite the text transforming the behaviors from negative to positive.



### Step 3: The Netiquette Manifesto

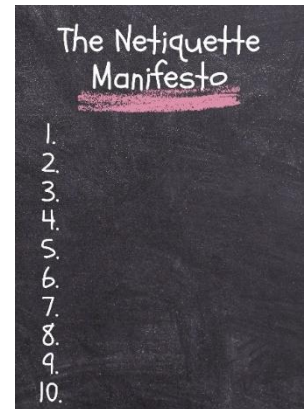
In the last activity, the educator goes to the blackboard and asks the learners to write together the “Netiquette manifesto”, i.e., all the positive behaviors they think should be kept online.

The learners should discuss what are the main rules and then list about ten examples of good netiquette.

This is the “Netiquette Manifesto” of the class, and everyone must commit to respect it.

Once the manifesto has been decided, the educator could explain to the learners a brief explanation of the netiquette's theory.

At the end of the activity the educator invites learners to carefully reflect the way in which people should interact online and how learners would like to spread and teach to others the rules that they have written (using social media? Sharing the manifesto? Etc.)



## 2.6. Managing digital identity





Unit 2.6	Managing digital identity
Duration	4 hours
Objectives	 Teaching learners what it means to have a digital identity and how they should take care of it.
Content	2.6.1 Definitions and protecting identity 2.6.2 Practical Activities
Resources	Paper and pens Computers
Training methodologies	 Group exercise Discussion / Debate  Working in pairs / Small groups  Simulation / Role plays

Table 15 - Structure of the unit of competence 2.7. – Managing digital identity of the Module 2 – Communication and collaboration.

### 2.6.1 Definitions and protecting identity

This module aims to make learners aware of all the information we leave online about ourselves and which represents our digital identity. Digital identity is something that relates to us, to our person. For example, when we use an ID and password to authenticate ourselves on a website, we are using our digital identity. Nowadays, we live in a world where more and more services require us to log in from devices, both private and public. E-commerce, banking, health services, tax services are just a few examples. Every time we register our digital identity or do certain actions online, our private data are taken and recorded, often without the user even realising it. This is why we need to be aware and learn how to best manage our digital identity online.

#### Definition of managing digital identity

According to the definition in the Digital Competence Framework 2.0, *managing digital identity means*: “To create and manage one or multiple digital identities, to be able to protect one's own reputation, to deal with the data that one produces through several digital tools, environments and services”.

#### Why do we have to worry about our data?

Every time we consent to privacy in order to access a site, download an app, answer surveys on social media or enter some site using our information, we are generating data. This data is relevant to many companies because it reveals consumer behaviour. We often give away our data or consent to its use without even being aware of it.

But online we do not just leave traces of what we like and do not like as consumers, we also leave very important private information that if used by others can be very damaging to us. Just think of our credit card details or our social accounts with photos and personal information.

### Identity theft

When our digital identity is hacked and our personal or financial data are stolen, we can speak of cybercriminals. They are people who specialise in online theft. They hack into our systems or use tricks to make us believe that they can give us our data on secure sites or apps, when in fact they are stealing it from us.

Impersonating you, these criminals steal your money and information. For example, some influencers (very famous people on social media) have announced having their identity stolen by a hacker, who stole their social media accounts and demanded a ransom to give them back.

### How to defend ourselves against cybercriminals?

First with awareness. Knowing how cybercriminals operate and how they can steal your digital identity is a factor key to preventing them.

Then you have to be very careful. For example, never open suspicious e-mails or messages that reach us. Often these cyber criminals pretend to be organisations that we have a service with (e.g., a bank), so we need to be able to recognise whether the information we receive may or may not be true. Is it written correctly in your language? Are there any strange signs? Does it talk about operations of which you are not aware? If you have the slightest suspicion, do not click, or download or touch anything. If it is your bank, for example, call your branch and ask for an explanation. Never click on suspicious links.

This phenomenon is called phishing attack and is really dangerous for the individuals who are affected by it.

### What are some ways to protect our digital identity?

- **Use two-factor authentication:** Authentication of your identity is not only done through one step (e.g. password), but also through additional steps such as entering a code or authorisation via the telephone.
- **Change and diversify passwords:** Do not use the same passwords for all your accounts and try to change them often.
- **Avoid sharing sensitive information:** be careful about the kind of data you share and try to share only the essentials online, such as your home address (be careful of geolocation on photos you post on social networks!).

## The rights of a Digital Citizen

- Digital Citizenship according to the Council of Europe refers to the ability to engage positively, critically and competently in the digital environment drawing on the skills of effective communication and creation, however it also refers to the ability a citizen applies when participating in a respectful manner towards human rights and dignity through the responsible use of technology.
- A digital citizen is entitled to enjoy the rights of Privacy, Security, Access and Inclusion and Freedom of expression. However, as a citizen with these rights the digital citizen has certain responsibilities such as ethics and empathy and other responsibilities to guarantee a safe and responsible digital environment for all digital citizens.

## 2.6.2 Practical Activities

### Step 1: The private-eye game

Imagine that you are talking to a friend who tells you that she has met a classmate of yours from high school.

You are curious to know more about that person with whom you were so close when you were a teenager.

Try joining his first and last name on the internet and then expand the research (you can also do the research on yourself or on a person you know).



What did you find out about that person?



Which tools did you use to help you in your research?



Which platforms did you consult?



Try to answer the following questions:

- What city does he/she live in?
- Are he/she married?
- What did he/she study?
- What is his/her job?

At the end of the activity, the educator invites learners to carefully reflect on what information we share online.

### Step 2: How secure is your password?

In this activity, the educator wants to teach learners the importance of having a secure password on their accounts.

The educator asks learners to imagine having to prepare passwords for one of the following person:

Helen Smith	Alejandro Garcia	María Ivanov
<ul style="list-style-type: none"> <li>• Born: 25th June 1988</li> <li>• Live in: Los Angeles (USA)</li> <li>• Married</li> <li>• She has got a dog named Oliver</li> </ul>	<ul style="list-style-type: none"> <li>• Born: 11th March 1965</li> <li>• Live in: Madrid (Spain)</li> <li>• Single</li> <li>• He loves motorbikes</li> </ul>	<ul style="list-style-type: none"> <li>• Born: 1<sup>st</sup> December 1952</li> <li>• Live in: Sofia (Bulgaria)</li> <li>• Married</li> <li>• She has three children</li> </ul>

Figure 11 – Profiles to be considered to prepare passwords.



**Try to write the different password for each person playing with words (at least 5).** Think of a different password depending on the account you need to create it for (e.i., bank; Facebook; private email; work email, e-commerce etc.).



Now test the security level of your password online (there are several platforms that you can use for example <https://howsecureismypassword.net/>).

At the end of the activity, the educator invites learners to carefully reflect how to create a good password to guarantee a security level online.

The educator will propose some debriefing questions:



How do you create your passwords? Do you always use the same one for all sites or do you have different ones?



Do you think there are sites where you need a higher level of password security than others?



What tricks should be used to create secure online passwords?



How often should passwords be changed?



Do you know how identity thieves can steal your passwords?

**Congratulations, you have now completed Module 2.**

**Do not forget to check the Annexes for additional resources and documents provided to support self-study!**

## Module 3: Content creation

Module 3 focuses on **Content Creation** for the digitally competent citizen. We aim to create a shared understanding of what it means to be a digitally competent citizen as well as developing and testing materials which create a clear pathway to upskilling yourself in the main relevant digital areas.

Within this module we will cover:

- Developing Digital Content- To create and edit digital content in different formats, to express oneself through digital means.
- Integrating and re-elaborating digital content - To modify, refine, improve and integrate information and content into an existing body of knowledge to create new, original and relevant content and knowledge.
- Copyright and licenses- To understand how copyright and licences apply to data, information and digital content
- Programming - To plan and develop a sequence of understandable instructions for a computing system to solve a given problem or perform a specific task.

We will outline how you can create and edit digital content to improve and integrate your information into an existing body of materials, while also highlighting the important issues around copyrighting and licensing in the digital sphere. We will also briefly touch on the programming aspects of how to utilise computer systems.

Please note that practical activities described in each unit might entail the support of an experienced trainer. Although the information presented in the manual is written in a way that is easy to understand, some actions, adjacent to the information presented, may require the support of experienced people.



Module 3 Content creation				
Duration	10 hours			
Objectives	To understand the nuances and elaborate on your content creation skills			
Units	3.1.Developing digital content	3.2 Integrating and re-elaborating digital content	3.3 Copyright and licenses	3.4 Programming
Training organization	E-Learning	E-Learning	E-Learning	E-Learning
Duration	2.5 hrs	2.5 hrs	2.5 hrs	2.5 hrs

Table 16 - Global structure of the Module 3 – Content Creation.

Note: Module 3 practical activities are presented in Power Point slides, which you can download from the resources section of the project website.

### 3.1 Developing digital content



Unit 3.1 Developing digital content	
Duration	2.5 hours
Objectives	Increased knowledge of Mojo equipment, practical ways to film as well as understanding of positioning, light and angles. Overview of Facebook live, Mobile apps for developing digital content. Finally an insight into computer editing programmes for your digital content
Content	Autonomous, flexible resources which can be used on the go- E-Learning
Resources	PC/ mobile or tablet for e-learning Power point presentation ( <b>download from the website</b> )
Training methodologies	 Presentation by trainer  Flipped Classroom

Table 17 - Structure of the unit of competence 3.1.- Developing digital content of the Module 3 – Content Creation.



## 3.1 Developing digital content

### 5 Types of Digital content

#### *Bloggng*

Blog posts are a basic way of creating engaging content for your users online! Just like the old-fashioned newspaper lots of people love to sit down and enjoy a well written, insightful blog piece or article. You can share lots of information in a non-formal setting, introducing yourself to your readers and creating a rapport with them and hooking them in to come back for more! It can be time consuming to maintain a successful blog so it is recommended that you create a bank of materials before you kick it all off. Come up with some ideas for your first 2- 3 months of blog post content, as well as implementing a schedule for upload to keep your readers engaged, this will help you to be a regular and consistent poster!

Inspired to start your own blog- find more information here:

[https://www.wix.com/blog/2021/02/how-to-start-a-blog/?utm\\_source=google&utm\\_medium=cpc&utm\\_campaign=9852964004^122617225367&experiment\\_id=b^504114447774^^\\_DSA&gclid=CjwKCAjwh5qLBhALEiwAiods-cylXXhYEWcT\\_ZrqTbAelxQDqSkTV\\_pdKfnoxlptSsbyl02lw87MxoC6dwQAvD\\_BwE](https://www.wix.com/blog/2021/02/how-to-start-a-blog/?utm_source=google&utm_medium=cpc&utm_campaign=9852964004^122617225367&experiment_id=b^504114447774^^_DSA&gclid=CjwKCAjwh5qLBhALEiwAiods-cylXXhYEWcT_ZrqTbAelxQDqSkTV_pdKfnoxlptSsbyl02lw87MxoC6dwQAvD_BwE)

#### *Longform content*

In the instantaneous world we live in today longform content can be a bit of a gamble. Most people like to receive their information in short and sweet, bite sized chunks, however the definition of longform is adapting to reflect this. Some people define longform content as articles longer than 700 words, while others think it must exceed 1800 words. These types of long form content articles can appeal to your avid readers, it engages them and provides them with an escape which they crave.

This type of content can work particularly well because of the focus on the Search Engine Optimisation, including key word optimisation. By pinpointing the words you use often and which will be of interest to your target audience you can ensure that you content lands on their screen! Be smart and savvy with your content and this can work exceptionally well.

Tips for making your content readable and valuable- <https://medium.com/swlh/10-tips-to-make-long-form-content-readable-and-valuable-5b6e117965ae>

### *Infographics*

Eye catching, Engaging and Easy to create! Infographics are up there with the most used digital content in the online sphere, the reason for this being that they catch the eye of the user and draw them in, wanting to know more. They can be really engaging, providing high quality imagery, lots of information in a quick snapshot. In addition to this they are super easy to make!

You can use tools such as Canva or even Microsoft PowerPoint to create beautiful branded imagery with brevity, to share with your audience. Don't be afraid to share these on your social media for event more impact!

Click here to try out Canva- <https://www.canva.com/>

### *Podcasts*

In the past five years the prevalence of podcasts has increased tenfold. If you're sitting around the lunch table today just ask around for who listens to podcast content and we can guarantee you will have at least a 50% positive feedback rate! Podcasts are the new and innovative way to intake information of all kinds. From true crime, to comedy, to natural history if you have a weird or whacky interest chances are there is already a podcast which covers it in detail!

This type of content allows people to absorb digital content even while they are on the go, for example out for a run or while on your morning commute you can easily pop in a podcast, still concentrate on the task at hand with a helpful dose of entertainment or education.

Click here for a how to get started with your podcast - <https://www.thepodcasthost.com/planning/how-to-start-a-podcast/>

### *Finally, **Video!***

Video is **KING** of digital content, in today's visual society video is the ideal way to get in touch with your audience in a way that will make a huge impact! It is estimated that YouTube has over 2 billion active users MONTHLY. If you are going to choose a digital content to commit your time and resources to let it be video creation. Video content is highly diverse, adaptive and can be captivating to the user, we all know the feeling of scrolling through social media past long winded posts, pictures and having our eye caught by a beautifully crafted video with immersive imagery, music and messages.

Video marketing is an instant crowd pleaser, YouTube generated \$19.7 billion revenue as of January 2021.<sup>14</sup> And TikTok has taken over from Facebook, Instagram and Snapchat as the most popular social media platform. Short introductory or explainer videos can be much more effective in engaging your users, taking up a little of their time but leaving them with lots of information in return!

Within this module we will discuss further how to film your video content, utilising the best positioning, lighting and angles as well as the mobile apps which can make your life easier when creating high quality video marketing content!

### 3.2 Integrating and re-elaborating digital content



Unit 3.2	Integrating and re-elaborating digital content
Duration	2.5 hours
Objectives	Presentation of typical forms of the content creation and its storage. Indication of what are the ways to publish and maintain content on the internet.
Content	Power point resources ( <b>download from the website</b> ) Autonomous, flexible resources which can be used on the go- E-Learning
Resources	PC/ mobile or tablet for e-learning
Training methodologies	 Presentation by trainer  Presentation by participants

Table 18 Structure of the unit of competence 3.2. – Integrating and re-elaborating digital content of the Module 3 – Content Creation.

### 3.2 Integrating and re-elaborating digital content

*Content Creation and Integration.* To modify, refine and integrate new information and content into an existing body of knowledge and resources to create new, original and relevant content and knowledge.

We have touched on the creation of highly engaging content for your audience, taking into account the context of your use. Who are you trying to reach? Use your strengths to reach your target group, carry out some market research to ensure you are making the right choice for you! We will also cover the publication and

<sup>14</sup> <https://www.globalmediainsight.com/blog/youtube-users-statistics/>

storage of content online. Within integrating your content into already existing resources we will show you how to use productivity software and apps to achieve this in an efficient and useful manner! Using tools which already exist means that you will expend less capital and energy, while still achieving the end goal which is to create content which is highly engaging, meets your needs and the needs of your target audience!

As we have touched on before YouTube has a massive bank of materials, publicly available which can be extremely useful, Podcast content is also freely available and can help to supplement the resources which you are creating.

Throughout 3.2 you will be introduced to a host of useful tools which will make your content integration and elaboration journey much more exciting and seamless.

- One Note
- Evernote
- Draw.io
- PIXLR
- Adobe Spark
- Google Docs

### *Storing your Content*

When you have spent your time and energy created and integrating your digital content it is vitally important that you have the skills and knowledge of where is safest to save this content for ease of access but also security.

Cloud file sharing can be a useful platform which provides users the ability to access their content from any device, this flexibility means that you are not tied to a physical PC and is of the utmost importance in a dynamic and every changing workspace. Discover Dropbox, Google Drive and One Drive and change the way you share your materials.

## Publication and sharing

Sharing your creations online is process of publishing content onto online platforms, be it a YouTube channel, your own personal website & blog page or your social media account. Published content may include text, images, videos and other type of digital media.

Publishing online can be low cost, highly effective and efficient for your use, so we can help you to find the best tools to publish. Learn more about WIX, Wordpress, Linkedin & Pinterest.

### 3.3 Copyright and licenses



Unit 3.3	Copyright and licenses
Duration	2.5hrs
Objectives	Copyright is a type of intellectual property rights (IPR) that provides protection over something: <ul style="list-style-type: none"> <li> you might create</li> <li> owned by one or more people or businesses</li> </ul>
Content	Autonomous, flexible resources which can be used on the go- E-Learning
Resources	Power point resources (download from the website) PC/ mobile or tablet for e-learning
Training methodologies	Presentation by trainer

Table 19 - Structure of the unit of competence 3.3.- Copyright and licenses of the Module 3 – Content Creation.

### 3.3 Copyright and licenses

*What is copyright?*

Copyright ownership gives the owner the exclusive right to use the work, with some exceptions. When a person creates an original work, fixed in a tangible medium, he or she automatically owns copyright to the work.

Many types of works are eligible for copyright protection, for example:

- Audiovisual works, such as TV programmes, films and online videos
- Sound recordings and musical compositions
- Written works, such as lectures, articles, books and musical compositions
- Visual works, such as paintings, posters and advertisements
- Video games and computer software
- Dramatic works, such as plays and musicals

*Is it possible to use a copyright-protected work without infringing?*

Yes, in some circumstances, it is possible to use a copyright-protected work without infringing the owner's copyright. Some content creators choose to make their work available for reuse with certain requirements. For more about this, you may wish to learn about the Creative Commons license.<sup>15</sup>

#### *Copyright Law of the European Union*

The copyright law of the European Union is the copyright law applicable within the European Union. Copyright law is largely harmonized in the Union, although country to country differences exist. The body of law was implemented in the EU through a number of directives, which the member states need to enact into their national law. The main copyright directives are the Copyright Term Directive, the Information Society Directive and the Directive on Copyright in the Digital Single Market.<sup>16</sup>

The EU copyright law consists of 11 directives and 2 regulations, harmonising the essential rights of authors, performers, producers and broadcasters. By setting harmonised standards, EU copyright law reduces national discrepancies, and guarantees the level of protection needed to foster creativity and investment in creativity. Harmonised standards promote cultural diversity and bring better access for consumers and business to digital content and services across Europe.<sup>17</sup>

Within 3.3 we will delve deeper into the requirements of copyright, how to utilise a creative commons licenses and how these types of licenses can be useful to your content!

<sup>15</sup> <https://support.google.com/legal/answer/3463239?hl=en-GB>

<sup>16</sup> [https://en.wikipedia.org/wiki/Copyright\\_law\\_of\\_the\\_European\\_Union](https://en.wikipedia.org/wiki/Copyright_law_of_the_European_Union)

<sup>17</sup> <https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation>

### 3.4 Programming



Unit 3.4	Programming
Duration	2.5 hours
Objectives	The objective of this module is to get an understanding of basic structures of Python language.
Content	Autonomous, flexible resources which can be used on the go- E-Learning
Resources	Power point resources ( <b>download from the website</b> ) PC/ mobile or tablet for e-learning
Training methodologies	 Presentation by trainer  Flipped Classroom

Table 20 - Structure of the unit of competence 3.4. - Programming of the Module 3 – Content Creation.

### 3.4 Programming and coding basics

*What is programming at a basic level?*

Coding is a basic literacy in the digital age, and it is important for each person to understand and be able to simple coding and use technology around them. There are many different coding languages. We chose Python. Python is a simple and easy to learn because of its clear syntax and readability.

Python is an easy to learn, powerful programming language.

Python is a programming language that is easy to learn and powerful in operation. While writing the code, you will be mainly focused on solving the problem, not on the syntax and structure of the language in which you program.



## Python Variables

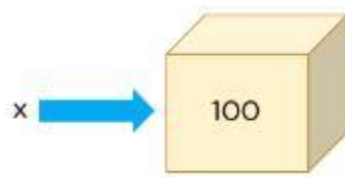
### 1. Variable Assignment

A Variable is a fundamental concept in any programming language. It is a reserved memory location that stores and manipulates data. Think of a variable as a name attached to a particular object. In Python, variables need not be declared or defined in advance, as is the case in many other programming languages. To create a variable, you just assign it a value and then start using it. Assignment is done with a single equals sign (=):

Variables are entities of a program that holds a value. Here is an example of a variable:

```
x=100
```

In the below diagram, the box holds a value of 100 and is named as x. Therefore, the variable is x, and the data it holds is the value.



The data type for a variable is the type of data it holds. <sup>18</sup>

In the above example, x is holding 100, which is a number, and the data type of x is a number.

In Python, there are three types of numbers: Integer, Float, and Complex.

Integers are numbers without decimal points. Floats are numbers with decimal points. Complex numbers have real parts and imaginary parts.

Another data type that is very different from a number is called a string, which is a collection of characters.

Let's see a variable with an integer data type:

---

<sup>18</sup> <https://www.simplilearn.com/tutorials/python-tutorial/python-variables>

```
x=100
```

To check the data type of x, use the type() function:

```
type(x)
```

```
x=100
type(x)
int
```

Python allows you to assign variables while performing arithmetic operations.

```
x=654*6734
```

```
type(x)
```

```
x=654*6734
type(x)
int
```

To display the output of the variable, use the print() function.

```
print(x) #It gives the product of the two numbers
```

Now, let's see an example of a floating-point number:

```
x=3.14
```

```
print(x)
```

```
type(x) #Here the type the variable is float
```

```
x=3.14
print(x)
3.14
type(x)
float
```

Strings are declared within a single or double quote.

```
x='Simplilearn'
```

```
print(x)
```

```
x="Simplilearn."
```

```
print(x)
```

```
type(x)
```

```
x='Simplilearn'
print(x)
Simplilearn
x="Simplilearn"
print(x)
Simplilearn
type(x)
str
```

To learn more we have linked an interesting page with excellent infographics:

<https://realpython.com/python-variables/>

**Congratulations, you have now completed Module 3.**

**Do not forget to check the Annexes for additional resources and documents  
provided to support self-study!**

## Module 4: Safety

Module 4 is focused on safety online and aims at bringing your attention to this issue alongside giving you information on how to reduce risks and keep your safety.

Please note that practical activities described in each unit might entail the support of an experienced trainer. Although the information presented in the manual is written in a way that is easy to understand, some actions, adjacent to the information presented, may require the support of experienced people.

Module 4	Safety			
Duration	25h			
Objectives	Within this unit, the participant will be trained to: <ul style="list-style-type: none"> <li>to protect devices, content, personal data and privacy in digital environments;</li> <li>to protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion;</li> <li>to be aware of the environmental impact of digital technologies and their use.</li> </ul>			
Units	4.1 Protecting devices	4.2 Protecting personal data and privacy	4.3 Protecting health and well-being	4.4 Protecting the environment
Training organization	Face-to-face E-Learning B-learning	Face-to-face E-Learning B-learning	Face-to-face E-Learning B-learning	Face-to-face E-Learning B-learning
Duration	6h	9h	5h	5h

Table 21 - Global structure of the Module 4 – Safety.

## 4.1 Protecting devices










Unit 4.1 Protecting devices	
Duration	6h
Objectives	 To understand that a computer is prone to network cyber attacks  To know how to set up a strong password  To be able to install a Chrome internet browser and update it periodically  To understand the effort that the human eye makes to read information from electronic devices  Understand that an incorrect working position can lead to medical problems with the spine  To understand the operating costs of the equipment  To understand that physical electronic components are not "environmentally friendly"
Content	4.1.1 Protecting devices 4.1.2 Software updates 4.1.3. Security and passwords 4.1.4 Increasing security 4.1.5 What is a malicious code? 4.1.6 Practical activities
Resources	Training manual Computer with internet access Editing programme Papers Pens
Training methodologies	 Presentation by trainer  Media selection

Table 22 - Structure of the unit of competence 4.1. – Protecting devices of the Module 4 – Safety.

### 4.1.1 Protecting devices

#### Why is computer security important?

Because computers play such critical roles in our lives, and because we input and view so much personally identifiable information on them, it is imperative to implement and maintain computer security. Strong computer security ensures safe processing and storage of our information.

#### How can I improve my computer's security?

The following are important steps you should consider to make your computer more secure. While no individual step will eliminate all risk, when used together, these defense-in-depth practices will strengthen your computer's security and help minimize threats.

### ➤ **Secure your home network**

When you connect a computer to the internet, it is also connected to millions of other computers—a connection that could allow attackers access to your computer. Although cable modems, digital subscriber lines (DSLs), and internet service providers (ISPs) have some level of security monitoring, it's crucial to secure your router—the first securable device that receives information from the internet. Be sure to secure it before you connect to the internet to strengthen your computer's security.

What is home network security and why should I care?

### ➤ **Home network security**

Home network security refers to the protection of a network that connects devices—such as routers, computers, smartphones, home appliances, Wi-Fi-enabled baby monitors, cameras—to each other and to the internet within a home.

Many home users share two common misconceptions about the security of their networks:

- Their home network is too small to be at risk of a cyberattack.
- Their devices are “secure enough” right out of the box.

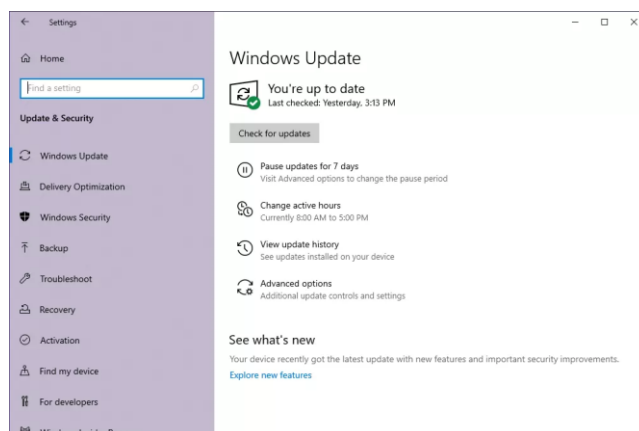
Most attacks are not personal in nature and can occur on any type of network—big or small, home or business. If a network connects to the internet, it is inherently more vulnerable and susceptible to outside threats.

How do I improve the security of my home network?

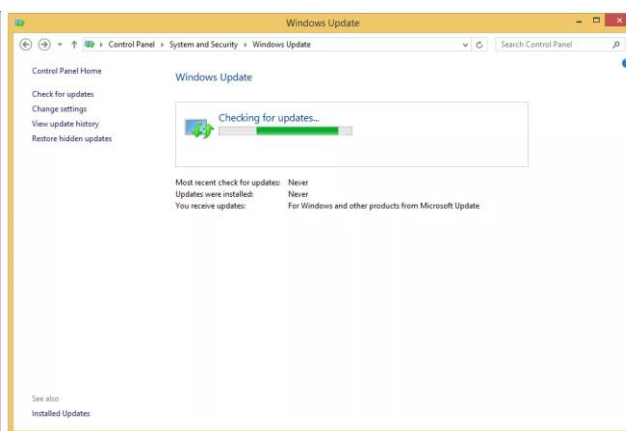
By following some of the simple but effective mitigation techniques below, you can significantly reduce the attack surface of your home network and make it more difficult for a malicious cyber actor to launch a successful attack.

### ➤ **Update your software regularly**

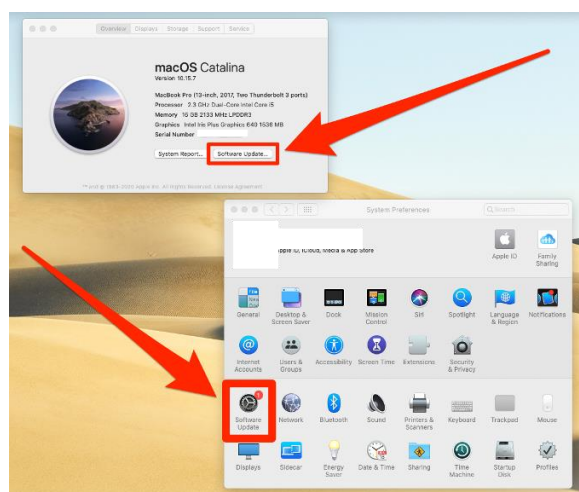
Regular software updates are one of the most effective steps you can take to improve the overall cybersecurity posture of your home networks and systems. Besides adding new features and functionality, software updates often include critical patches and security fixes for newly discovered threats and vulnerabilities. Most modern software applications will automatically check for newly released updates. If automated updates are not available, consider purchasing a software program that identifies and centrally manages all installed software updates.



Windows 10



Windows 8,7, Vista



MacOS update



Ubuntu (Linux) update

## What are patches?

Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features.

### 4.1.2 Software updates

#### How do you find out what software updates you need to install?

When software updates become available, vendors usually put them on their websites for users to download. Install updates as soon as possible to protect your computer, phone, or other digital device against attackers who would take advantage of system vulnerabilities. Attackers may target vulnerabilities for months or even years after updates are available.

Some software will automatically check for updates, and many vendors offer users the option to receive updates automatically. If automatic options are available, you can take advantage of them. If they are not available, periodically check your vendor's websites for updates.

Make sure that you only download software updates from trusted vendor websites. Do not trust a link in an email message—attackers have used email messages to direct users to websites hosting malicious files disguised as legitimate updates. Users should also be suspicious of email messages that claim to have a software update file attached—these attachments may contain malware.

If possible, only apply automatic updates from trusted network locations (e.g., home, work). Avoid updating software (automatically or manually) while connected to untrusted networks (e.g., airport, hotel, coffee shop). If updates must be installed over an untrusted network, use a Virtual Private Network connection to a trusted network and apply updates.

#### What is the difference between manual and automatic updates?

Users can install updates manually or elect for their software programs to update automatically.

Manual updates require the user or administrator to visit the vendor's website to download and install software files.






Automatic updates require user or administrator consent when installing or configuring the software. Once you consent to automatic updates, software updates are “pushed” (or installed) to your system automatically.

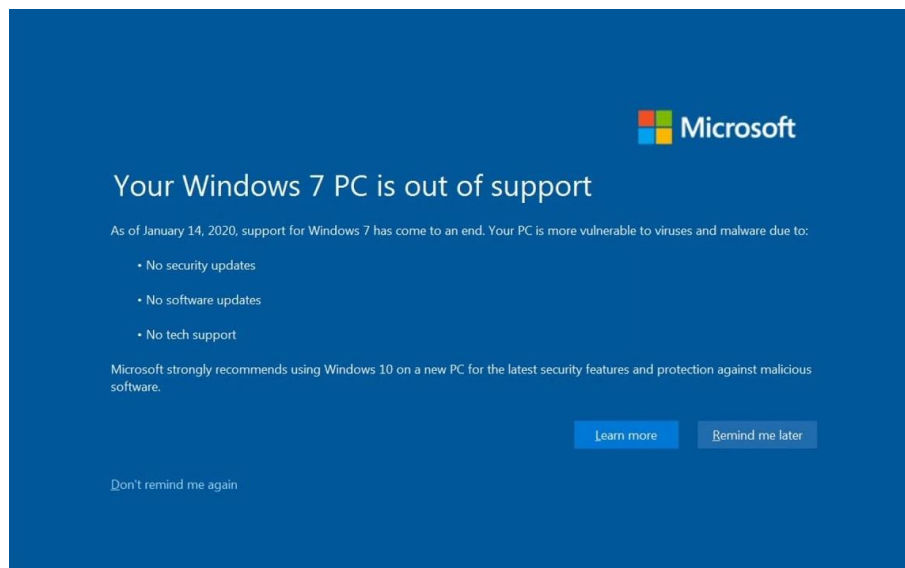
#### What is end-of-life software?

Sometimes vendors will discontinue support for a software program or issue software updates for it (also known as end-of-life [EOL] software). Continued use of EOL software poses consequential risk to your system that can allow an attacker to exploit security vulnerabilities. The use of unsupported software can also cause software compatibility issues as well as decreased system performance and productivity.



## Best Practices for Software Updates

-  Enable automatic software updates whenever possible. This will ensure that software updates are installed as quickly as possible.
-  Do not use unsupported EOL software.
-  Always visit vendor sites directly rather than clicking on advertisements or email links.
-  Avoid software updates while using untrusted networks.
-  New vulnerabilities are continually emerging, but the best defense against attackers exploiting patched vulnerabilities is simple: keep your software up to date. This is the most effective measure you can take to protect your computer, phone, and other digital devices.



Windows 7 EOL

## Remove unnecessary services and software

Disable all unnecessary services to reduce the attack surface of your network and devices, including your router. Unused or unwanted services and software can create security holes on a device's system, which could lead to an increased attack surface of your network environment. This is especially true with new computer systems on which vendors will often pre-install a large number of trial software and applications—referred to as “bloatware”—that users may not find useful.

## **Adjust factory-default configurations on software and hardware**

Many software and hardware products come “out of the box” with overly permissive factory-default configurations intended to make them user-friendly and reduce the troubleshooting time for customer service. Unfortunately, these default configurations are not geared towards security. Leaving them enabled after the installation may create more avenues for an attacker to exploit. Users should take steps to harden the default configuration parameters to reduce vulnerabilities and protect against intrusions.

### **4.1.3 Security and passwords**

#### **Change default log-in passwords and usernames**

Most network devices are pre-configured with default administrator passwords to simplify setup. These default credentials are not secure—they may be readily available on the internet, or may even be physically labeled on the device itself. Leaving these unchanged creates opportunities for malicious cyber actors to gain unauthorized access to information, install malicious software, and cause other problems.

#### **Use strong and unique passwords**

Choose strong passwords to help secure your devices. Additionally, do not use the same password with multiple accounts. This way, if one of your accounts is compromised, the attacker will not be able to breach any other of your accounts.

#### **Why you need strong passwords?**

You probably use personal identification numbers (PINs), passwords, or passphrases every day: from getting money from the ATM or using your debit card in a store, to logging in to your email or into an online retailer. Tracking all of the number, letter, and word combinations may be frustrating, but these protections are important because hackers represent a real threat to your information. Often, an attack is not specifically about your account, but about using the access to your information to launch a larger attack.

One of the best ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that those requesting access are the people they claim to be is the next step. This authentication process is more important and more difficult in the cyber world. Passwords are the most common means of authentication, but only work if they are complex and confidential. Many systems and services have

been successfully breached because of non-secure and inadequate passwords. Once a system is compromised, it is open to exploitation by other unwanted sources.

### Avoid common mistakes

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to crack them. Consider a four-digit PIN. Is yours a combination of the month, day, or year of your birthday? Does it contain your address or phone number? Think about how easy it is to find someone's birthday or similar information. What about your email password—is it a word that can be found in the dictionary? If so, it may be susceptible to dictionary attacks, which attempt to guess passwords based on common words or phrases.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "l!Tpbb" for "[l] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Changing the same example used above to "l!2pBb." creates a password very different from any dictionary word.

### Length and complexity

You should consider using the longest password or passphrase permissible (8–64 characters) when you can. For example, "Pattern2baseball#4mYmiemale!" would be a strong password because it has 28 characters and includes the upper and lowercase letters, numbers, and special characters. You may need to try different variations of a passphrase—for example, some applications limit the length of passwords and some do not accept spaces or certain special characters. Avoid common phrases, famous quotations, and song lyrics.

Password

.....

☐ *show password*

Password must contain numbers

Password must contain uppercase letters

Password must have at least one special characters

Length must be greater than 8 characters

Password should not contain strings

Password must not contain repetitions

## Dos and don'ts

Once you have come up with a strong, memorable password it is tempting to reuse it—don't! Reusing a password, even a strong one, endangers your accounts just as much as using a weak password. If attackers guess your password, they would have access to your other accounts with the same password. Use the following techniques to develop unique passwords for each of your accounts:



Use different passwords on different systems and accounts.



Use the longest password or passphrase permissible by each password system.



Develop mnemonics to remember complex passwords.



Consider using a password manager program to keep track of your passwords. (See more information below.)



Do not use passwords that are based on personal information that can be easily accessed or guessed.



Do not use words that can be found in any dictionary of any language.

## How to protect your passwords

After choosing a password that is easy to remember but difficult for others to guess, do not write it down and leave it somewhere where others can find it. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, makes it easily accessible for someone with physical access to your office. Do not tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords.

Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password. If you use a password manager, remember to use a strong master password.

Password problems can stem from your web browsers' ability to save passwords and your online sessions in memory. Depending on your web browsers' settings, anyone with access to your computer may be able to discover all of your passwords and gain access to your information. Always remember to log out when you are using a public computer (at the library, an internet cafe, or even a shared computer at your office). Avoid using public computers and public Wi-Fi to access sensitive accounts such as banking and email.

There is no guarantee that these techniques will prevent an attacker from learning your password, but they will make it more difficult.

#### Don't forget security basics

- Keep your operating system, browser, and other software up to date.
- Use and maintain antivirus software and a firewall.
- Regularly scan your computer for spyware. (Some antivirus programs incorporate spyware detection.)
- Use caution with email attachments and untrusted links.

### 4.1.4 Increasing security

#### Run up-to-date antivirus software

A reputable antivirus software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware, such as viruses, worms, and ransomware. Many antivirus solutions are extremely easy to install and intuitive to use. It is recommended that all computers and mobile devices on your home network run antivirus software. Additionally, be sure to enable automatic virus definition updates to ensure maximum protection against the latest threats. Note: because detection relies on signatures—known patterns that can identify code as malware—even the best antivirus will not provide adequate protections against new and advanced threats, such as zero-day exploits and polymorphic viruses.

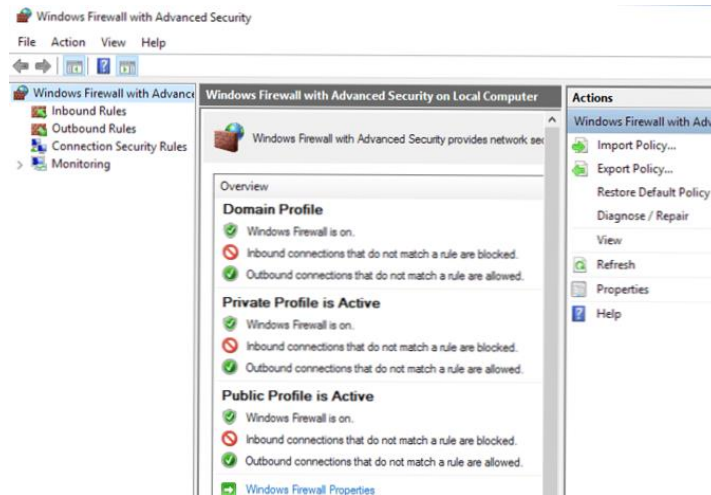


<https://review-shark.com/2021-best-antivirus-software-for-computer-and-laptop/>

### Install a network firewall

Install a firewall at the boundary of your home network to defend against external threats. A firewall can block malicious traffic from entering your home network and alert you to potentially dangerous activity. When properly configured, it can also serve as a barrier for internal threats, preventing unwanted or malicious software from reaching out to the internet. Most wireless routers come with a configurable, built-in network firewall that includes additional features—such as access controls, web-filtering, and denial-of-service (DoS) defense—that you can tailor to fit your networking environment. Keep in mind that some firewall features, including the firewall itself, may be turned off by default. Ensuring that your firewall is on and all the settings are properly configured will strengthen the network security of your network. Note: your internet service provider (ISP) may be able to help you determine whether your firewall has the most appropriate settings for your particular equipment and environment.

In addition to a network firewall, consider installing a firewall on all computers connected to your network. Often referred to as host- or software-based, these firewalls inspect and filter a computer's inbound and outbound network traffic based on a predetermined policy or set of rules. Most modern Windows and Linux operating systems come with a built-in, customizable, and feature-rich firewall. Additionally, most vendors bundle their antivirus software with additional security features such as parental controls, email protection, and malicious websites blocking.



## Regularly back up your data

Make and store—using either external media or a cloud-based service—regular backup copies of all valuable information residing on your device. Consider using a third-party backup application, which can simplify and automate the process. Be sure to encrypt your backup to protect the confidentiality and integrity of your information. Data backups are crucial to minimize the impact if that data is lost, corrupted, infected, or stolen.

## Increase wireless security

You might need to consult your router’s instruction manual or contact your ISP for specific instructions on how to change a particular setting on your device.

Use the strongest encryption protocol available. It is recommended to use the Wi-Fi Protected Access 3 (WPA3) Personal Advanced Encryption Standard (AES) and Temporary Key Integrity Protocol (TKIP), which is currently the most secure router configuration available for home use. It incorporates AES and is capable of using cryptographic keys of 128, 192, and 256 bits. This standard has been approved by the National Institute of Standards and Technology (NIST).

Change the router’s default administrator password. Change your router’s administrator password to help protect it from an attack using default credentials.

Change the default service set identifier (SSID). Sometimes referred to as the “network name,” an SSID is a unique name that identifies a particular wireless local area network (WLAN). All wireless devices on a Wireless Local Area Network (WLAN) must use the same SSID to communicate with each other. Because the device’s default SSID typically identifies the manufacturer or the actual device, an attacker can use this to identify the device and exploit any of its known vulnerabilities. Make your SSID unique and not tied to your identity or location, which would make it easier for the attacker to identify your home network.





**Disable Wi-Fi Protected Setup (WPS).** WPS provides simplified mechanisms for a wireless device to join a Wi-Fi network without the need to enter the wireless network password. However, a design flaw in the WPS specification for PIN authentication significantly reduces the time required for a cyberattacker to brute force an entire PIN, because it informs them when the first half of the eight-digit PIN is correct. Many routers lack a proper lockout policy after a certain number of failed attempts to guess the PIN, making a brute-force attack much more likely to occur. See *Brute Force Attacks Conducted by Cyber Actors*.

**Reduce wireless signal strength.** Your Wi-Fi signal frequently propagates beyond the perimeters of your home. This extended emission allows eavesdropping by intruders outside your network perimeter. Therefore, carefully consider antenna placement, antenna type, and transmission power levels. By experimenting with your router placement and signal strength levels, you can decrease the transmitting coverage of your Wi-Fi network, thus reducing this risk of compromise. Note: while this reduces your risk, a motivated attacker may still be able to intercept a signal that has limited coverage.

**Turn the network off when not in use.** While it may be impractical to turn the Wi-Fi signal off and on frequently, consider disabling it during travel or extended periods when you will not need to be online. Additionally, many routers offer the option to configure a wireless schedule that will automatically disable the Wi-Fi at specified times. When your Wi-Fi is disabled, you prevent outside attackers from being able to exploit your home network.

**Disable Universal Plug and Play (UPnP) when not needed.** UPnP is a handy feature that allows networked devices to seamlessly discover and establish communication with each other on the network. However, though the UPnP feature eases initial network configuration, it is also a security risk. Recent large-scale network attacks prove that malware within your network can use UPnP to bypass your router's firewall, allow attackers to take control of your devices remotely, and spread malware to other devices. You should therefore disable UPnP unless you have a specific need for it.

**Upgrade firmware.** Check your router manufacturer's website to ensure you are running the latest firmware version. Firmware updates enhance product performance, fix flaws, and address security vulnerabilities. Note: some routers have the option to turn on automatic updates.

**Disable remote management.** Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.

**Monitor for unknown device connections.** Use your router manufacturer's website to monitor for unauthorized devices joining or attempting to join your network. Also see the manufacturer's website for tips on how to prevent unauthorized devices from connecting to your network.

## Mitigate Email Threats

Phishing emails continue to be one of the most common initial attack vectors employed by for malware delivery and credential harvesting. Attacking the human element—considered the weakest component in every network—continues to be extremely effective. To infect a system, the attacker simply has to persuade a user to click on a link or open an attachment. The good news is that there are many indicators that you can use to quickly identify a phishing email. The best defense against these attacks is to become an educated and cautious user and familiarize yourself with the most common elements of a phishing attack.



----- Forwarded Message: -----  
From: "alerts@citibank.com" <ALERTS@CITIBANK.COM>  
To: recipient@email.com  
Subject: Security Alert: 06699  
Date: Thu, 29 May 2008 12:41:41 +0000



This is a Security Alert you requested to help you protect your account.

Your account has been blocked.

219 You have exceeded the number of three (3) failed login attempts.

To unlock your account, please [your account](#)

Thank you for your cooperation.

**Sincerely Yours,**

Letha Cox

[Letha.Cox@citibank.com](mailto:Letha.Cox@citibank.com)

## Avoiding Social Engineering and Phishing Attacks

Do not give sensitive information to others unless you are sure that they are indeed who they claim to be and that they should have access to the information.






### What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

## What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

-  Natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
-  Epidemics and health scares (e.g., H1N1, COVID-19)
-  Economic concerns (e.g., IRS scams)
-  Major political elections
-  Holidays

## What is a vishing attack?

Vishing is the social engineering approach that leverages voice communication. This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed, which can take advantage of the public's misplaced trust in the security of phone services, especially landline services. Landline communication cannot be intercepted without physical access to the line; however, this trait is not beneficial when communicating directly with a malicious actor.

## What is a smishing attack?

Smishing is a form of social engineering that exploits SMS, or text, messages. Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.

## What are common indicators of phishing attempts?

**Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.

**Generic greetings and signature.** Both a generic greeting—such as “Dear Valued Customer” or “Sir/Ma’am”—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.

**Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

**Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.

**Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

## How do you avoid being a victim?

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

Don't send sensitive information over the internet before checking a website's security. (See Protecting Your Privacy for more information.)

Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with "https"—an indication that sites are secure—rather than "http."

Look for a closed padlock icon—a sign your information will be encrypted.



If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.

Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

Take advantage of any anti-phishing features offered by your email client and web browser.

Enforce multi-factor authentication (MFA).

### What do you do if you think you are a victim?

If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

## 4.1.5 What is malicious code?

Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses.

```

45 <script>
46   var js, fjs = d.getElementsByTagName(
47     if (d.getElementById(id)) return;
48     js = d.createElement(s); js.id = id;
49     js.src = "//connect.facebook.net/en_US/sdk.js#xfbml=1&version=v2.6&appId=1884444444444444";
50     fjs.parentNode.insertBefore(js, fjs);
51   })(document, 'script', 'facebook-jssdk');</script>
52 <div id="page" class="site">
53   <a class="skip-link screen-reader-text" href="#content"><?php esc_html_e( 'Skip to content', 'urduube' ); ?></a>
54   <header id="masthead" class="site-header" role="banner">
55     <div class="site-branding">
56       <div class="navBtn pull-left">
57         <?php if(is_home() && $xpanel['homepage-style'] == 1) { ?>
58           <a href="#" id="openMenu"><i class="fa fa-bars fa-3x"></i></a>
59           <?php } else { ?>
60             <a href="#" id="openMenu2"><i class="fa fa-bars fa-3x"></i></a>
61           <?php } ?>
62         </div>
63         <div class="logo pull-left">
64           <a href="<?php echo esc_url( home_url() ) ?>">
65             
66           </a>
67         </div>
68         <div class="search-box hidden-xs hidden-sm pull-left ml-10">
69           <?php get_search_form(); ?>
70         </div>
71         <div class="submit-btn hidden-xs hidden-sm pull-left ml-10">
72           <?php echo get_page_link($xpanel['submit-link']) ?> <div class="header-submit-btn"><i class="fa fa-search fa-3x"></i></div>

```

**Viruses** have the ability to damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages.

**Worms** are a type of virus that self-propagates from computer to computer. Its functionality is to use all of your computer's resources, which can cause your computer to stop responding.

**Trojan Horses** are computer programs that are hiding a virus or a potentially damaging program. It is not uncommon that free software contains a Trojan horse making a user think they are using legitimate software, instead the program is performing malicious actions on your computer.

**Malicious data files** are non-executable files—such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file—that exploits weaknesses in the software program used to open it. Attackers frequently use malicious data files to install malware on a victim's system, commonly distributing the files via email, social media, and websites.

### How do you recover if you become a victim of malicious code?

Using antivirus software is the best way to defend your computer against malicious code. If you think your computer is infected, run your antivirus software program. Ideally, your antivirus program will identify any malicious code on your computer and quarantine them so they no longer affect your system. You should also consider these additional steps:



Minimize the damage. If you are at work and have access to an information technology (IT) department, contact them immediately. The sooner they can investigate and “clean” your computer, the less likely it is to cause additional damage to your computer—and other computers on the network. If you are on a home computer or laptop, disconnect your computer from the internet; this will prevent the attacker from accessing your system.



Remove the malicious code. If you have antivirus software installed on your computer, update the software and perform a manual scan of your entire system. If you do not have antivirus software, you can purchase it online or in a computer store. If the software cannot locate and remove the infection, you may need to reinstall your operating system, usually with a system restore disk. Note that reinstalling or restoring the operating system typically erases all of your files and any additional software that you have installed on your computer. After reinstalling the operating system and any other software, install all of the appropriate patches to fix known vulnerabilities.

Threats to your computer will continue to evolve. Although you cannot eliminate every hazard, by using caution, installing and using antivirus software, and following other simple security practices, you can significantly reduce your risk and strengthen your protection against malicious code.





## What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

Although the features of social networking sites differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, email, instant messages) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest.

## What security implications do these sites present?

Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because

-  the internet provides a sense of anonymity
-  the lack of physical interaction provides a false sense of security
-  they tailor the information for their friends to read, forgetting that others may see it
-  they want to offer insights to impress potential friends or associates

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you. Predators may form relationships online and then convince unsuspecting individuals to meet them in person. That could lead to a dangerous situation. The personal information can also be used to conduct a social engineering attack. Using information that you provide about your location, hobbies, interests, and friends, a malicious person could impersonate a trusted friend or convince you that they have the authority to access other personal or financial data.

Additionally, because of the popularity of these sites, attackers may use them to distribute malicious code. Sites that offer applications developed by third parties are particularly susceptible. Attackers may be able to create customized applications that appear to be innocent while infecting your computer or sharing your information without your knowledge.



## 4.1.6 Practical activities

### Step 1: Cleaning dust from computers

1. This problem can be noticed by the noise produced by the speed of the cooling fans, when using the personal computer or personal laptop.
2. You have probably noticed that at the beginning of using the computer, when it was new, the cooling fans were quiet because the cooling fans were not dusty.
3. After a longer period of use, the computer / laptop becomes very noisy due to the high speed of the dusty fans, which no longer manage to ensure the air flow necessary to cool the electronic components in the computer, reaching a point to stop (lock) and leads to destruction of internal components, microprocessors due to the high operating temperature.
4. The negative aspect of dust is the thermal effect created by the deposition of dust on components (on and around the processor radiator).
5. Thus the existence of dust in the computer can cause the destruction of electronic components. Due to the dust they overheat leading to their destruction. For this reason, computers must be dusted regularly.
6. Assuming you have a computer at home that you use, please answer the following question for yourself: "When was the last time you cleaned the computer of dust?"
7. Cleaning can be done at a specialized computer troubleshooting workshop.
8. Dust cleaning on laptops requires more difficult operations for this reason you must call a specialized service.
9. To understand what it means to clean a dusty computer, you can search the internet, opening an internet search engine and typing in the search field "how to clean dust from computers?". One website we recommend is: <https://www.wikihow.com/Clean-a-Dusty-Computer>
10. However, considering the fact that this course is addressed to beginners, with less knowledge in this field, we recommend that for a start, to clean the computer to use a specialized service.

COMPUTERS » COMPUTER MAINTENANCE

## How to Clean a Dusty Computer

Co-authored by **James Sears**

Last Updated: October 15, 2020 References

Every computer slowly fills up with dust and other loose debris as it filters air through its hardware. While the goal of the fans found in any computer is to cool off all the components that get hot, the dust that clogs up a computer does the opposite. It's important to try and get rid of the dust in your computer with canned air and a microfiber cloth on a regular basis. However, a deeper clean with rubbing alcohol and cotton swabs might be necessary if it's been a while since your last dusting efforts.

Download Article

**METHODS**

- 1 Opening up Your Computer
- 2 Dusting Internal Components with Compressed Air
- 3 Deep Cleaning with Rubbing Alcohol
- 4 Show 1 more...

**OTHER SECTIONS**

- Things You'll Need
- Related Articles
- References



## Step 2: For a computer it is necessary to install an antivirus / firewall protection program

1. To understand what an antivirus software is, we recommend you to access the website: <https://us.norton.com/internetsecurity-malware-what-is-antivirus.html>
2. Of course, there are many antivirus software on the market. An internet search, for example, for the keywords "antivirus software compare" can find countless pages to find information about existing software, such as: <https://www.pcmag.com/picks/the-best-antivirus-protection> where in the "OUR 13 TOP PICKS" section are listed several antivirus software
3. In your computer, if you do not have another antivirus installed, we recommend you search in a search page for the keywords "free trial antivirus" and access the link <https://www.kaspersky.com/downloads/thank-you/antivirus-free-trial> and in the opened page, click on the "DOWNLOAD NOW" button.
4. The computer we use, for example, has WINDOWS 10 operating system and "Google Chrome" as internet browser
5. The recommendation for Kaspersky was made, due to the fact that on the computer we use, this is the antivirus security solution installed, and in order to do not generate conflicts with other types of antivirus software, we recommended this solution.
6. At the bottom of the Chrome browser window, after pressing the "DOWNLOAD NOW" button, is displayed the executable archive "kav21.3.10.391en\_26075.exe" (of course the archive name may vary depending on the downloaded version)
7. Now after downloading from the internet and installing, you have installed an antivirus security solution in your computer! Congratulations!
8. The antivirus always works and is active in the background of the operating system
9. At the bottom right of the screen, next to the clock, an icon with a "K" appears. It is possible that this icon is hidden by the windows system, which is why it will be necessary to first click on the button "^", next to the clock
10. If you click on the "K" icon, the Kaspersky antivirus settings interface is launched.
11. In the opened interface click on the "TASKS" button area and in the open window in the "FULL SCAN" area click on START. We notice that the antivirus software starts scanning the computer for viruses, if any exist.
12. After the scan is complete, the scan can be restarted whenever desired. The antivirus can be set to start the computer scanning process automatically



13. Also in this opened window when clicking on TASKS, scrolling below, you reach the UPDATE area. By pressing the START button in this area, the antivirus application will be updated to the latest version and to the latest database provided by the manufacturer. It is recommended that this update be done periodically
14. It should be noted that security solutions, can be both for protecting your personal computer against viruses and for protecting your computer from unauthorized access, when the computer is in a computer network.
15. For this situation on the website for Kaspersky <https://www.kaspersky.com/home-security> are presented 3 variants of the protection software, next to each being specified for what it can ensure the protection
16. For example, the "Kaspersky Internet Security" protection solution is an integrated solution that provides both antivirus protection and protection in the computer network (firewall).
17. In general, all antivirus protection software offers integrated options for both antivirus protection and protection in the computer network.
18. Similarly, other antivirus programs can be installed by accessing the dedicated page of the manufacturer for downloading and purchasing related licenses.
19. The presentation is not strictly limited to Kaspersky antivirus! When choosing and according to the needs of each of you, similarly, other antivirus software can be installed both on the computer and on portable electronic systems.

## 4.2 Protecting personal data and privacy





Unit 4.2	Protecting personal data and privacy	
Duration	9h	
Objectives	 To be aware of issues related to personal data sharing  To be able to set up security settings to preserve privacy	
Content	4.2.1 Protecting yourself online 4.2.2 Guidelines for sharing personal information 4.2.3 Practical activities	
Resources	Training manual, computers with internet access	
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate	

Table 23 - Structure of the unit of competence 4.2. – Protecting personal data and privacy of the Module 4 – Security.

### 4.2.1 Protecting yourself online

#### How can you protect yourself?

**Limit the amount of personal information you post** - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

**Remember that the internet is a public resource** - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.

**Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.

**Be skeptical** - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.

**Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

**Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

**Use strong passwords** - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

**Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

**Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. (See Understanding Patches.) Many operating systems offer automatic updates. If this option is available, you should enable it.

**Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. (See Understanding Anti-Virus Software.) Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

**Children are especially susceptible to the threats that social networking sites present** - Although many of these sites have age restrictions, children may misrepresent their ages so that they can join. By teaching children about Internet safety, being aware of their online habits, and guiding them to appropriate sites, parents can make sure that the children become safe and responsible users.



### Why is it important to remember that the internet is public?

The internet is an accessible, popular resource for communicating with others and conducting research. You may have a sense of anonymity while online but should remember that you are not anonymous, and it is just as easy for people to find information about you as it is for you to find information about them.

Many people have become so familiar and comfortable with the internet that they adopt practices that make them vulnerable. For example, although people are typically wary of sharing personal information with strangers they meet on the street, they may not hesitate to post that same information online. Once it is online, it can be accessed by a world of strangers, and you have no idea what they might do with that information.

### 4.2.2 Guidelines for sharing personal information

What guidelines can you follow when publishing information on the internet?

**View the internet as a novel, not a diary.** Make sure you are comfortable with anyone seeing the information you put on blogs, social networking sites, and personal websites—write it with the expectation that it is available for public consumption and that people you have never met will find your page. Although some sites use passwords or other security restrictions to protect the information, these methods are not used for most websites. If you want the information to be private or restricted to a small, select group of people, the internet is not the best forum.

**Limit the amount of personal information you post.** Do not post information that could make you vulnerable, such as your address, phone number, email, or information about your schedule or routine. Supplying your email address may increase the amount of spam you receive (see Reducing Spam for more information). Providing details about your hobbies, your job, your family and friends, or your past may give attackers enough information to perform a successful social engineering attack (see Avoiding Social Engineering and Phishing Attacks and Staying Safe on Social Networking Sites for more information).

**Realize that you cannot take it back.** Once you publish something online, it is available to other people and to search engines. You can change or remove information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines "cache" copies of web pages; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the web pages a user has visited, so the original version may be stored in a temporary file on the user's computer. Think about these implications before publishing information—once something is out there, you cannot guarantee that you can completely remove it.

As a general practice, let common sense guide your decisions about what to post online. Before you publish something on the internet, determine what value it provides and consider the implications of having the information available to the public. Identity theft is an increasing problem, and the more information an attacker can gather about you, the easier it is to pretend to be you.

### How Anonymous Are You?





You may think that you are anonymous as you browse websites, but pieces of information about you are always left behind. You can reduce the amount of information revealed about you by visiting legitimate sites, checking privacy policies, and minimizing the amount of personal information you provide.

### What information is collected?

When you visit a website, a certain amount of information is automatically sent to the site. This information may include the following:



**IP address** - Each computer on the internet is assigned a specific, unique IP (internet protocol) address. Your computer may have a static IP address or a dynamic IP address. If you have a static IP address, it never changes. However, some ISPs own a block of addresses and assign an open one each time you connect to the internet—this is a dynamic IP address. You can determine your computer's IP address at any given time by visiting [www.showmyip.com](http://www.showmyip.com).

-  Domain name - The internet is divided into domains, and every user's account is associated with one of those domains. You can identify the domain by looking at the end of URL; for example, .edu indicates an educational institution, .gov indicates a US government agency, .org refers to organization, and .com is for commercial use. Many countries also have specific domain names. The list of active domain names is available from the Internet Assigned Numbers Authority (IANA).
-  Software details - It may be possible for an organization to determine which browser, including the version, that you used to access its site. The organization may also be able to determine what operating system your computer is running.
-  Page visits - Information about which pages you visited, how long you stayed on a given page, and whether you came to the site from a search engine is often available to the organization operating the website.
-  If a website uses cookies, the organization may be able to collect even more information, such as your browsing patterns, which include other sites you have visited. If the site you are visiting is malicious, files on your computer, as well as passwords stored in the temporary memory, may be at risk.

### How is this information used?

Generally, organizations use the information that is gathered automatically for legitimate purposes, such as generating statistics about their sites. By analyzing the statistics, the organizations can better understand the popularity of the site and which areas of content are being accessed the most. They may be able to use this information to modify the site to better support the behavior of the people visiting it.

Another way to apply information gathered about users is marketing. If the site uses cookies to determine other sites or pages you have visited, it may use this information to advertise certain products. The products may be on the same site or may be offered by partner sites.

However, some sites may collect your information for malicious purposes. If attackers are able to access files, passwords, or personal information on your computer, they may be able to use this data to their advantage. The attackers may be able to steal your identity, using and abusing your personal information for financial gain. A common practice is for attackers to use this type of information once or twice, then sell or trade it to other people. The attackers profit from the sale or trade, and increasing the number of transactions makes it more difficult to trace any activity back to them. The attackers may also alter the security settings on your computer so that they can access and use your computer for other malicious activity.

### Are you exposing any other personal information?

While using cookies may be one method for gathering information, the easiest way for attackers to get access to personal information is to ask for it. By representing a malicious site as a legitimate one, attackers may be able

to convince you to give them your address, credit card information, social security number, or other personal data.

### 4.2.3 Practical Activities

#### Step 1: Lock the computer with password

1. Today's equipment offers multiple ways to protect yourself! For example in WINDOWS 10 in the SETTINGS -> Sign-in options section you have the possibility to password your computer through one of the options: facial recognition, fingerprint, PIN, security key, password or image recognition.
2. We will not discuss all this today, but it should be mentioned that any computer offers the possibility set a password (this can be done in general from the SETTINGS section of your equipment)
3. Today we focus on setting a password. The password is a sequence of characters written in a given order, which can contain: uppercase, lowercase, numbers, special characters
4. For example, if in WINDOWS we set the password "@calculatorMeuDeNota10" to SETTINGS -> Sign-in options, then when accessing the computer at restart or exiting the operating system from standby, the password will be requested. What password? @calculatorulMeuDeNota10, the letters written in exactly the same order and the same type of letter. ATTENTION: the computer will not recognize the password @CALCULATORULMEUDENOTA10 or @calculatorulmeudenota10 or @ calculatorulMeu De Nota 10. The password recognized by the system will be exactly as the established one, respectively @ calculatorulMeuDeNota10
5. Attention: a password set, don't forget it! It would be best to write it down somewhere where you can find it. If you have forgotten your password, there are different ways to recover it, but this requires much more advanced knowledge and often brings problems in recovering it.
6. A password must contain special characters (@), lowercase letters (calculatorulmeudenota), uppercase letters (M D N), numbers (10).
7. The more characters a password contains, that password will be much stronger, and will be the harder for someone to find it.
8. To understand what a strong password is, we recommend you access the following site: <https://ro.safetydetectives.com/password-meter/>
9. In the upper right part, you can set the language in which the information from the site will be displayed
10. In the field under the heading "How secure is my password?" you can type and test password patterns
11. The higher the number of characters the password contains and more characters listed above, the higher the score obtained on the right side of the field will be, and the type of password becomes from VERY WEAK to VERY STRONG
12. Try to find a password that gets a grade of 100! Do you succeed? Password from this exercise what score do you think it will get?



13. Finally, we recommend you to read the Frequently Asked Questions section at the bottom of the page <https://ro.safetydetectives.com/password-meter/>
14. In this way you will get more information on how to create very good and secure passwords.

## Step 2: Using a browser and periodic updates

1. Open a web page, type the internet address [www.google.com](http://www.google.com) and type the following words "chrome download" in the search field
2. On the computer, search for and download the Chrome internet browser (if not already installed) at <https://www.google.com/chrome/>
3. From the opened page press the DOWNLOAD CHROME button
4. Access the downloaded file and follow the installation steps
5. Open one or more web pages in the Chrome browser (it's up to you which web pages do you want to access)
6. Notice in the navigation bar, whether or not there is a padlock in front of the accessed internet address
7. That padlock represent a security certificate for the accessed page and in its absence the navigation on the page is not safe. So a safe browsing can be done on those internet pages when the padlock exists
8. On a secure web page (where that padlock exists), click on that padlock and observe from the information provided if the certificate is valid
9. Click on Certificate (Valid) and observe the date until which the certificate is valid
10. The "lock" icon is a confirmation that the Internet connection between the person accessing that site and the server of that site is a secure connection, it is an encrypted communication (other users can not access, intercept, the established connection of you with that website)
11. Close the certificate information window and click on the 3 vertical dots at the top right (located below the X close window) to access Chrome settings
12. Click on "Help" and in the new menu click on "About Google Chrome"
13. At this point Google Chrome will try to update to the latest available version of the software with the following message:  
"Updating Google Chrome (50%)  
Version 90.0.4430.212 (Official Build) (64-bit)"
14. After the update, Chrome may ask you to restart your browser with a message  
"Nearly up to date! Relaunch Google Chrome to finish updating. Incognito windows will not reopen.  
Version 90.0.4430.212 (Official Build) (64-bit)"
15. Press the button "Relunch"
16. If it is not necessary to reopen the browser or the browser is already updated, a message will appear  
"Google Chrome is up to date  
Version 91.0.4472.77 (Official Build) (64-bit)"
17. In this way the Chrome browser can be update



18. Please note that any software and not just the Chrome browser, offers the possibility to update to higher versions but not all software offers this feature for free
19. Updating to newer versions offers the security and stability of the software in use

### 4.3 Protecting health and well-being






Unit 4.3 Protecting health and well-being	
Duration	5h
Objectives	 to be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies;  to be able to protect oneself and others from possible dangers in digital environments;  to be able to control the aspects that distract from work and digital life;  to be able to take preventive measures to protect the health of the person for whom he is responsible
Content	4.3.1 Negative effects of technology: what to know 4.3.2 Have you heard of cyberbullying? 4.3.3 Practical activities
Resources	Training manual, computers with internet access
Training methodologies	 Presentation by trainer

Table 24 - Structure of the unit of competence 4.3. – Protecting health and well-being of the Module 4 – Security.

#### 4.3.1 Negative effects of technology: what to know

People are more connected than ever, thanks in large part to rapid advancements in technology.

While some forms of technology may have made positive changes in the world, there is evidence for the negative effects of technology and its overuse, as well.

Social media and mobile devices may lead to psychological and physical issues, such as eyestrain and difficulty focusing on important tasks. They may also contribute to more serious health conditions, such as depression.



## Psychological effects

Overuse or dependence on technology may have adverse psychological effects, including: Isolation. Technologies, such as social media, are designed to bring people together, yet they may have the opposite effect in some cases.

A 2017 study in young adults aged 19–32 years found that people with higher social media use were more than three times as likely to feel socially isolated than those who did not use social media as often.

Finding ways to reduce social media use, such as setting time limits for social apps, may help reduce feelings of isolation in some people.

## Depression and anxiety

The authors of a 2016 systematic review Trusted Source discussed the link between social networks and mental health issues, such as depression and anxiety.

Their research found mixed results. People who had more positive interactions and social support on these platforms appeared to have lower levels of depression and anxiety.

However, the reverse was also true. People who perceived that they had more negative social interactions online and who were more prone to social comparison experienced higher levels of depression and anxiety.

So, while there does appear to be a link between social media and mental health, a significant determining factor is the types of interactions people feel they are having on these platforms.

## Physical health effects







Technology use may increase the risk of physical issues as well, including:

### Eyestrain

Technologies, such as handheld tablets, smartphones, and computers, can hold a person's attention for long periods. This may lead to eyestrain.

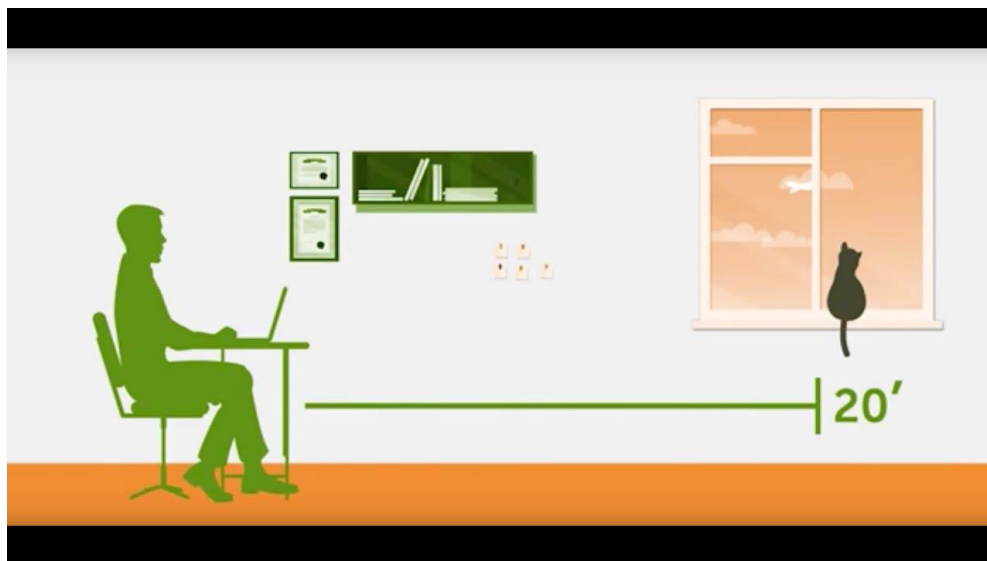
Symptoms of digital eyestrain can include blurred vision and dry eyes. Eyestrain may also lead to pains in other areas of the body, such as the head, neck, or shoulders.

Several technological factors may lead to eyestrain, such as:

-  screen time
-  screen glare
-  screen brightness
-  viewing too close or too far away
-  poor sitting posture
-  underlying vision issues

Taking regular breaks away from the screen may reduce the likelihood of eyestrain.

Anyone regularly experiencing these symptoms should see an optometrist for a checkup.



### The 20-20-20 rule for digital viewing

When using any form of digital screen for longer periods of time, it is recommended to use the 20-20-20 rule. To use the rule, after every 20 minutes of screen time, take a 20-second break to look at something at least 20 m away. Doing this may help reduce the strain on the eyes from staring at a screen for a continuous period.

### Poor posture

The way many people use mobile devices and computers may also contribute to incorrect posture. Over time, this may lead to musculoskeletal issues. Many technologies promote a “down and forward” user position, meaning the person is hunched forward and looking down at the screen. This can put an unnecessary amount of pressure on the neck and spine. A 5-year study in the journal *Applied Ergonomics* found an association between

texting on a mobile phone and neck or upper back pain in young adults. The results indicated the effects were mostly short term, though some people continued to have long-term symptoms.

However, some studies challenge these results.

A 2018 study Trusted Source in the European Spine Journal found that the posture of the neck while texting made no difference in symptoms such as neck pain.

This study concluded that texting and “text neck” did not influence neck pain in young adults. However, the study did not include a long-term follow-up. It may be that other factors influence neck pain, as well, such as age and activity levels. Correcting posture problems while using technology may lead to an overall improvement in posture and strength in the core, neck, and back.

For example, if a person finds themselves sitting in the same position for hours at a time, such as sitting at a desk while working, regularly standing or stretching may help reduce strain on the body.

Additionally, taking short breaks, such as walking around the office every hour, may also help keep the muscles loose and avoid tension and incorrect posture.







## Sleep problems

Using technology too close to bedtime may cause issues with sleep. This effect has to do with the fact that blue light, such as the light from cell phones, e-readers, and computers, stimulates the brain. Authors of a 2014 study found that this blue light is enough to disturb the body’s natural circadian rhythm. This disturbance could make it harder to fall asleep or lead to a person feeling less alert the next day. To avoid the potential impact of blue

light on the brain, people can stop using electronic devices that emit blue light in the hour or two before bedtime. Gentle activities to wind down with instead, such as reading a book, doing gentle stretches, or taking a bath, are alternatives.

### Reduced physical activity

Most everyday digital technologies are sedentary. More extended use of these technologies promotes a more sedentary lifestyle, which is known to have negative health effects, such as contributing to:

-  obesity
-  cardiovascular disease
-  type 2 diabetes
-  premature death

Finding ways to take breaks from sedentary technologies may help promote a more active lifestyle.

Research from 2017 indicates that active technologies, such as app notifications, emails, and wearable technologies that promote exercise may reduce short-term sedentary behavior. This could help people set healthful patterns and become more physically active.

### 4.3.2 Have you heard of cyberbullying?

Cyberbullying is using technology to harass, or bully, someone else. Bullies used to be restricted to methods such as physical intimidation, postal mail, or the telephone, but computers, cell phones, tablets, and other mobile devices offers bullies forums such as email, instant messaging, web pages, and digital photos.

Forms of cyberbullying can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking. It can affect any age group; however, teenagers and young adults are common victims, and cyberbullying is a growing problem in schools.






#### Why has cyberbullying become such a problem?

The relative anonymity of the internet is appealing for bullies because it enhances the intimidation and makes tracing the activity more difficult. Some bullies also find it easier to be more vicious because there is no personal contact. The internet and email can also increase the visibility of the activity. Information or pictures posted online or forwarded in mass emails can reach a larger audience faster than more traditional methods, causing more damage to the victims. A large amount of personal information is available online, so bullies may be able to arbitrarily choose their victims.

Cyberbullying may also indicate a tendency toward more serious behavior. While bullying has always been an unfortunate reality, most bullies grow out of it. Cyberbullying has not existed long enough to have solid research, but there is evidence that it may be an early warning for violent behavior.



### How can you protect yourself or your children?

-  Teach your children good online habits. Explain the risks of technology, and teach children how to be responsible online. Reduce their risk of becoming cyberbullies by setting guidelines for and monitoring their use of the internet and other electronic media (cell phones, tablets, etc.).
-  Keep lines of communication open. Regularly talk to your children about their online activities so that they feel comfortable telling you if they are being victimized.
-  Watch for warning signs. If you notice changes in your child's behavior, try to identify the cause as soon as possible. If cyberbullying is involved, acting early can limit the damage.
-  Limit availability of personal information. Limiting the number of people who have access to contact information or details about interests, habits, or employment reduces exposure to bullies that you or your child do not know. This may limit the risk of becoming a victim and may make it easier to identify the bully if you or your child are victimized.
-  Avoid escalating the situation. Responding with hostility is likely to provoke a bully and escalate the situation. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. Other options include subtle actions. For example, you may be able to block the messages on social networking sites or stop unwanted emails by changing the email address. If you continue to get messages at the new email address, you may have a stronger case for legal action.



Document the activity. Keep a record of any online activity (emails, web pages, instant messages, etc.), including relevant dates and times. In addition to archiving an electronic version, consider printing a copy.



Report cyberbullying to the appropriate authorities. If you or your child are being harassed or threatened, report the activity. Many schools have instituted anti-bullying programs, so school officials may have established policies for dealing with activity that involves learners. If necessary, contact your local law enforcement.

### 4.3.3 Practical activities

#### Step 1: Eye protection

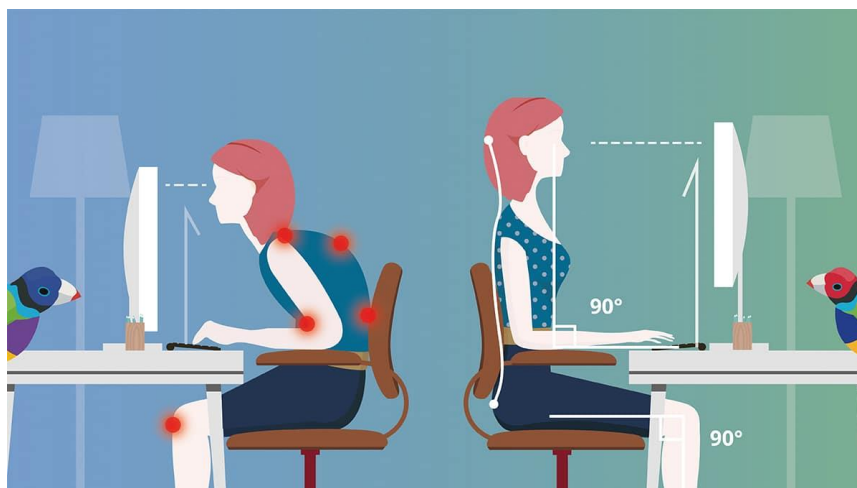
1. On your computer, open an MS Office or Notepad editing application. We used Notepad, a software included in the Windows operating system.
2. Write a text of a few letters / words, with the standard defined font size without being changed.
3. Select with the mouse, the text written in Notepad and with the selected text, from the top menu bar press Format-> Font-> and in the area called Size select the largest available size (in my case 72). Notice, the eye how ease can read the written text, the restful feeling you have when reading a text with an bigger size font.
4. Select again with the mouse, the text written in Notepad and with the selected text, from the top menu bar press Format-> Font-> and in the area called Size select the smallest size available for the font (in my case 8 ). Notice, the eye how hard can read the written text, the feeling of forcing the eye, that you feel when you read a text with a very small size font.
5. If you want, to observe those 2 differences, you can do this exercise several times.
6. Now, please look at this exercise from the following perspective: Suppose you spend 5 hours a day in front of the computer. Whether you have work to do, whether you are watching a movie or looking at photos, at any time the eye will try to adapt as much and as well as possible to read as much possible information from the images displayed on the monitor, even if that information is easier or harder to see. This way of forcing the eye can lead to vision problems over time.
7. For this reason there are different ways to prolong your eye health. Google knows this problem and in the extensions in Google Chrome can be added an extension suggestively called "eyeCare - Protect your vision". It can be searched in the google search engine by keywords such as "Eye Care Chrome" and from the displayed results access the link <https://chrome.google.com/webstore/detail/eyecare-protect-your-vision/eeeningnfkaonkonalcicgemnnijjhn>
8. In the page, next to the eyeCare - Protect your vision extension, click the "Add to Chrome" button
9. In the newly opened window click the Add extension button
10. This extension is a reminder for the 20-20-20 rule (every 20 minutes, take your eyes off your computer and look at something 20 feet away for at least 20 seconds)



11. In this way, the eye is set to look at a different distance from the monitor (20 feet away), thus contributing to eye health.

## Step 2: Protecting physical health (computer work position)

1. The first step in this exercise is to be aware of the position you have in front of the computer (do not change this position, do not stretch your back. Stay exactly in the same position you are in, for the next point).
2. Look at the picture below, and say what position you are in: the left position (with the spine in a curved position) or the right position (with the right spine)?



3. Thus, if you are in the position in the image on the right side: CONGRATULATIONS! But if you are in the position in the image on the left side, a position where most people are usually, then you need to understand the following aspects:
4. After a longer period spent in front of electronic equipment, involuntarily, without realizing it, the body tends to relax and from the correct working position you can reach the position to the left of the image, which leads in time to health problems on spine, especially at the people who spends many hours a day, and many days a week at the computer
5. For this reason we must be aware of our position when working on the computer and correct ourselves! This little effort can keep our spine healthy over time.
6. How is your back now? Did you straighten your spine?

## 4.4 Protecting the environment






Unit 4.4	Protecting the environment
Duration	5 hours
Objectives	 To be able to select safe, efficient and cost-effective media  To understand digital media impact  To know how to dispose electronic devices safely
Content	4.4.1 Proper disposal of electronic devices 4.4.2 Practical activities
Resources	Training manual, computers with internet access
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate

Table 25 - Structure of the unit of competence 4.4. – Protecting the environment of the Module 4 – Security.





### 4.4.1 Proper Disposal of Electronic Devices

#### Why is it important to dispose of electronic devices safely?

In addition to effectively securing sensitive information on electronic devices, it is important to follow best practices for electronic device disposal. Computers, smartphones, and cameras allow you to keep a great deal of information at your fingertips, but when you dispose of, donate, or recycle a device you may inadvertently disclose sensitive information, which could be exploited by cyber criminals.



Types of electronic devices include:






-  Computers, smartphones, and tablets — electronic devices that can automatically store and process data; most contain a central processing unit and memory, and use an operating system that runs programs and applications;
-  Digital media — these electronic devices create, store, and play digital content. Digital media devices include items like digital cameras and media players;
-  External hardware and peripheral devices — hardware devices that provide input and output for computers, such as printers, monitors, and external hard drives; these devices contain permanently stored digital characters; and
-  Gaming consoles — electronic, digital, or computer devices that output a video signal or visual image to display a video game.

What are some effective methods for removing data from your device?

There are a variety of methods for permanently erasing data from your devices (also called sanitizing). Because methods of sanitization vary according to device, it is important to use the method that applies to that particular device.

Before sanitizing a device, consider backing up your data. Saving your data to another device or a second location (e.g., an external hard drive or the cloud) can help you recover your data if you accidentally erase information you had not intended to or if your device is stolen (this can also help you identify exactly what information a thief may have been able to access). Options for digital storage include cloud data services, CDs, DVDs, and removable flash drives or removable hard drives.

Methods for sanitization include:

-  Deleting data. Removing data from your device can be one method of sanitization. When you delete files from a device—although the files may appear to have been removed—data remains on the media even after a delete or format command is executed. Do not rely solely on the deletion method you routinely use, such as moving a file to the trash or recycle bin or selecting “delete” from the menu. Even if you empty the trash, the deleted files are still on device and can be retrieved. Permanent data deletion requires several steps.
-  Computers. Use a disk cleaning software designed to permanently remove the data stored on a computer hard drive to prevent the possibility of recovery.
-  Secure erase. This is a set of commands in the firmware of most computer hard drives. If you select a program that runs the secure erase command set, it will erase the data by overwriting all areas of the hard drive.
-  Disk wiping. This is a utility that erases sensitive information on hard drives and securely wipes flash drives and secure digital cards.
-  Smartphones and tablets. Ensure that all data is removed from your device by performing a “hard reset.” This will return the device to its original factory settings. Each device has a different hard reset procedure,

but most smartphones and tablets can be reset through their settings. In addition, physically remove the memory card and the subscriber identity module card, if your device has one.



Digital cameras, media players, and gaming consoles. Perform a standard factory reset (i.e., a hard reset) and physically remove the hard drive or memory card.



Office equipment (e.g., copiers, printers, fax machines, multifunction devices). Remove any memory cards from the equipment. Perform a full manufacture reset to restore the equipment to its factory default.



Overwriting. Another method of sanitization is to delete sensitive information and write new binary data over it. Using random data instead of easily identifiable patterns makes it harder for attackers to discover the original information underneath. Since data stored on a computer is written in binary code—strings of 0s and 1s—one method of overwriting is to zero-fill a hard disk and select programs that use all zeros in the last layer. Users should overwrite the entire hard disk and add multiple layers of new data (three to seven passes of new binary data) to prevent attackers from obtaining the original data.



Cipher.exe is a built-in command-line tool in Microsoft Windows operating systems that can be used to encrypt or decrypt data on New Technology File System drives. This tool also securely deletes data by overwriting it.



Clearing is a level of media sanitation that does not allow information to be retrieved by data, disk, or file recovery utilities. Devices must be resistant to keystroke recovery attempts from standard input devices (e.g., a keyboard or mouse) and from data scavenging tools.



Destroying. Physical destruction of a device is the ultimate way to prevent others from retrieving your information. Specialized services are available that will disintegrate, burn, melt, or pulverize your computer drive and other devices. These sanitization methods are designed to completely destroy the media and are typically carried out at an outsourced metal destruction or licensed incineration facility. If you choose not to use a service, you can destroy your hard drive by driving nails or drilling holes into the device yourself. The remaining physical pieces of the drive must be small enough (at least 1/125 inches) that your information cannot be reconstructed from them. There are also hardware devices available that erase CDs and DVDs by destroying their surface.



Magnetic media degaussers. Degaussers expose devices to strong magnetic fields that remove the data that is magnetically stored on traditional magnetic media.



Solid-state destruction. The destruction of all data storage chip memory by crushing, shredding, or disintegration is called solid-state destruction. Solid-State Drives should be destroyed with devices that are specifically engineered for this purpose.



CD and DVD destruction. Many office and home paper shredders can shred CDs and DVDs (be sure to check that the shredder you are using can shred CDs and DVDs before attempting this method).

## How can you safely dispose of out-of-date electronic devices?

Electronic waste (sometimes called e-waste) is a term used to describe electronics that are nearing the end of their useful life and are discarded, donated, or recycled. Although donating and recycling electronic devices conserves natural resources, you may still choose to dispose of e-waste by contacting your local landfill and

requesting a designated e-waste drop off location. Be aware that although there are many options for disposal, it is your responsibility to ensure that the location chosen is reputable and certified.

## 4.4.2 Practical activities

### Step 1: Electricity consumption - Equipment operating costs

1. As we all know electrical equipment, it can only work if it is powered by electricity. But how much energy is consumed for a computer? For the answer let's go through the calculation described below.
2. Consider two computer units: a laptop (for example the one I use) and a computer (a central unit), with technical characteristics approximately the same as the laptop
3. Laptop: I read the value of the power supply for the laptop and I notice that it is 130W (watts)
4. Let's do together the following calculation: laptop used 7 days a week (5 days at work and 2 days on weekends for movies, music, photos, etc.), about 8 hours / day (h / day) on average
5. Let's estimate the average lifespan of the laptop at about 5 to 7 years
6. Let's calculate the power consumption for this laptop, as follows:

For 1 year of use	For 7 years of use
<ul style="list-style-type: none"> <li>• Power supply (Watts) x number of days (zile) x average days (h/zi) x 1 year = 130W x 365 days x 8h/day x 1year = 379.600 Wh/year = 379,6 kWh/year (kiloWatts hour in 1 year)</li> </ul>	<ul style="list-style-type: none"> <li>• Power consumed for 1 year x 7 years = 379.600 kWh/year x 7 year= 2.657.200 Wh = 2.657,2 kWh</li> </ul>

Figure 12 – Data for the calculation of the power consumption.

7. Computer calculation (central unit): We made an research on internet for the best power supplies for a computer: <https://www.digitaltrends.com/computing/best-pc-power-supply/> and I chose some examples of power supplies: "Corsair RM750" 750W, "FSP Dagger " 550W or "Thermaltake Toughpower Grand RGB" 650W

8. If we consider for calculation the source "FSP Dagger" the power value is 550W (it is the lowest in power of the examples). For the 550W source we apply the same calculation from figure 12, only we replace 130 kWh with 550 kWh and we get 11242 kWh.
9. The difference (Economy) of energy between laptop and computer is approximately  $11.242 - 2.657,2 = 8.584,8$  kWh
10. Let's think about the following 2 aspects: from a personal point of view if you buy a laptop you will have an electricity saving after 7 years of use of 8584.8 kWh! If you multiply this value by the price of one kWh, what money savings do you get after 7 years of use?
11. From a global point of view various sources are used to obtain electricity, such as wind power, caloric power, hydroelectric energy, etc. If for a single computer you get such an energy saving, then calculated, suppose for 1000 computers of the same electrical power, how many natural resources are saved? But for 1,000,000 computers? So in the future, when you will buy a computer, you can also think about at the aspect of environmental protection.
12. And now at the end, a little exercise for you. If we had to choose the most powerful source from those exemplified by 750W, how much energy would have been consumed in 7 years in addition to the laptop? Can you do this calculation?

## Step 2: Electronics recycling

Hypothetically create a scenario where, in the night you go with a flashlight. At some point, it is assumed that there is a need to replace the battery in the flashlight with a new charged one. If that battery is accidentally thrown somewhere in nature, the battery will not dissolve like biodegradable substances, it will exist where it was thrown for a long time. In addition, acidic and toxic substances from battery can leak and contaminate the area where it was dumped, enter the groundwater and contaminate water, etc. If we think globally, and not just on this battery, there are thousands of tons of electrical waste that if not recycled, can contaminate the environment. For this reason, it is necessary to recycle electrical waste, and there is legislation related to this aspect.

How can you help?

If do you have electrical equipment that you are going to throw away (Ex: an old and rusty computer or discharged batteries), throw this waste in the collection centers for recycling! In this way you can protect the environment!

OR: if you do not want to throw away those old equipment and you want to have a small income from them (suppose an old computer) and you intend to buy a new one there are government programs (In Romania, for

example, it is the Scrap Program for home appliances) to stimulate to renew equipment with more economical ones and at the same time the old ones are recycled.

OR: there are merchants, who in exchange for the old equipment, offer a discount when purchasing another new equipment from the same field. These are BUY-BACK type offers that have the same effect for recycling electronic equipment and be more energy efficiency.

And finally, a little exercise for you: do you have an old computer that you would like to change it (not now, in the future)? If so, try to find on the internet, which merchants can offer you BUY-BACK solutions?

**Congratulations, you have now completed Module 4.**

**Do not forget to check the Annexes for additional resources and documents  
provided to support self-study!**



## Module 5: Problem solving

The "Problem Solving" module is intended for those interested in identifying and solving the most common hardware and software problems, as well as a secure way to select and purchase the tools needed to solve everyday problems using digital means.

Please note that practical activities described in each unit might entail the support of an experienced trainer. Although the information presented in the manual is written in a way that is easy to understand, some actions, adjacent to the information presented, may require the support of experienced people.




Module 5	Problem solving			
Duration	25h			
Objectives	 Being able to solve common and simple technical ICT problems.  Being able to search, find and choose the proper solution for a certain ICT issue.  Being able to develop themselves and stay in contact with ICT development.			
Units	5.1 Solving technical problems	5.2 Identifying needs and technological responses	5.3 Creatively using digital technologies	5.4 Identifying digital competence gaps
Training organization	Face-to-face E-Learning	Face-to-face E-Learning	Face-to-face E-Learning	Face-to-face E-Learning
Duration	7h	7h	6h	5h

Table 26 - Global structure of the Module 5 – Problem solving.



## 5.1 Solving technical problems


Unit 5.1	Solving technical problems
Duration	7h
Objectives	To be able to solve Internet speed related problems
Content	5.1.1 Computers and its systems 5.1.2 Most common technical problems 5.1.3 Practical activities
Resources	Training manual Computer with internet connection Modem
Training methodologies	 Presentation by trainer

Table 27 - Structure of the unit of competence 5.1. – Solving technical problems of the Module 5 – Problem Solving.

### 5.1.1 Computers and its systems

The "Problem Solving" module is intended for those interested in identifying and solving the most common hardware and software problems, as well as a secure way to select and purchase the tools needed to solve everyday problems using digital means.

#### What is a computer?

A computer is an electronic device that manipulates information, or data. It has the ability to store, retrieve, and process data. You may already know that you can use a computer to type documents, send email, play games, and browse the Web. You can also use it to edit or create spreadsheets, presentations, and even videos.

#### What are the different types of computers?

When most people hear the word **computer**, they think of a **personal computer** such as a **desktop** or **laptop**. However, computers come in many shapes and sizes, and they perform many different functions in our daily lives

Many of today's electronics are basically specialized computers, though we don't always think of them that way. Here are a few common examples:

**Tablet computers or tablets**—are handheld computers that are even more portable than laptops. Instead of a keyboard and mouse, tablets use a touch-sensitive screen for typing and navigation. The iPad is an example of a tablet.

**Smartphones** – Many cell phones can do a lot of things computers can do, including browsing the Internet and playing games. They are often called smartphones and for many people, a smartphone can actually replace electronics like an old laptop, digital music player, and digital camera in the same device.

## Hardware vs. software

Before we talk about different types of computers, let's talk about two things all computers have in common: **hardware** and **software**.

- **Hardware** is any part of your computer that has a **physical structure**, such as the keyboard or mouse. It also includes all of the computer's internal parts
- **Software** is any **set of instructions** that tells the hardware **what to do** and **how to do it**. Examples of software include web browsers, games, and word processors

## What is an operating system (OS)?

An operating system is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of its software and hardware. It also allows you to communicate with the computer without knowing how to speak the computer's language. Without an operating system, a computer is useless. (Ex. of operating systems: Windows, Linux, macOS are used for desktops and laptops; Google Android and Apple iOS are used for tablets and smartphones)

## What is an application?

You may have heard people talking about using a program, an application, or an app but what exactly does that mean? Simply put, an app is a type of software that allows you to perform specific tasks. Applications for desktop or laptop computers are sometimes called desktop applications, while those for mobile devices are called mobile apps.

If you are regularly using computers in your day-to-day life, you will eventually run into some technical problems that need your attention. Although most complex computer issues can often be solved by a specialized technician, there are many other small, but common, issues that occur on a regular basis on a computer and its usage in a digital environment. The good news is that many problems with computers have simple solutions, and learning to recognize a problem and fix it yourself will save you a lot of time and money.

## 5.1.2 Most common technical problems

### 1. The Computer Won't Start

A computer that suddenly shuts off or has difficulty starting up could have a failing power supply. Check that the computer is plugged into the power point properly and, if that does not work, test the power point with another working device to confirm whether or not there is adequate power.

### 2. The Screen is Blank

If the computer is on but the screen is blank, there may be an issue with the connection between the computer and the screen. First, check to see if the monitor is plugged into a power point and that the connection between the monitor and computer hard drive is secure. If the problem is on a laptop, then you may need to get a professional to fix it as some of the internal wires may be worn.

### 3. Abnormally Functioning Operating System or Software

If the operating system or other software is either unresponsive or is acting up, then try restarting your computer and run a virus scan. To avoid having this happen, install reliable anti-virus software.

### 4. Windows Won't Boot

If you are having troubles booting Windows, then you may have to reinstall it with the Windows recovery disk.

### 5. The Screen is Frozen

When your computer freezes, you may have no other option than to reboot and risk losing any unsaved work. Freezes can be a sign of insufficient ram, registry conflicts, corrupt or missing files, or spyware. Press and hold the power button until the computer turns off, then restart it and get to work cleaning up the system so that it does not freeze again.

### 6. Computer is Slow

If your computer is slower than normal, you can often fix the problem simply by cleaning the hard disk of unwanted files. You can also install a firewall, anti-virus and anti-spyware tools, and schedule regular registry scans. External hard drives are great storage solutions for overtaxed CPU's, and will help your computer run faster.

### 7. Strange Noises

A lot of noise coming from your computer is generally a sign of either hardware malfunction or a noisy fan. Hard drives often make noise just before they fail, so you may want to back up information just in case, and fans are very easy to replace.

### 8. Slow Internet

To improve your Internet browser performance, you need to clear cookies and Internet temporary files frequently. In the Windows search bar, type '%temp%' and hit enter to open the temporary files folder.

### 9. PC Overheating

If a computer case lacks a sufficient cooling system, then the computer's components may start to generate excess heat during operation. To avoid your computer burning itself out, turn it off and let it rest if it is getting hot. Additionally, you can check the fan to make sure it is working properly.

### 10. Dropped Internet Connections

Dropped Internet connections can be very frustrating. Often the problem is simple and may be caused by a bad cable or phone line, which is easy to fix. More serious problems include viruses, a bad network card or modem, or a problem with the driver.

### 11. Your smartphone is running slowly

This is the most common smartphone problem, especially occurs as your phone gets older. The reason behind the slow speed is the installation of unnecessary apps that use your device's RAM and save numerous numbers of files in your phone.

Wipe out all the unnecessary apps and files from the mobile, clean up cache data. You can do this by diagnostic app also. If still, you face this issue, restore it to factory data.

### 12. Poor Battery Life

Unfortunately, this phone problem happens to everyone. The common problems are battery draining, slow charging or charging failure. We are glued to our phone so battery draining problem is the common issue. This major issue is when your phone is discharging without being utilized.

Find out that if any particular apps are draining too much battery, you can check this in Settings->Battery, and if you identify any bug, remove those apps. Enable the battery saving mode, turn off the locations, dim the brightness.

### 13. Storage Space

Most of the smartphone storage is filled with photos and videos. You should take care of the storage when you buy a new smartphone because, after a couple of days, you start panicking for the low storage. Very few smartphones have an expandable memory feature nowadays.

Delete the cache first. Use apps like cache cleaner which lets you clean cache for a specific app. Uninstall apps or move apps from the phone. Transfer the images on clouds to free up the space on your device.

### 14. Phone or App Crashes

This happens when there is a bug in the installed apps or your phone is running out of space. This is one of the frustrating mobile phone problems.

Clear the app data from "App manager". Avoid using multiple apps at same time. Troubleshoot your phone by restarting the device, remove the battery or restore it to factory settings.

### 15. Smartphone Overheating

Excess usage of smartphone brings overheating problem. Demanding apps, more likely gaming apps makes the temperature high of your phone which can affect the performance of the battery. Maybe you have downloaded malicious apps that run in the background.

Try not to use your phone while on charge. Do not use high CPU sucking apps, and give a break to your phone. If still, your phone is heating, this is the manufacturer defect.

### 16. Connecting problem with Bluetooth, wifi, cellular network

This is the temporary mobile phone problem which can easily get solved. Keep the phone on airplane mode for 30 to 60 seconds and try to reconnect it. Still having an issue? Repair or change the setting of Bluetooth and WiFi again.

### 17. Apps not downloading

The main cause of this problem is corrupt cache. Go to the google play store app and clear the cache of the app. Better to delete the history of google play store. Make sure you are using the latest version of google play store. If there is still an issue, clear data, and cache on google play services.

### 18. Synchronization Issue

The sync problem gets resolved automatically after some time. If not, remove the google account and add it again. Make sure your internet connection is not limited and working properly. Check for the system update and update it if required.

### 19. MicroSD Card Not Working On Your Smartphone

It can be caused when your SD card has bad read/write errors. Your mobile is not recognizing the SD card after formatting. Check the capacity of memory card, and format it to exFAT if it is up to 32GB. Restart the phone in recovery mode and select wipe cache in Android. This will clear out the SD card and format it to FAT32 which is best suited for storing in a phone.

### 20. Cracked Screen or Immersion in Water

This mobile phone problem accidentally happens and we cannot do anything in this. To avoid such incidents, use the good phone protector. Yes, they may be expensive but it is a worthy investment to avoid these accidents.

A computer is an electronic device that manipulates information, or data. It has the ability to store, retrieve, and process data. You may already know that you can use a computer to type documents, send email, play games, and browse the Web. You can also use it to edit or create spreadsheets, presentations, and even videos.



## 5.1.2 Practical Activities

### Step 1: Restart your modem and your wireless devices

Once you have connected your modem and set up your home network, both your wired and wireless Internet connections should be reliable, every day. Slow speeds and disconnections can result from weak signals, old equipment or cables, interference, device capabilities/limitations, and possibly third party related issues. If you think there is an issue with your WiFi, try the easy solutions outlined below to solve the most common issues.

A simple restart of your modem can fix many WiFi or connection issues

1. Unplug the power cable from the back of the WiFi modem or from the wall outlet.
2. Wait 30 seconds.
3. Reconnect the power cable to the modem.

Within a few minutes, your WiFi network should reappear in the list of available networks on your wireless devices. Try connecting a device to WiFi to see if it works.

Restarting your wireless devices also may be the solution to many common problems, including lags or loss of internet access. See your device manual on how to perform a standard restart.

### Step 2: Modem placement and coverage

The location of your modem in your home plays a significant role on your WiFi coverage and is a key factor for a stable WiFi connection. For better WiFi coverage, your modem should be placed in a central location, this works especially well if you have an open floor plan house. Alternatively, placing your modem central to where the Internet is most often used is a good choice as well. Ensure you are placing your modem

- ✓ Out in the open
- ✓ Raised off the ground

Avoid placing your modem

- ✗ In basements
- ✗ In cabinets
- ✗ Behind other objects

To avoid interference, try to keep your modem away from

- ✗ Household appliances

- ✗ Metal objects
- ✗ Electrical equipment

### Step 3: Check your connections

Loose connections, damaged cables, and line splitters can degrade Internet signals before they even reach your modem and prevent you from reaching higher Internet speeds. To resolve this, you should ensure that your cables are properly connected.

1. Unplug the power cable from the back of the modem.
2. Unscrew the coaxial cable from the back of the modem.
3. Inspect the coaxial cable for bends or kinks that indicate damage.
4. Follow the coaxial cable to the cable jack on the wall.
5. Determine if the coaxial cable goes into the jack directly, or if it passes through other devices, such as a splitter.
6. If a splitter is present, temporarily remove the splitter so the coaxial line can connect the cable jack to the modem directly.
7. Reconnect the coaxial and power cables to the back of your modem.
8. Wait for the modem to come back online.

If you are using an Ethernet cable to connect your computer to the router, or your modem to a third-party router, inspect those cables as well and replace them if they appear damaged.

### Step 4: Restore modem settings

In some rare circumstances, it might help to restore your modem to its factory settings as a last resort, which will reset any custom settings you may have setup, including your Wi-Fi network name and password to their defaults, found on the sticker on your modem.

To restore your modem:

1. Locate the small pinhole reset button of your modem.
2. Push and hold the button with a paperclip or pin for 15 seconds.
3. Watch the modem lights flash, and then after a few moments, remain lit.

Within a few minutes, your Wi-Fi network should reappear in the list of available networks on your wireless devices. Try connecting a device to Wi-Fi to see if it works.

## 5.2 Identifying needs and technological responses

Unit 5.2	Identifying needs and technological responses
Duration	7h
Objectives	Being able to solve common and simple technical ICT problems.
Content	5.2.1 Identifying needs and technological responses 5.2.2 Practical activities
Resources	Training manual Computers with internet access
Training methodologies	Presentation by trainer

Table 28 - Structure of the unit of competence 5.2. – Identifying needs and technological responses of the Module 5 – Problem Solving.

### 5.2.1 Identifying needs and technological responses

The first step when it comes to solve any computing problem is find out which component is not working correctly. Sometimes it is due to something simple such as the audio is not working, or we cannot properly see the screen or keyboard/mouse have stopped working. Other times the computer does not even start, it suddenly restarts or turns off and we do not know what is happening. In order to identify the problem, we have to pay attention to the clues that the computer gives us.

There are many different things that could cause a problem with your computer. No matter what's causing the issue, troubleshooting will always be a process of trial and error, in some cases, you may need to use several different approaches before you can find a solution; other problems may be easy to fix. We recommend starting by using the following tips.



**Write down your steps:** Once you start troubleshooting, you may want to write down each step you take. This way, you will be able to remember exactly what you have done and can avoid repeating the same mistakes. If you end up asking other people for help, it will be much easier if they know exactly what you have tried already.



**Take notes about error messages:** If your computer gives you an error message, be sure to write down as much information as possible. You may be able to use this information later to find out if other people are having the same error.



**Always check the cables:** If you are having trouble with a specific piece of computer hardware, such as your monitor or keyboard, an easy first step is to check all related cables to make sure they are properly connected.





**Restart the computer:** When all else fails, restarting the computer is a good thing to try. This can solve a lot of basic issues you may experience with your computer.



**Using the process of elimination:** If you are having an issue with your computer, you may be able to find out what is wrong using the process of elimination. This means you will make a list of things that could be causing the problem and then test them out one by one to eliminate them. Once you have identified the source of your computer issue, it will be easier to find a solution.

## Search on the internet

You can find some workaround through thousands of video tutorials on YouTube or from online sources that provide step-by-step instructions on computer troubleshooting.

### What is a video tutorial?

It is a video guide on how to solve a specific problem.

### What is the purpose of video tutorial?

Video tutorials offer a multidimensional experience that may combine charts, slides, photos, graphics, narration, screenshots, on-screen captions, music and live video. This allows students with different learning abilities to retain information in a method more suited to them.

For example, if you want to install a printer you can type on a search engine “**printer installation tutorial**”. One of the results is a video named: **Set up or Install a Printer on Windows 10 | How-To** <https://www.youtube.com/watch?v=E83yneh4xCA>, click on it and follow step-by-step the information about printer installation.

**Online sources:** Websites which can provide you the proper know-how in computer troubleshooting and tech support.

Example: [Bleeping Computer](http://www.bleepingcomputer.com): <http://www.bleepingcomputer.com>

The site is an excellent source of information, advice, and tutorials on computer software and hardware, troubleshooting, and security, to name a few. It has a searchable database of articles that is updated monthly by its stable of regular contributors.



## Examples of Hardware Needs:



**Web camera:** A webcam is a video camera that feeds or streams an image or video in real time to or through a computer network, such as the Internet. Webcams are typically small cameras that sit on a desk, attach to a user's monitor, or are built into the hardware.



**Printer:** a machine for printing text or pictures, especially one linked to a computer.



**Scanner:** a device that scans documents and converts them into digital data.



**Microphone:** A microphone (mic for short) is an electronic device that converts audio waves into electronic signals, which is then taken by the computer as an input. In desktops, it is much like any other peripheral device and is usually connected separately.



**Audio Speakers:** Speakers are transducers that convert electromagnetic waves into sound waves. The speakers receive audio input from a device such as a computer or an audio receiver. ... The sound produced by speakers is defined by frequency and amplitude. The frequency determines how high or low the pitch of the sound is.



**Smartphone camera:** Smartphones that are camera phones may run mobile applications to add capabilities such as geotagging and image stitching. ... Starting in the mid-2010s, some advanced camera phones feature optical image stabilization (OIS), larger sensors, bright lenses, 4K video and even optical zoom.



**Ports and connections:** In computer hardware, a port serves as an interface between the computer and other computers or peripheral devices. In computer terms, a port generally refers to the part of a computing device available for connection to peripherals such as input and output devices.



**Wireless technology:** Wireless technology provides the ability to communicate between two or more entities over distances without the use of wires or cables of any sort. Some of these terms may be familiar to you: radio and television broadcasting, radar communication, cellular communication, global position systems (GPS), Wi-Fi, Bluetooth and radio frequency identification are all examples of “wireless”, with wildly different uses in some cases.

## Examples of Software Needs:



**File extensions:** File extensions are a way of labelling the names of files so you and your computer can keep track of what they contain. ... The last part of the file name is used to indicate the type of file so the computer can open the correct program when you want to use the file.

Windows uses file extensions to determine how it opens different types of files. When a user double-clicks on a file to open it, Windows will open it with the application associated with that file's extension. The Windows system configuration maintains a list of applications and their associated file extensions. These are called "default programs." If a particular file extension is registered with a program, Windows will start that program whenever the user elects to open a file with that extension. Only one application, however, can be registered as the default program for each file extension. To use a program other than the default to open a file, right-click the file and choose "Open with."



**Update software:** Software updates are important because they often include critical patches to security holes. ... They can also improve the stability of your software, and remove outdated features. All of these updates are aimed at making the user experience better



**Antivirus install:** Antivirus software helps protect your computer against malware and cybercriminals. Antivirus software looks at data — web pages, files, software, applications — traveling over the network to your devices. ... It seeks to block or remove malware as quickly as possible.



**Display settings:** Your computer has a number of display settings that allow you to customize your viewing experience based on your activity. Your display settings are adjustable according to what you are using your computer for and what type of monitor you have

## 5.2.2 Practical Activities

### Step 1: Restart your phone

1. On most phones, press your phone's power button for about 30 seconds, or until your phone restart
2. On the screen, you might need to tap Restart .

### Step 2: Check for Android updates



Important: Settings can vary by phone.

1. Open your phone's Settings app.
2. Near the bottom, tap System > Advanced > System update. If needed, first tap About phone or About tablet.
3. Your update status will appear. Follow any steps on the screen.

### Step 3: Check storage & clear space

Your phone can start having issues when less than 10% of storage is free. If you are running low on storage, below you can find information on how to free up space.

#### Delete photos & videos



1. On your Android phone or tablet, open the Google Photos app .
2. Sign in to your Google Account.
3. Tap and hold a photo or video you want to move to the trash. You can select multiple items.
4. At the top, tap Trash .

On most phones, you can check how much storage you have available in the Settings app. Settings can vary by phone.

## Empty your trash



If you see a request to "Delete permanently" when you try to move an item to trash, your trash is full. Your trash can hold 1.5GB.

Important: If you empty your trash, you permanently delete any items in your trash.

1. On your Android phone or tablet, open the Google Photos app .
2. Sign in to your Google Account.
3. At the bottom, tap Library > Trash > More  > Empty Trash > Delete.

## Remove downloaded movies, music & other media

To delete content from Google Play:



1. Open the Google Play app with the content, like Play Music or Play Movies & TV.
2. Tap the Menu  > Settings > Manage downloads.
3. Tap Downloaded  > Remove.

To delete content from other sources, delete from the app that you used to download it.

## Step 4: Close apps that do not respond

Android manages the memory that apps use. You do not usually need to close apps but if an app is not responding, try closing the app.

## Step 5: Update de app

1. On your phone, open the Google Play Store app .
2. Tap Menu  > My apps & games.
3. Apps with available updates are labeled "Update."
  - If an update is available, tap Update.
  - If more updates are available, tap Update all.

## Step 6: Uninstall apps you do not use

Caution: Any data saved in this app will be erased.

1. Touch and hold the app that you want to uninstall.
2. To see your options, start dragging the app.
3. Drag the app to Uninstall at the top of the screen. If you do not see "Uninstall," you cannot uninstall the app.
4. Lift your finger.

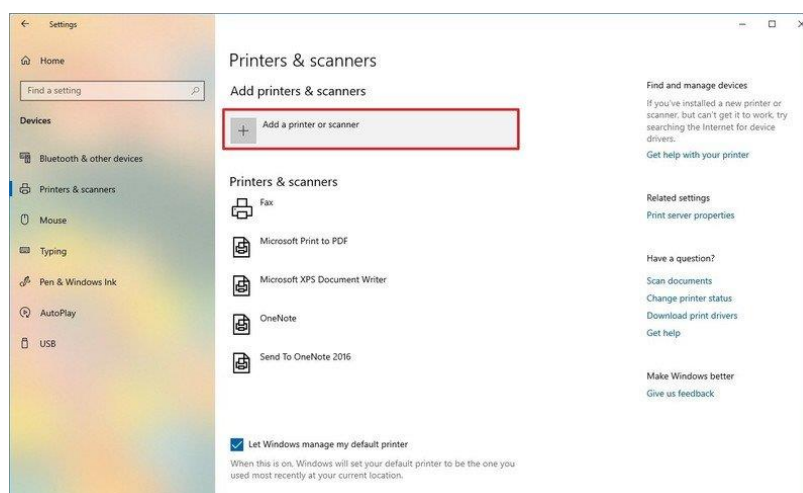
Tip: If you want to use the app again, you can try reinstalling it.

## Installing a local printer manually

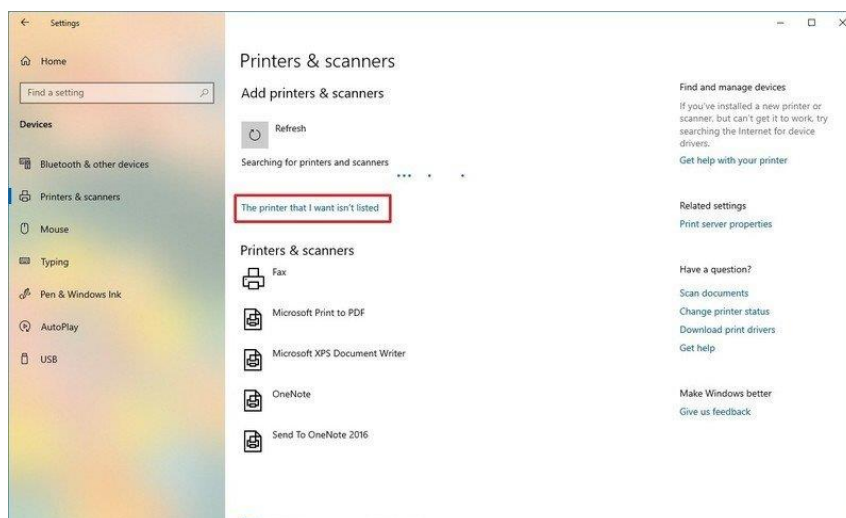
When the system is not detecting your printer automatically, you can still add the device manually depending on the connection type and age of the printer.

**Important:** Before proceeding, make sure that your computer is connected to the internet to allow Windows Update to download additional drivers.

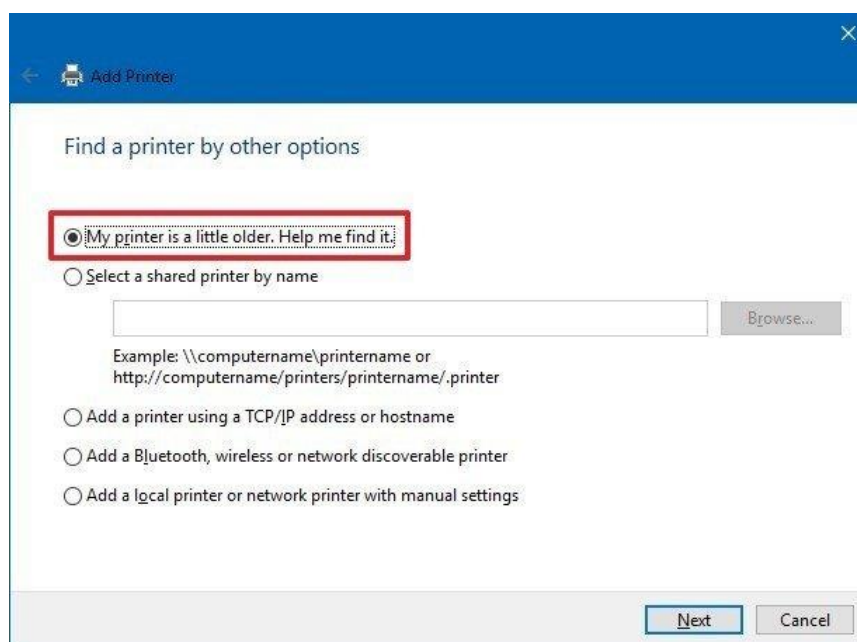
1. Open **Settings**.
2. Click on **Devices**.
3. Click on **Printers & scanners**.
4. Click the **Add a printer or scanner** button.



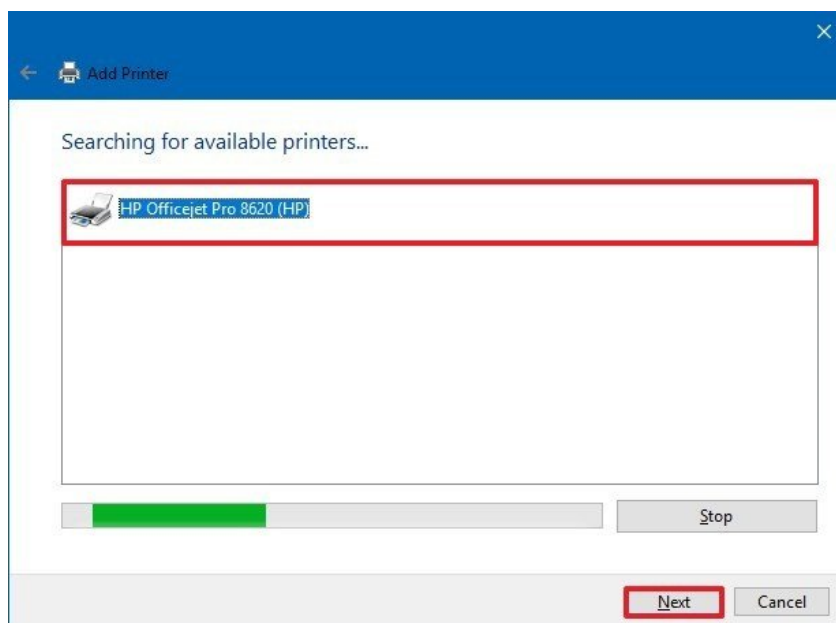
5. Wait a few moments.
6. Click **The printer that I want is not listed** option.



7. Select the **My printer is a little older. Help me find it** option.

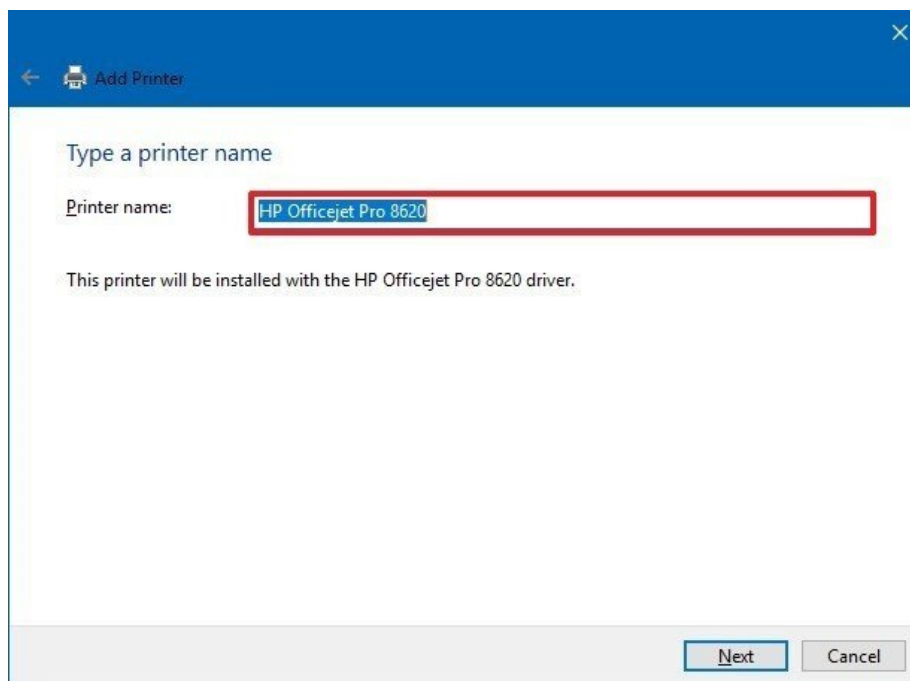


8. Select your printer from the list.
9. Click the **Next** button.



10. Type a name for the printer.

11. Click the **Next** button.



12. Select the **Do not share this printer** option.

13. Click the **Next** button.



← Add Printer

### Printer Sharing

If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.

☒ Do not share this printer

☐ Share this printer so that others on your network can find and use it

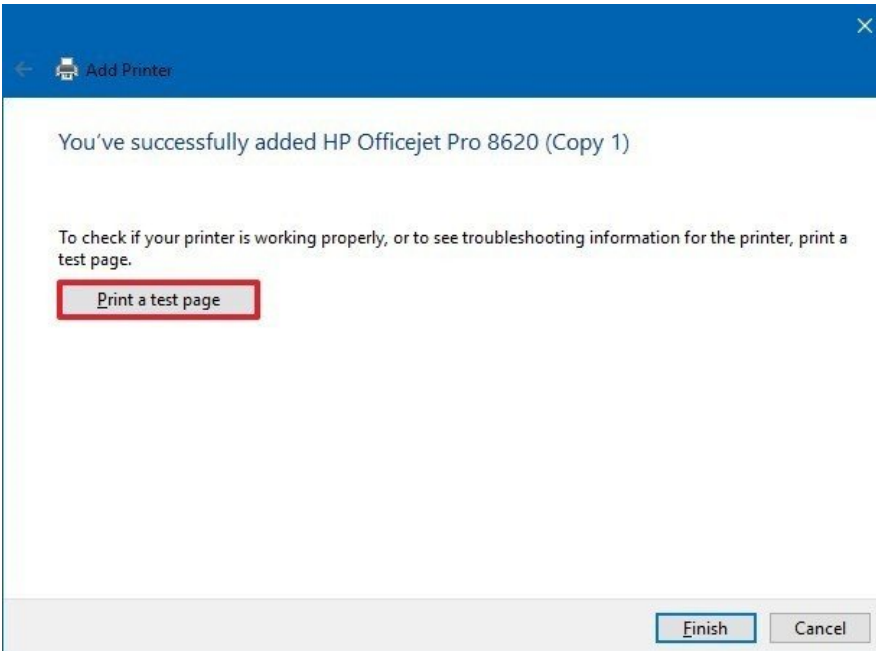
Share name: HP Officejet Pro 8620

Location:

Comment:

Next Cancel

14. Click the **Print a test page** option to confirm that the device is working.



← Add Printer

You've successfully added HP Officejet Pro 8620 (Copy 1)

To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.

Print a test page

Finish Cancel

15. Click the **Finish** button.

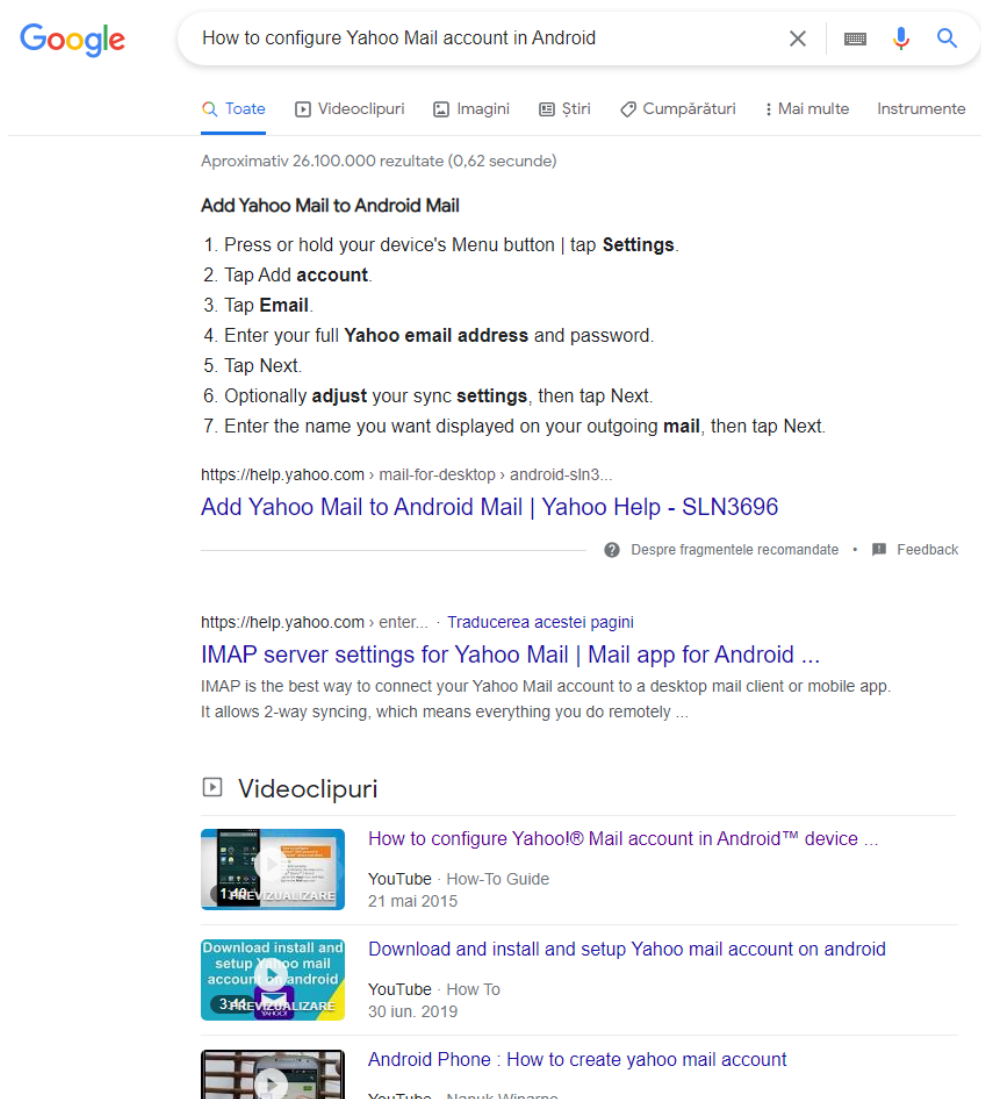
Once you have completed the steps, you should be able to start printing to the device.



## How to configure Yahoo!® Mail account in Android™ device mail client

Do you want to check your Yahoo!® Mail account emails on your Android™ device? If you want to configure Yahoo!® Mail account in your smartphone device mail client, you can use a video tutorial to help you solve this situation.

1. Open a browser page and type the name of a search engine Ex. Google.
2. On the bar of Google search engine type “How to configure Yahoo Mail account in Android”.
3. Many results will appear on screen. Pick one of the video results of the search criteria a double click on it. Ex. First video :( <https://www.youtube.com/watch?v=C0KxJ-T7rRw>)



The screenshot shows a Google search page with the query "How to configure Yahoo Mail account in Android". The search results include a text-based link to a Yahoo Help article titled "Add Yahoo Mail to Android Mail" and a section for video results. The video results list three YouTube videos: "How to configure Yahoo!® Mail account in Android™ device ...", "Download and install and setup Yahoo mail account on android", and "Android Phone : How to create yahoo mail account".

4. Watch this video and follow the steps to do so.

Ask audience to give example of needs and repeat the search for tutorials accordingly to their responses.

## 5.3 Creatively using digital technologies





Unit 5.3	Creatively using digital technologies
Duration	6h
Objectives	 Understand and explore creative digital technologies
Content	5.3.1 Digital creativity 5.3.2 Practical activities
Resources	Training manual Computers with internet access
Training methodologies	 Presentation by trainer  Group exercise Discussion / Debate  Working in pairs / Small groups

Table 29 - Structure of the unit of competence 5.3. – Creatively using digital technologies of the Module 5 – Problem Solving.

### 5.3.1 Digital Creativity

Creativity is quickly becoming one of the most highly valued traits of the 21st century, and according to a 2016 report from the World Economic Forum, it is one of the top three skills employers will be looking for by 2020. A survey by IBM also found that 60% of CEOs believe creativity is the most important leadership quality today.

Digital Creativity is a new, dynamic, inter-disciplinary and rapidly growing field. While there is a growing clarity as to what creativity is the meaning of digital expands on a daily basis. Unsurprisingly digital creativity can mean many things to different in business, the third sector, in education and in informal learning.

New hardware/software is undoubtedly allowing young people to engage with the world, often playfully and experimentally, in ways which they could not have done even ten years ago. Certainly digital creativity is astonishingly fast and, in all likelihood, is more than the sum of digital + creativity.

## Digital Creativity examples:



**Text processing.** In computing, the term **text processing** refers to the theory and practice of automating the creation or manipulation of electronic **text**. ... The term **processing** refers to automated (or mechanized) **processing**, as opposed to the same manipulation done manually.



**Media editing.** Editing is the process of selecting and preparing written, photographic, visual, audible, or cinematic material used by a person or an entity to convey a message or information.



**Designing presentations.** What is **presentation design**? **Presentation designers** craft an array of ideas, stories, words, and images into a set of **slides** that are arranged to tell a story and persuade an audience.



**Email.** **Email** is a system of sending written messages electronically from one computer to another. **Email** is an abbreviation of '**electronic mail**'.



**Social media.** Social media is a computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. By design, social media is Internet-based and gives users quick electronic communication of content.



**Data visualization.** Data visualization is the graphical representation of information and **data**. By using visual elements like charts, graphs, and maps, **data visualization** tools provide an accessible way to see and understand trends, outliers, and patterns in **data**.

## Digital creativity tools



**Calendars:** A **digital calendar** lets you go out as far as you need to, see the recurring events you will have, and schedule something for 2031 as though it were next week. You always have it with you. Probably. As wonderful as a paper planner is, it is one more thing to carry with you.



**Photo editing app:** An **image editing** application for digital photos. It is used to crop and touch up photos, as well as organize them into albums and slide shows. **Photo** editors typically do not have the myriad filters and features of a full-blown **image editor** such as Adobe's Photoshop or Corel's Paint Shop Pro.



**Text editing app:** A **text editor** is a type of computer program that edits plain **text**. **Text** editors are provided with operating systems and software development packages, and can be used to change files such as configuration files, documentation files and programming language source code.



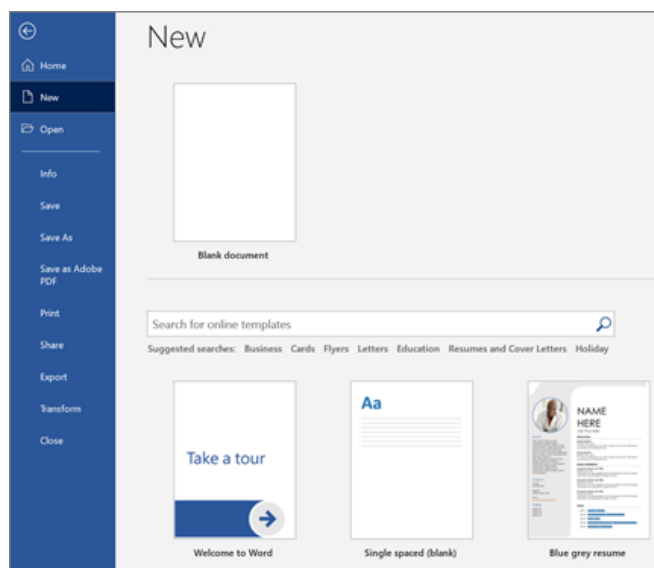
**Social media app:** **Social media** apps are applications which can either be downloaded and stored on your phone or tablet, or streamed through your internet browser. Social media apps generally involve messaging, photo-sharing and interactive content. Facebook, Instagram, Twitter.

## 5.3.2 Practical Activities

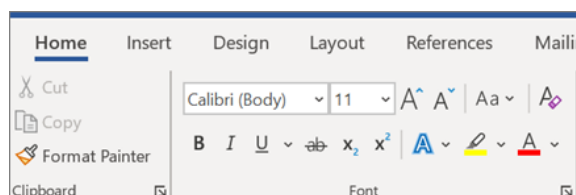
## Step 1: Create a document

1. Open a text app ex. Ms Word.
2. On the File tab, click New.
3. In the Search for online templates box, enter the type of document you want to create and press ENTER.

Tip: To start from scratch, select Blank document or for practice using Word features, try a learning guide like Welcome to Word, Insert your first table of contents, and more.



4. Add and format text
  1. Place the cursor and type some text.
  2. To format, select the text and then select an option: Bold, Italic, Bullets, Numbering, and more.



5. Add Pictures, Shapes, SmartArt, Chart, and more

1. Select the Insert tab.
2. Select what you want to add:
  - Tables - select Tables, hover over the size you want, and select it.

- Pictures - select Pictures, browse for the picture you want, and select Insert.
- Online Pictures - select Online Pictures, search and choose the picture you want, and select Insert.
- Shapes - select Shapes, and then select a shape from the drop-down.
- Icons - select Icons, choose the one you want, and select Insert.
- 3D Models - select 3D Models, choose from a file or online source, go to the image you want, and select Insert.
- SmartArt - select SmartArt, choose a SmartArt Graphic, and select OK.
- Chart - select Chart, select the chart you want, and select OK.
- Screenshot - select Screenshot and select one from the drop-down.

#### 6. Print a document in Word

1. Click File > Print.
2. To preview each page, click the forward and backward arrows at the bottom of the page. If the text is too small to read, use the zoom slider at the bottom of the page to enlarge it.
3. Choose the number of copies, and any other options you want, and click the Print button.

### Step 2: Create a post on social media

Follow the next steps to create a post on Facebook, both in the mobile app and on the Facebook website. Posts can contain text, photos, videos, and location data. You can post on your own page, a friend's page, or on the page of a group that you are a part of.

1. Open Facebook. The Facebook app icon looks like a white "f" on a dark-blue background. Facebook will open to your News Feed if you are already logged in.

If you are not already logged in, enter your email address (or phone number) and password, then tap Log in.

2. Go to the page where you want to post. Depending on where you want to create your post, this will vary:

- Your page - You can create a post for your page from the top of the News Feed.
- A friend's page - Tap the search bar at the top of the screen, type in a friend's name, tap their name, then tap their profile image.
- A group - Tap ≡, tap Groups, tap the Groups tab, and tap your group.

3. Tap the post box. This box is at the top of the News Feed. If you are posting to a friend's page, it is below the photo section that is near the top of their page. If you are posting to a group, you will find the box just below the cover photo.

- There will generally be a phrase like "Write something" or "What's on your mind?" in the box.

4. Upload a photo or a video. Tap Photo/Video near the middle of the post screen, then select a photo or video to upload and tap Done. Doing so adds the photo or video to your post.

- You can tap multiple photos or videos to upload them all at once.
- Skip this step if you want to upload a text-only post.

5. Add text to your post. Tap the text field, then type in the text for your post.

- You can also tap a colored circle along the middle of the screen to set a background for your post. You can only add color to posts with 130 characters or fewer.

6. Tap Add to your post. It is in the middle of the screen. This will bring up the following post options:

- Photo/Video - Add more photos or videos.
- Check In - Allows you to add an address or location to your post.
- Feeling/Activity/Sticker - Lets you add an emotion, activity, or emoji.
- Tag People - Allows you to add a person to this post. Doing so puts the post on their page as well.

7. Select a post option to add more to the post. This is completely optional. If you do not want to add more to the post, skip to the next step.

8. Tap Post. It is in the top-right corner of the screen. Doing so will create your post and add it to the page you are on.

## 5.4 Identifying digital competence gaps




Unit 5.4	Identifying digital competence gaps
Duration	5h
Objectives	 Being able to use technologies to interact with others
Content	5.4.1 The digital skills gap in Europe 5.4.2 Practical activities
Resources	Training manual Computer with internet access
Training methodologies	 Presentation by trainer  Working in pairs / Small groups

Table 30 - Structure of the unit of competence 5.4. – Identifying digital competences gaps of the Module 5 – Problem Solving

### 5.4.1 The Digital Skills Gap in Europe

Digital technologies are used in many sectors such as farming, healthcare, transport, education, retail, automatics, energy, shipping, logistics, teaching and the information and communications technology industry. The demand for information and communications technology specialists is growing fast. In the future, 9 out of 10 jobs will require digital skills. At the same time, 169 million Europeans between 16 and 74 years – 44% – do not have basic digital skills

**Like anything, if you want to grow in this field, you must continue to learn.**

Students will be able to find out what improvements they will have to make to acquire or improve the skills and competencies needed to perform as good as possible in their (future) role. Eventually, this will also have a positive impact on your daily life.

1. **Invest in education.** Sites like Udemy and Skillshare have some brilliant courses on a whole host of digital topics. From [SEO](#) and Google Analytics to Social Media and Content Marketing, you will be sure to find something in the area you are looking to learn more about. Always be sure to check out the reviews before purchasing a course and have a look how long it will take to complete. Some courses can be completed in a day whereas others will require more time.
2. **Hit subscribe.** When you come across a really useful article, hit subscribe on the website to receive future newsletters. It is worth it when the content really stands out to you as, chances are, future articles will be just as helpful.

Be sure to do this selectively though, as the last thing you want is to be bombarded. By filtering out the superior content, you will know when an email lands in your inbox, it is worth a read.

3. **Join groups.** Communities, forums and online groups can be a great resource for staying up to date in this field. Learn from others and share your experience in ongoing conversations. Just be sure to proceed with caution as some groups can contain a lot of spam and irrelevant information.

Search Facebook and LinkedIn for groups in your niche, whether that is digital marketing in general or something more specific such as e-commerce or social media. Remember, the more specific you are, the more relevant the conversations and posts will be.

4. **Get on board with Google Alerts.** This nifty tool is a great way of staying up to date with trends and tips. Simply let Google know the keywords you would like to be notified about when they appear in search results and you will be alerted with an email.

For example, when 'SEO trends 2019' appears, you will be sent an email with a link through to the corresponding site. This is a great way of staying updated on just about anything. Plus, you can limit the number of times Google emails, and have everything wrapped up in a weekly summary to avoid a daily bombardment.

5. **Head to YouTube.** Nowadays, there is a video on just about anything on YouTube. Yes, you do have to sift through sometimes to find the gems, but it can be well worth it. It can be the case that a concept you are struggling with can be easily solved in a matter of minutes when you land on an informative video.
6. **Use hashtags.** This is a great way to search recent trends, news and updates in any field. Just take a few minutes out when travelling on the train or during lunch to head to Twitter or LinkedIn and search a few hashtags. You will be able to navigate quickly to the top content under that hashtag and read the latest content. If you come across someone who shares regular updates in your niche, they are probably worth following.



## 5.4.2 Practical Activities

### Step 1: Subscribe to an YouTube channel

1. Go to <https://www.youtube.com> in a web browser. This opens the YouTube website.
2. Sign in to your account. You have to be signed in to a Google account to subscribe to YouTube channels. If you are not signed in, click the blue **"SIGN IN"** button at the top-right corner and then log in with your Google account.



If you are already signed in and want to switch accounts, click the profile photo at the top-right corner, select **Switch account**, and then choose another account from the list. If you do not see the account you want to use, click Add account to add or create another account.

3. Browse for a channel. You can check out what is **Trending** in the left panel, search for a particular channel, or find something new by searching for keywords.



If you know the name of the channel you want to subscribe to (or you want to search by keyword), type it into the search bar at the top of YouTube and press **Enter** or **Return**. To see just channels, click **Filter** at the top-left corner of the search results and select **Channels** under "Type."



You can also subscribe to a channel from any of the channel's videos. Type the name of a video into the search bar and press **Enter** or **Return**. Then, click a video to start watching it—the channel's name will appear below the video's title.

4. Click **SUBSCRIBE** to subscribe to a channel. It is a red-and-white button—if you are on the channel's home page, it will be near the top-right corner of the page below the cover image. If you have a video open, it is below the video to the right of the channel's name.



Now that you are subscribed, the text on the "SUBSCRIBE" button will turn gray and change to **SUBSCRIBED**. Clicking that button at any time will unsubscribe you from the channel.

5. View your subscriptions. Click the three horizontal lines at the top-left corner of YouTube to open the menu and select **Subscriptions** to see all of the channels you are subscribed to.



Your subscriptions appear under "SUBSCRIPTIONS" in the left panel.



Click one of your subscribed channels to view its most recent content.

6. Adjust your notification preferences. You will be notified of some channel updates by default. To receive more or fewer updates from a channel, click the channel, and then click the bell icon next to the "SUBSCRIBED" button. Then, click **All**, **None**, or **Personalized**. **Personalized** bases notifications on your activity.



To specify how you are notified of updates, click your profile photo at the top-right corner, select **Settings**, and then click **Notifications** in the left panel. Use the sliders to control which notifications you are notified about.

## Step 2: Join a group of interest on social media

1. Open Facebook. The Facebook mobile app icon is a white "f" on a dark-blue background. Facebook will open to your News Feed if you are already logged in.



If you are not already logged in, enter your email address (or phone number) and password, then tap Log in.

2. Tap the search bar. It is at the top of the screen. This will bring up your device's keyboard.

3. Enter a group name or keyword. Type in a group's name (or a word or phrase in which you are interested), then tap Search. This will search Facebook for accounts, pages, places, and groups that match your search.

4. Tap **Groups**. This is a tab near the top of the screen, just below the search bar. This will display any groups related to your search.



You may have to swipe the row of tabs here to the left to display the Groups option.

5. Tap **Join** next to a group. The Join button is on the right side of a group's name. Tapping it will cause a "Requested" stamp to appear to the right of the group. Once you are accepted into the group by an administrator, you will be able to post in the group.



If the group is public instead of closed, you will be able to see (but not interact with) the group's posts and members.

**Congratulations, you have now completed Module 5 and finished the course.**

**Do not forget to check the Annexes for additional resources and documents provided to support self-study! Well-done!**

# EVALUATION OF THE TRAINING



## 1. Evaluation of the learning

Within the methodology of the No One Behind project, the consortium developed the evaluation system that is duly introduced in the document *Innovative methodology for educating and training adults from rural zone to improve their digital and ICT skills*<sup>19</sup>. According with this system, for each unit of competence are defined the qualitative indicators to assess the domain of the competence of adult learners (Table):

M1 - Information and Data Literacy	
Browsing, searching and filtering data, information and digital content	<ul style="list-style-type: none"> <li>- Be able to identify different web browsers.</li> <li>- Be able to recognize different search engines.</li> <li>- Be able to search information and content online.</li> <li>- Be able to navigate between digital environments.</li> <li>- Be able to understand the risks of confidentiality and privacy of searching on the internet.</li> <li>- Be able to know the role of the internet in obtaining information in the context of today's world.</li> </ul>
Evaluating data, information and digital content	<ul style="list-style-type: none"> <li>- Be able to recognize the dangers of fake news and misinformation in the digital age.</li> <li>- Be able to identify the veracity of data and the accuracy of digital information.</li> <li>- Be able to detect the credibility and reliability of common sources of data, information and their digital content.</li> <li>- Be able to search for reliable and credible data and information.</li> </ul>
Managing data, information and digital content	<ul style="list-style-type: none"> <li>- Be able to identify different types of programmes, tools and environments to store and manage data, information and digital content.</li> <li>- Be able to use digital tools and platforms to store and manage data.</li> <li>- Be able to organize content and data in a digital platform in a structured way.</li> <li>- Be able to access digital environments defining adequate privacy settings.</li> </ul>
M2 - Communication and Collaboration	
Interacting through digital technologies	<ul style="list-style-type: none"> <li>- Be able to identify different digital tools, characterize them and use them in accordance with the context.</li> <li>- Be able to interact and communicate with different audiences using adequate digital tools and devices.</li> <li>- Be able to recognize and characterize different digital platforms and devices for communication.</li> <li>- Be able to search for information online in safe and ethically.</li> </ul>
Sharing through digital technologies	<ul style="list-style-type: none"> <li>- Be able to share information with others using adequate tools and/or platforms.</li> <li>- Be able to recognize and characterize different digital platforms and devices for sharing information.</li> <li>- Be able to share information with others in safe and ethically.</li> <li>- Be able to search for information online in safe and ethically.</li> </ul>
Engaging in citizenship through digital technologies	<ul style="list-style-type: none"> <li>- Be able to communicate online ethically and open-minded.</li> <li>- Be able to participate online in society as a citizen.</li> <li>- Be able to use legal online services.</li> </ul>

<sup>19</sup> Accessible [here](#).

	<ul style="list-style-type: none"> <li>- Be able to provide feedback and opinions with respect for others.</li> <li>- Be able to recognize information and interactive online services.</li> <li>- Be able to configure settings to keep information private.</li> </ul>
Collaborating through digital technologies	<ul style="list-style-type: none"> <li>- Be able to use different tools and platforms to communicate online with others.</li> <li>- Be able to share information online using appropriate tools and platforms.</li> <li>- Be able to identify the most used online platforms in their country or region.</li> <li>- Be able to distinguish between instant messaging or chat platforms, voice-over-IP, social media platforms, forums and e-mail.</li> </ul>
Netiquette	<ul style="list-style-type: none"> <li>- Be able to demonstrate polite interaction online with others.</li> <li>- Be able to identify what kind of behaviour should be used in different online environments (such as email, social media or chat).</li> <li>- Be able to apply “good manners” in an online environment communicating with others.</li> <li>- Be able to understand the importance of online rules when using digital resources.</li> </ul>
Managing digital identity	<ul style="list-style-type: none"> <li>- Be able to describe the concept of digital identity.</li> <li>- Be able to understand how to protect the digital identity.</li> <li>- Be able to describe simple ways to protect the reputation online.</li> <li>- Be able to manage the digital footprint.</li> <li>- Be able to know how to be respectful of the digital identities of others and careful about what to post about other people.</li> </ul>
<b>M3 - Digital content creation</b>	
Developing digital content	<ul style="list-style-type: none"> <li>- Be able to create and edit digital content in different formats.</li> <li>- Be able to create new, original content and knowledge.</li> <li>- Be able to represent well what it is intended to communicate.</li> <li>- Be able to identify the value of digital content as a visual aid.</li> <li>- Be able to adapt the expression through the creation of the most appropriate digital means.</li> </ul>
Integrating and re-elaborating digital content	<ul style="list-style-type: none"> <li>- Be able to modify information and content into an existing document or platform.</li> <li>- Be able to integrate new information and content into an existing document or platform.</li> <li>- Be able to assess the most appropriate ways to integrate specific new items of content and information.</li> </ul>
Copyright and licenses	<ul style="list-style-type: none"> <li>- Be able to apply copyright and licenses in an accurate way.</li> <li>- Be able to identify which licenses are required in certain circumstances.</li> <li>- Be able to know how to protect themselves against copyright infringement.</li> </ul>
Programming	<ul style="list-style-type: none"> <li>- Be able to list simple instructions for a computing system to solve a simple problem or perform a simple task.</li> <li>- Be able to solve simple technical issues.</li> <li>- Be able to apply instructions to perform tasks or solve problems..</li> </ul>
<b>M4 - Safety</b>	
Protecting devices	<ul style="list-style-type: none"> <li>- Be able to understand the importance of protecting devices and avoid risks.</li> <li>- Be able to identify the difference between different types of malware.</li> <li>- Be able to understand the importance of measures related to reliability and confidentiality.</li> </ul>
Protecting personal data and privacy	<ul style="list-style-type: none"> <li>- Be able to keep personal data protected.</li> <li>- Be able to understand the risk of identity theft.</li> <li>- Be able to apply “Privacy Policy” when using digital services.</li> <li>- Be able to understand the basic rules of security.</li> </ul>

Protecting health and well-being	<ul style="list-style-type: none"> <li>- Be able to avoid health risks and threats to physical and psychological well-being while using digital technologies.</li> <li>- Be able to control possible dangers and threats in digital environments.</li> <li>- Be able to identify the risks of misusing online and digital services.</li> </ul>
Protecting the environment	<ul style="list-style-type: none"> <li>- Be able to recognize simple environmental impacts of digital technologies and their use.</li> <li>- Be able to use digital services without being dependent on them.</li> <li>- Be able to protect the environment from the impact of disposing digital devices.</li> </ul>
<b>M5 - Problem Solving</b>	
Solving technical problems	<ul style="list-style-type: none"> <li>- Be able to navigate online in everyday contexts.</li> <li>- Be able to identify when a digital device is appropriate enough to work on.</li> <li>- Be able to identify when a problem has occurred on a digital device or service.</li> </ul>
Identifying needs and technological responses	<ul style="list-style-type: none"> <li>- Be able to recognize technical problems originating from a digital device or from the environment.</li> <li>- Be able to recognize solving methods.</li> <li>- Be able to understand how to use help facilities, manuals guides.</li> </ul>
Creatively using digital technologies	<ul style="list-style-type: none"> <li>- Be able to use the appropriate digital technology for a specific purpose (gather information, create content).</li> <li>- Be able to use components of digital systems and digital information in real-world conditions.</li> </ul>
Identifying digital competence gaps	<ul style="list-style-type: none"> <li>- Be able to evaluate himself or others if new digital environments are appropriate means of improving digital competence level.</li> <li>- Be able to seek opportunities for self-development and keep up to date with the digital evolution.</li> </ul>

Table 31 – Identification of the criteria of evidence of each unit of competence, for the assessment of the domain of the competence by adult learners.

These criteria of evidence should be used to assess the domain of the competence by learners and it can be assessed in two ways:



By adult educators or trainers through the observation of the performance of learners during the development of the proposed activities and at the end of the training by filling in an evaluation sheet.







By adult learners that assess their domain of the competence by filling in a self-assessment evaluation sheet, at the beginning and at the end of each module.

In both cases, it can be used the evaluation sheets provided in the [Annexes II to V](#).

## 2. Evaluation of the training

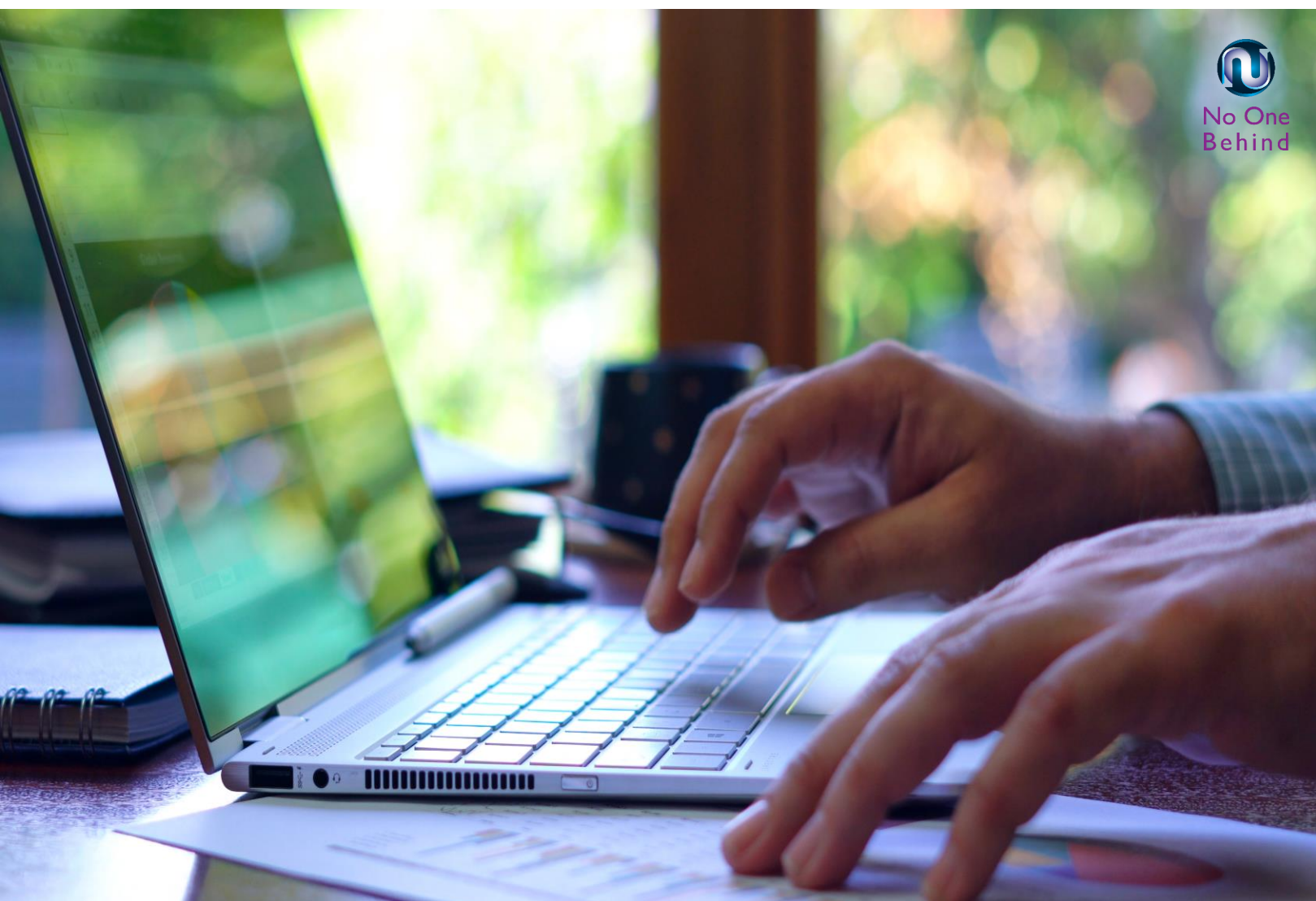
At the end of the training course, is foreseen the evaluation of it by learners who benefit from it. The evaluation of the training will allow to understand the:

-  adequacy and relevance of the training to the target groups defined
-  quality of the training curriculum in terms of contents and duration
-  value of the supports and materials provided
-  support provided during the training

This will be done through a questionnaire (Annex VI) that will be available online. We also recommend a debriefing moment, at the end of each module and at the end of the course where learners can find the space to talk about their learning experience, what they liked the most and the least, what were their main difficulties, how they plan to keep practicing what they learned in the course and so on.




















# ANNEXES




























## Annex I – Additional resources


Module	Unit	Resources
Module 1	1.1	 <b>IT online training</b> – <a href="https://edu.gcfglobal.org/en/subjects/tech/">https://edu.gcfglobal.org/en/subjects/tech/</a>  <b>Tutorial “Using search engines”</b> – <a href="https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/">https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/</a>  <b>How to search the internet effectively (1)</b> – <a href="https://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_How_Search_Internet_Effectively.pdf">https://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_How_Search_Internet_Effectively.pdf</a>  <b>How to search the internet effectively (2)</b> – <a href="https://mediasmarts.ca/sites/default/files/tipsheet/tipsheet_we_are_broadcasters.pdf">https://mediasmarts.ca/sites/default/files/tipsheet/tipsheet_we_are_broadcasters.pdf</a>
	1.2	 <b>Data protection</b> - <a href="https://ec.europa.eu/info/sites/default/files/charter-application_en.pdf">https://ec.europa.eu/info/sites/default/files/charter-application_en.pdf</a>  <b>How do fake news spread</b> - <a href="https://www.youtube.com/watch?v=cSKGa_7XJkg">https://www.youtube.com/watch?v=cSKGa_7XJkg</a>
Module 2	2.1	 <b>Basic Email Tutorial:</b> <a href="https://www.youtube.com/watch?v=cnxsl8h5gj4">https://www.youtube.com/watch?v=cnxsl8h5gj4</a>  <b>Using digital tools to transform classrooms:</b> <a href="https://www.youtube.com/watch?v=B99FXVamqMM">https://www.youtube.com/watch?v=B99FXVamqMM</a>  <b>What your Digital Communication Style Says about you:</b> <a href="https://www.webroot.com/us/en/resources/tips-articles/what-your-digital-communication-style-says-about-you">https://www.webroot.com/us/en/resources/tips-articles/what-your-digital-communication-style-says-about-you</a>
	2.2	 <b>Best lessons to share lesson notes digitally:</b> <a href="http://blog.whoosreading.org/digital-notes/">http://blog.whoosreading.org/digital-notes/</a>  <b>Digitally share and Comment:</b> <a href="https://applieddigitalskills.withgoogle.com/c/middle-and-high-school/en/create-a-presentation-all-about-a-topic/create-a-presentation-all-about-a-topic/digitally-share-and-comment.html">https://applieddigitalskills.withgoogle.com/c/middle-and-high-school/en/create-a-presentation-all-about-a-topic/create-a-presentation-all-about-a-topic/digitally-share-and-comment.html</a>
	2.3	 <b>Digital Citizenship:</b> <a href="https://education.microsoft.com/en-us/course/192d4b4a/overview">https://education.microsoft.com/en-us/course/192d4b4a/overview</a>  <a href="https://www.youtube.com/watch?v=ju9aOc2MLyo">https://www.youtube.com/watch?v=ju9aOc2MLyo</a>  <a href="https://www.youtube.com/watch?v=HIII6YjE2ds">https://www.youtube.com/watch?v=HIII6YjE2ds</a>  <a href="https://ikeepSAFE.org/content/uploads/2020/02/Class-2_Student_FINAL-1.pdf">https://ikeepSAFE.org/content/uploads/2020/02/Class-2_Student_FINAL-1.pdf</a>  <b>What is personal information:</b> <a href="https://www.common sense media.org/educators/lesson/keep-it-private-k-2">https://www.common sense media.org/educators/lesson/keep-it-private-k-2</a>  <b>Digital Citizenship and its teaching:</b> <a href="https://files.eric.ed.gov/fulltext/EJ1286737.pdf">https://files.eric.ed.gov/fulltext/EJ1286737.pdf</a>
	2.4	 <b>30 Of The Best Digital Collaboration Tools For Students -</b> <a href="https://www.teachthought.com/technology/12-tech-tools-for-student-to-student-digital-collaboration/">https://www.teachthought.com/technology/12-tech-tools-for-student-to-student-digital-collaboration/</a>  <b>Importance of Teamwork &amp; Collaboration in a Digital World</b> - <a href="https://blog.bit.ai/importance-of-teamwork-and-collaboration/">https://blog.bit.ai/importance-of-teamwork-and-collaboration/</a>  <b>Digital Collaboration Tool:</b> <a href="https://www.youtube.com/watch?v=TSz2CxnuGkQ">https://www.youtube.com/watch?v=TSz2CxnuGkQ</a>  <a href="https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework">https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework</a>  <a href="https://zapier.com/blog/dropbox-vs-google-drive/">https://zapier.com/blog/dropbox-vs-google-drive/</a>  <a href="https://support.google.com/a/users/answer/9302892?hl=en">https://support.google.com/a/users/answer/9302892?hl=en</a>  <a href="https://kissflow.com/project/best-project-management-tools/">https://kissflow.com/project/best-project-management-tools/</a>
	2.5	 <b>Netiquette meaning, definition &amp; explanation</b> - <a href="https://www.youtube.com/watch?v=7-HopTAFUm0">https://www.youtube.com/watch?v=7-HopTAFUm0</a>

### Digital Competent Citizen Training Manual


		 <b>Examples of bad netiquette</b> - <a href="https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette">https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette</a>  <b>Examples of good netiquette</b> - <a href="https://www.cybersmile.org/advice-help/category/examples-of-good-netiquette">https://www.cybersmile.org/advice-help/category/examples-of-good-netiquette</a>  <a href="https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework">https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework</a>  <a href="https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette">https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette</a>  <a href="https://slangit.com/meaning/keyboard_warrior">https://slangit.com/meaning/keyboard_warrior</a>
	2.6	 <b>Passwords: How to protect your digital assets -</b> <a href="https://www.funeralwise.com/learn/digitallegacy/how-to-manage-passwords/">https://www.funeralwise.com/learn/digitallegacy/how-to-manage-passwords/</a>  <b>The Digital Identity: What It Is + Why It's Valuable</b> - <a href="https://learn.g2.com/digital-identity">https://learn.g2.com/digital-identity</a>  <b>What is Digital Identity and How Does it Work</b> - <a href="https://www.techfunnel.com/information-technology/what-is-digital-identity/">https://www.techfunnel.com/information-technology/what-is-digital-identity/</a>  <a href="https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework">https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework</a>  <a href="https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/">https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/</a>  <a href="https://www.techrepublic.com/article/how-to-protect-yourself-and-your-organization-against-digital-identity-fraud/">https://www.techrepublic.com/article/how-to-protect-yourself-and-your-organization-against-digital-identity-fraud/</a>  <a href="https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message">https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message</a>
Module 5		 <a href="https://medium.com/beyond/6-ways-to-stay-on-top-of-emerging-technology-trends-ca6a7b27bc20">https://medium.com/beyond/6-ways-to-stay-on-top-of-emerging-technology-trends-ca6a7b27bc20</a>  <a href="https://www.imaginaire.co.uk/16-ways-to-stay-up-to-date-with-digital-marketing-trends-in-2019-our-guide-to-tips-and-resources">https://www.imaginaire.co.uk/16-ways-to-stay-up-to-date-with-digital-marketing-trends-in-2019-our-guide-to-tips-and-resources</a>  <a href="https://digital-strategy.ec.europa.eu/en/library/digital-skills-gap-europe">https://digital-strategy.ec.europa.eu/en/library/digital-skills-gap-europe</a>  <a href="http://www.dcds-project.eu/wp-content/uploads/2019/02/D6_DCD-Methodology-_v1_revised.pdf">http://www.dcds-project.eu/wp-content/uploads/2019/02/D6_DCD-Methodology-_v1_revised.pdf</a>  <a href="http://www.dcds-project.eu/wp-content/uploads/2018/12/D5_Contents_assessment_tool.pdf">http://www.dcds-project.eu/wp-content/uploads/2018/12/D5_Contents_assessment_tool.pdf</a>  <a href="https://www.digitalhrtech.com/skills-gap-analysis">https://www.digitalhrtech.com/skills-gap-analysis</a>  341727166_Digital_Creative_Skills_What_are_they_What_does_progression_look_like_How_are_they_developed_What_promising_practices_are_there  <a href="https://www.opencolleges.edu.au/informed/features/8-ways-boost-creativity-technology">https://www.opencolleges.edu.au/informed/features/8-ways-boost-creativity-technology</a>  <a href="https://www.techwalla.com/articles/why-is-a-file-extension-important">https://www.techwalla.com/articles/why-is-a-file-extension-important</a>  <a href="https://slidetodoc.com/solving-technical-problems-identifying-needs-and-technological-responses/">https://slidetodoc.com/solving-technical-problems-identifying-needs-and-technological-responses/</a>  <a href="https://www.mcafee.com/blogs/consumer/consumer-threat-reports/software-updates-important/">https://www.mcafee.com/blogs/consumer/consumer-threat-reports/software-updates-important/</a>

## Additional Resources – Power Point presentations


### Module 2, Unit 2.1 – Interacting through digital technologies




1




2




3




4




5




6




7




8



9



10



11

## Module 2, Unit 2.2 - Sharing through digital technologies

**Sharing through Digital Technologies**

- Connecting through Digital Technologies
- Setting up shared folders
- Using and editing a shared folder

**Sharing through Digital Technologies**

**Introduction**  
Digital technologies are tools, systems, devices and resources that generate, store or process data. Some of the most common Digital Technologies include social media, online games, multimedia and mobile devices.

**What is sharing with digital technologies?**  
According to the Digital Competence Framework 2.0 it means to share data, information and digital contents with others through appropriate digital technologies as mentioned above.

**Digital Tools**

- **Programs**  
Word, Paint, Notes
- **Websites**  
Google.com (Google drive)
- **Online courses**  
Podcasts, Videos, Social media

**Sharing through Digital Technologies**

**What is Google Drive?**  
Google Drive is a file storage service developed by Google. It is a cloud-based service available on a website and as an app and allows to store files in the "cloud" and synchronize the same device.

**How to share a file?**

1. On your computer, visit <https://www.google.com/drive/>
2. Sign in with your Google account and password
3. Select the file you want to share on Google Drive
4. Click the "Share" button in the top right corner
5. Under "People" type the email address of your colleague
6. Click "Send"

**Great Job!!!**

You just shared your first file!!!

**Sharing and Editing**

**Sharing and Editing**

[https://www.youtube.com/watch?v=VQ\\_JBYE1H4](https://www.youtube.com/watch?v=VQ_JBYE1H4)

**Task Completed!!!**

**Well Done!!!**

## Module 2, Unit 2.3 – Engaging in Citizenship through digital technologies

### Engaging in Citizenship through Digital Technologies

1

### Today's Session

This presentation is a contribution to understanding the concepts of:

- Digital Citizenship
- Cyber Security Awareness

Through this session we will focus on understanding how to identify cyber security risks, how to prevent them and resolve them.

2

### Digital Citizenship

Digital Citizenship refers to the behavior, the positive engagement, individuals impose when entering the digital world. In more detail a Digital Citizen is a person who has the knowledge and skills to participate and digital technologies to communicate with others, participate in society and create and consume content through digital tools.



3

### Basic Concepts



SAFETY REPUTATION RELATIONSHIPS ETHICS

4

### E- Safety

This concept has become a fundamental topic in the digital world and involves an individual's knowledge about internet privacy and how an individual's behavior can contribute towards a healthy interaction with the use of the internet.

Common Dangers  
Phishing, Malware, cyberbullying, accessing and getting private information

5

### Reputation



Reputation is the perception of an individual or organization based on the information available about them. It is a key factor in decision-making and can be both positive and negative.

6

### Relationships

Digital relationships involve using technology to develop a more interactive and relevant interaction between individuals.

These technologies can contribute both positively and negatively specifically in personal relationships depending on how individuals use technology and might create problems between partners potentially stirring conflict and dissatisfaction in the relationship.



7

### Ethics

Digital Ethics is the study of how to manage oneself ethically, professionally and in a manner in online and digital mediums.

Some examples of an ethical behavior when on internet:

- Asks for permission to collect and store data about others
- Asks for permission to sell any personal data that has been stored
- Has been provided with the right to request that data which items to be deleted
- Has been provided with access to personal data that has been collected and stored



8

### Digital Footprint



9

### Digital Footprints

Digital Footprints or Digital Data are records of what an individual searches, visits, creates, posts, data, media through digital tools on a mobile device or on a computer station.

Let's check this video to get a better idea of what is a digital trail.

<https://www.youtube.com/watch?v=9j8qGfPm0g>

10

### Role Playing

TWO VOLUNTEERS PLEASE!!!

11

### Digital Citizenship

A good Citizen

- Adheres to equal human rights
- Treats others with respect
- Does not steal or damage others' property
- Communicates clearly, respectfully and with empathy
- Respects himself and does not repeat cyberbullying
- Protects self and others from harm
- Respects a positive self-image

A good Digital Citizen

- Adheres to equal digital rights for all
- Seeks to understand or perspectives
- Respects digital rights, intellectual property and other rights of digital citizens
- Communicates and acts with empathy for others
- Respects his digital footprint
- Applies digital technology to online issues
- Is ethically, physically, emotional and mental
- Respects his digital footprint
- Understands the importance of the digital world and proactively manages digital identity

12

### SECURITY and PRIVACY

**SECURITY**  
Numerous processes which protect an individual's personal information from other people. This can be achieved through different ways:

- VPN, Virtual Private Networks
- Antivirus programs
- Strong Passwords

**PRIVACY**  
A person's right to preserve and protect his/her identity and maintain a safe and protected space around one's integrity, physical presence, thoughts, feelings and intimate activities.

In the digital world Privacy must be seen as a crucially important right for individuals as a society and as a collective.

13

### ANY QUESTIONS



14

## Annex II – Evaluation sheet Module 1. Information and Data Literacy

1.1. Browsing, searching and filtering information			
Unit of competence	None	Basic	Above Basic
Be able to identify different web browsers.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to recognize different search engines.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to search for information and content online.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to navigate between digital environments.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to understand the risks of confidentiality and privacy of searching on the internet.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to know the role of the internet in obtaining information in the context of today's world.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2. Evaluating data, information and digital content			
Unit of competence	None	Basic	Above Basic
Be able to recognize the dangers of fake news and misinformation in the digital age.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to identify the veracity of data and accuracy of digital information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to detect the credibility and reliability of common sources of data, information and their digital content.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to search for reliable and credible data and information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3. Managing data, information and digital content			
Unit of competence	None	Basic	Above Basic
Be able to identify different types of programmes, tools and environments to store and manage data, information and digital content.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to use digital tools and platforms to store and manage data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to organize content and data in a digital platform in a structured way.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to access digital environments defining the adequate privacy settings.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## Annex III – Evaluation sheet Module 2. Communication and collaboration

2.1. Interacting through technologies				
	Unit of competence	None	Basic	Above Basic
Communication and Collaboration	Be able to identify different digital tools, characterize them and use them in accordance with the context.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to interact and communicate with different audiences using adequate digital tools and devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to recognize and characterize different digital platforms and devices for communication.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to search for information online in safe and ethically.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	2.2. Sharing through digital technologies			
	Unit of competence	None	Basic	Above Basic
	Be able to share information with others using adequate tools and/or platforms.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to recognize and characterize different digital platforms and devices for sharing information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to share information with others in safe and ethically.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to search for information online in safe and ethically.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	2.3. Engaging in citizenship through digital technologies			
	Unit of competence	None	Basic	Above Basic
	Be able to communicate online ethically and open-minded.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to participate online in society as a citizen.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to use legal online services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to provide feedback and opinions with respect for others.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to recognize information and interactive online services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to configure settings to keep information private.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
2.4. Collaborating through digital technologies				
Unit of competence	None	Basic	Above Basic	
Be able to use different tools and platforms to communicate online with others.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to share information online using appropriate tools and platforms.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to identify the most used online platforms in their country or region.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to distinguish between instant messaging or chat platforms, voice-over-IP, social media platforms, forums and e-mail.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

2.5. Netiquette			
Unit of competence	None	Basic	Above Basic
Be able to demonstrate polite interaction online with others.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to identify what kind of behaviour should be used in different online environments (such as email, social media or chat).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to apply “good manners” in an online environment communicating with others.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to understand the importance of online rules when using digital resources.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.6. Managing digital identity			
Unit of competence	None	Basic	Above Basic
Be able to describe the concept of digital identity.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to understand how to protect the digital identity.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to describe simple ways to protect the reputation online.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to manage the digital footprint.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to know how to be respectful of the digital identities of others and careful about what to post about other people.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



## Annex IV – Evaluation sheet Module 3. Content creation

Digital Content Creation	<b>3.1. Developing content</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to create and edit digital content in different formats.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to create new, original content and knowledge.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to represent well what it is intended to communicate.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to identify the value of digital content as a visual aid.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to adapt the expression through the creation of the most appropriate digital means.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<b>3.2. Integrating and re-elaborating</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to modify information and content into an existing document or platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to integrate new information and content into an existing document or platform.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to assess the most appropriate ways to integrate specific new items of content and information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<b>3.3. Copyright and Licenses</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to apply copyright and licenses in an accurate way.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to identify which licenses are required in certain circumstances.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to know how to protect themselves against copyright infringement.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<b>3.4. Programming</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to list simple instructions for a computing system to solve a simple problem or perform a simple task.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to solve simple technical issues.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to apply instructions to perform tasks or solve problems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Annex IV – Evaluation sheet Module 4. Safety

Safety	<b>4.1. Protecting devices</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to understand the importance of protecting devices and avoid risks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to identify the difference between different types of malware.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to understand the importance of measures related to reliability and confidentiality.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<b>4.2. Protecting personal data</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to keep personal data protected.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to understand the risk of identity theft.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to apply "Privacy Policy" when using digital services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to understand the basic rules of security.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<b>4.3. Protecting health</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to control possible dangers and threats in digital environments.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to identify the risks of misusing online and digital services.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<b>4.4 Protecting the environment</b>			
	<b>Unit of competence</b>	<b>None</b>	<b>Basic</b>	<b>Above Basic</b>
	Be able to recognize simple environmental impacts of digital technologies and their use.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to use digital services without being dependent on them.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Be able to protect the environment from the impact of disposing digital devices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

## Annex V – Evaluation sheet Module 5. Problem solving

5.1. Solving Technical Problems				
Problem-solving	Unit of competence	None	Basic	Above Basic
	Be able to navigate online in everyday contexts.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to identify when a digital device is appropriate enough to work on.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Be able to identify when a problem has occurred on a digital device or service.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	5.2. Identifying needs and technological responses			
Unit of competence	None	Basic	Above Basic	
Be able to recognize technical problems originating from a digital device or from the environment.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to recognize solving methods.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to understand how to use help facilities, manuals guides.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.3. Innovating and creatively using technology				
Unit of competence	None	Basic	Above Basic	
Be able to use the appropriate digital technology for a specific purpose (gather information, create content).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to use components of digital systems and digital information in real-world conditions.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5.4. Identifying digital competence gaps				
Unit of competence	None	Basic	Above Basic	
Be able to evaluate himself or others if new digital environments are appropriate means of improving digital competence level.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Be able to seek opportunities for self-development and keep up to date with the digital evolution.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

## Annex VI – Evaluation of the training

This evaluation sheet has as main objective the collection of data and your feedback about the quality of the training programme for a “digital competent” citizen. This questionnaire must be filled in individually and at the end of the training. The questionnaire is confidential, and your opinion is crucial to the improvement of the training programme. The questionnaire is structured in **three parts**: the **part A – Statistics** has two questions allowing partners to make a statistic analysis of the workshops implemented; the **part B -Quantitative Evaluation** is composed by **13 statements**, to be answer using the following **scale** from **1 to 5**: 1 – strongly disagree, 2 – mostly disagree, 3 - Neither agree or disagree, 4 –mostly agree and 5- strongly agree<sup>20</sup>; the **part B – Qualitative Evaluation** is composed by two **open-questions**: a first one in which you should provide **additional comments/suggestions** about the **statements** that you **scored with 1, 2 or 3**; a second one in which you can add any additional comment to the training programme and workshop.

### Part A – Personal data

#### Country of residence

Romania ☐

Portugal ☐

Greece ☐

Italy ☐

Denmark ☐

#### Profession

### Part B – Quantitative Evaluation

	1	2	3	4	5	NA
The training curriculum is relevant to my personal and/or professional life.						
The training corresponded to my initial expectations.						
The objectives of the training were achieved.						
The units and contents addressed were interesting and relevant.						
The duration of the training is according to its objectives, contents and activities/assignments.						
The training allowed the acquisition of digital competences.						
The contents, practices and/or instruments introduced in the training were suitable to be implemented in my daily activities.						
The support materials used during the training were adequate (in terms of design, language, utility, information provided).						
The activities, assignments and exercises proposed during the training are adequate to the acquisition and development/consolidation of digital competences.						
The trainers provided the necessary support to the participants during the training.						
The trainers were clear and efficient during the training.						
The trainers promoted the participation and involvement of participants in the training.						

<sup>20</sup> If one of the statements does not apply to your experience, please answer “NA” (*Not Applicable*).

### Part C – Qualitative Evaluation

1. Please provide **additional recommendations/suggestions** regarding the statement that you **scored with 1, 2 or 3**:

2. Do you have any additional comment related to the training curriculum? Please share it here.

Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

**Thank you for your contribution!**

# REFERENCES



**European Commission:** [https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data\\_en](https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en)

Celebic, G. & Rendulic, D. (2011). *Basic Concepts of Information and Communication Technology Handbook*. Open Society for Idea Exchange (ODRAZI), Zagreb. Source: [http://www.itdesk.info/handbook\\_basic\\_ict\\_concepts.pdf](http://www.itdesk.info/handbook_basic_ict_concepts.pdf)

**Encyclopaedia Britannica:** <https://www.britannica.com/technology/browser>

**Australian Cyber Security Centre:** <https://www.cyber.gov.au/acsc/view-all-content/guidance/proactive-measures-protect-your-information>

**Georgetown University Library:** <https://www.library.georgetown.edu/tutorials/research-guides/evaluating-internet-content>

**Smithsonian Magazine:** <https://www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/?no-ist>

**Washington State University Vancouver:** <https://webliteracy.pressbooks.com/chapter/building-a-habit-by-checking-your-emotions/#footnote-51-1>

**The balance small business:** <https://www.thebalancesmb.com/copyright-definition-2948254>

**University, Spring Arbor.** Fundamentals of Communication: 8 Basic Concepts and Definitions. *Spring Arbor University*. [Online] June 2021. <https://online.arbor.edu/news/fundamentals-communication-eight-basic-concepts-and-definitions>.

*7 Examples of Digital Channels.* **Spacey, John.** 2017, Simplicable .

*The 10 new paradigms of communication in the digital age.* **Orihuela, Jose Luis.** 2017, Jlori.

*4 Types of Communication Styles.* **Alvernia University.** Pennsylvania : s.n., 2018, Alvernia University, p. 2.

**LEADGENERA.** LEADGENERA. *Content Marketing*. [Online] June 2021. <https://leadgenera.com/knowledge-hub/marketing/the-10-best-social-media-and-content-apps-for-2020/>.

**Commision, European.** The Digital Competence Framework 2.0. *EU SCIENCE HUB*. [Online] January 9th, 2019. <https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework>.

**Care, Department of Health and Social.** Engage. *Digital passport*. [Online] <https://engage.dhsc.gov.uk/digitalpassport/tools/>.

**Google.** Google. *Google Drive*. [Online] Google. <https://support.google.com/drive/answer/2424384?hl=en&co=GENIE.Platform%3DDesktop>.

**European Commission.** Europa. *Digital Citizenship Transformation*. [Online] European Commission.  
<https://epale.ec.europa.eu/en/blog/digital-citizenship-transformation>.

**Common Sense.** *Everything You Need to Teach Digital Citizenship*. [website] s.l. : Common Sense, 2021.

**Australian Government.** eSafety Commissioner . *Digital Citizens Guide*. [Online]  
<https://www.esafety.gov.au/media/2563>.

**Liveworkstudio.** live|work. *Digital Relationships*. [Online]  
<https://www.liveworkstudio.com/themes/organisational-change/digital-relationships/>.

**Eferin, Kate Gromova and Yaroslav.** World Bank Blogs. *Ethics in the digital world: Where we are now and what's next*. [Online] April 9th, 2021. <https://blogs.worldbank.org/opendata/ethics-digital-world-where-we-are-now-and-whats-next>.

**Zwerdling, Daniel.** npr. *Your Digital Trail, And How It Can Be Used Against You*. [Online] 2013.  
<https://www.npr.org/sections/alltechconsidered/2013/09/30/226835934/your-digital-trail-and-how-it-can-be-used-against-you>.

**The University of Alabama at Birmingham.** UAB Institute for Human Rights Blog. *Digital Citizenship: The Good, The Bad, & The Role of the Internet*. [Online] January 2019.  
<https://sites.uab.edu/humanrights/2019/01/18/digital-citizenship-the-good-the-bad-the-role-of-the-internet/>.

#### BYU Library:

- <https://guides.lib.byu.edu/c.php?g=216340&p=1428402>
- <https://www.techwalla.com/articles/why-is-a-file-extension-important>
- <https://slidetodoc.com/solving-technical-problems-identifying-needs-and-technological-responses/>
- <https://www.mcafee.com/blogs/consumer/consumer-threat-reports/software-updates-important/>
- <https://www.opencolleges.edu.au/informed/features/8-ways-boost-creativity-technology/>





No One  
Behind



Co-funded by the  
Erasmus+ Programme  
of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

**Project n. ° 2020-1-RO01-KA204-079988**