No One Behind

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

Acest proiect a fost finanțat cu sprijinul Comisiei Europene. Această publicație reflectă doar punctul de vedere al autorului, iar Comisia nu poate fi făcută responsabilă pentru orice utilizare care poate fi făcută a informațiilor conținute în ea. (Proiect nr. º 2020-1-RO01-KA204-079988)

No One Behind

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

Manual de instruire pentru un cetățean "digital competent"

Erasmus Plus Programme – KA2 Strategic Partnership for Adult Education

Format din:

P1 – Agentia Nationala pentru Programe Comunitarie 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

AUTORI | No One behind | August 2021

Parteneriat

North-East Regional Development Agency - NERDA, Romania
Lucian Alexa and Olivian Secara
Website: https://www.adrnordest.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
Rafaela Paspati 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/

CUPRINS

TABEL DE FIGURI

TABEL DE TABELE

ABBREVIATIONS

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

No One Behind

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

REZUMAT

Manualul de formare pentru un cetățean digital competent a fost elaborat în cadrul proiectului ***No One Behind*** pentru a ghida formatorii și cursanții printr-o cale ușoară de promovare a competențelor digitale ale adulților din zonele rurale.

Manualul oferă un curriculum de formare și materiale pentru a sprijini educatorii adulți (și alte părți interesate) în dezvoltarea competențelor digitale ale adulților din zonele rurale, permițându-le să devină "cetățeni competenți digital".

Programa de formare a fost structurată pe baza profilului cetățeanului digital competent, conceput și de consorțiu în conformitate cu principiile sistemului european de credite pentru educație și formare profesională (ECVET) și ale Cadrului european al calificărilor (CEC). Profilul este prezentat pe scurt la începutul acestui manual.

În ceea ce privește structura și conținutul, curriculumul și materialele sunt legate de DigComp – European Digital Competence Framework pentru cetățeni și conține astfel 5 module de formare, acoperind 21 de competențe digitale ale cadrului:

- Alfabetizarea informațiilor și a datelor
- Comunicare și colaborare
- Crearea de conținut digital
- Siguranță
- Rezolvarea Problemelor

Pentru fiecare dintre aceste module, acest manual oferă:

- o prezentare generală a obiectivelor, conținutului și structurii care trebuie urmate de educatorii și cursanții adulți;
- planuri, activități și resurse specifice legate de unitățile de competență identificate în fiecare modul și care promovează dezvoltarea și consolidarea competențelor digitale ale adulților.

Face parte, de asemenea, din acest document un set de grile pentru a sprijini evaluarea nivelului de dezvoltare a competențelor digitale ale adulților din zonele rurale, care urmează să fie realizat înainte și după începerea formării.

No One Behind

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

INTRODUCERE

1. Introducere în manualul de instruire *No One Behind*

Acest manual de formare este rezultatul muncii comune a diverselor organizații care se gândesc să producă un ghid pas cu pas pentru a promova competențele digitale în cadrul grupurilor de persoane care trăiesc în zonele rurale și pentru a promova incluziunea socială prin creșterea competenței lor digitale. Unitatile si continutul sunt organizate astfel incat manualul sa fie folosit pentru auto-invatare dar si ca instrument/indrumare pentru formatorii care doresc sa ofere un training de abilitati digitale pentru persoanele care au foarte putine competente digitale.

Pentru cine este acest manual?

Educatori pentru adulți: asistenți sociali, profesori, mentori, profesori și alți profesioniști care lucrează cu adulți;

Adulți din mediul rural dispuși să-și îmbunătățească viața de zi cu zi, să-și schimbe locul de muncă sau să găsească noi oportunități prin dezvoltarea unor competențe digitale utile.

Scopul acestui manual este de a ghida formatorii și cursanții printr-o cale ușoară și inovatoare de promovare a competențelor digitale, urmând orientările cadrului DigComp.

Manualul este organizat în patru secțiuni principale, după cum urmează:

- **Rezumat** – Cu o sinteză a conținutului manualului de instruire, care poate fi folosit pentru a-l prezenta grupurilor țintă și social media.
- **Introducere** – Începând cu o scurtă introducere în manualul de formare și cu includerea unei scurte prezentări a profilului cetățeanului "digital competent" prezentat în metodologie [1].
- **Curicula cetateanului competent digital** –Acesta cuprinde cinci capitole corespunzătoare celor cinci module ale formării. Fiecare capitol oferă informații despre structura modulului și unitățile corespondente de competență. De asemenea, oferă orientări și materiale pentru a sprijini punerea în aplicare a formării și dobândirea/consolidarea competențelor digitale ale cursanților.
- **Evaluarea formarii** –Această secțiune oferă directive legate de evaluarea competențelor digitale și învățarea cursanților, oferind sprijinul necesar pentru asigurarea acesteia. De asemenea, oferă sprijin pentru evaluarea formării de către cursanți.

Un set de anexe pentru a sprijini punerea în aplicare a formării sunt, de asemenea, furnizate în prezentul document, inclusiv:

- Anexa I – Resurse aditionale – Cu legături legate de modulele și unitățile de competențe incluse în acest manual de formare, formatorii și cursanții pot avea acces pentru a afla mai multe.

[1] Prezentarea completa a profilului este disponibila in documentul *Innovative methodology for educating and training adults fr om rural zone to improve their digital and ICT skills*· Accesibla aici.

- Anexa II – Fisa de evaluare Modul 1 – O grilă de evaluare care să fie utilizată pentru a măsura nivelul de dezvoltare a competențelor digitale ale cursanților în ceea ce privește *Alfabetizarea în domeniul informației și al datelor.*
- Anexa III – Fisade evaluare Modul 2 – O grilă de evaluare care să fie utilizată pentru a măsura nivelul de dezvoltare a competențelor digitale ale cursanților în ceea ce privește *Comunicarea și colaborarea.*
- Anexa IV – Fisa de evaluare Modul 3– O grilă de evaluare care să fie utilizată pentru a măsura nivelul de dezvoltare a competențelor digitale ale cursanților în legătură cu *Crearea de conținut*.
- Anexa IV – Fisa de evaluare Modul 4– O grilă de evaluare care să fie utilizată pentru a măsura nivelul de dezvoltare a competențelor digitale ale cursanților în ceea ce privește *Siguranța.*
- Anexa V – fisa de evaluare Modul 5– O grilă de evaluare care să fie utilizată pentru a măsura nivelul de dezvoltare a competențelor digitale ale cursanților în legătură cu Rezolvarea problemelor.
- Anexa VI – Evaluaerea pregatirii - Grila de evaluare pentru evaluarea calitatii si relevantitatii instruirii de catre elevi.

2. Profilul cetățeanului "digital competent"

În spatele cursului de formare introdus în acest manual se află profilul cetățeanului "digital competent", definit așa cum se arată în schema de mai jos (Figura 1.):

Cetățean digital competent

PREZENTARE GENERALĂ

EQF[2] Nivel

3

EQF Credite: 5

Descriere: Cetățeanul "digital competent" va putea:

- să înțeleagă utilitatea competențelor digitale
- utilizarea în viața de zi cu zi a principalelor sisteme digitale
- să înțeleagă riscurile și posibilele amenințări legate de mediul internet
- să înțeleagă cum să interacționeze cu ceilalți și să utilizeze tehnologiile pentru a accesa serviciile

STRUCTURA GLOBALĂ

Nr.	Module	Durata	Credit
1	Alfabetizarea în materie de informații și date	25h	1
2	Comunicare și colaborare	25h	1
3	Crearea de conținut digital	25h	1
4	Siguranță	25h	1
5	Rezolvarea problemelor	25h	1

Figura 1 – Prezentare generala si structura globala a Cetateanului Competent Digital asa cum este definite de consotiu si in conformitate cu ECVET[3].

Fiecare modul este structurat pe unități de competențe, esențiale pentru a ghida educatorii și cursanții adulți în dobândirea, dezvoltarea și consolidarea competențelor digitale (Figura 2.).

[2] European Qualification Framework: mai multe informatii gasiti aici.

[3] European credit system for vocational education and training: mai multe informatii gasiti aici.

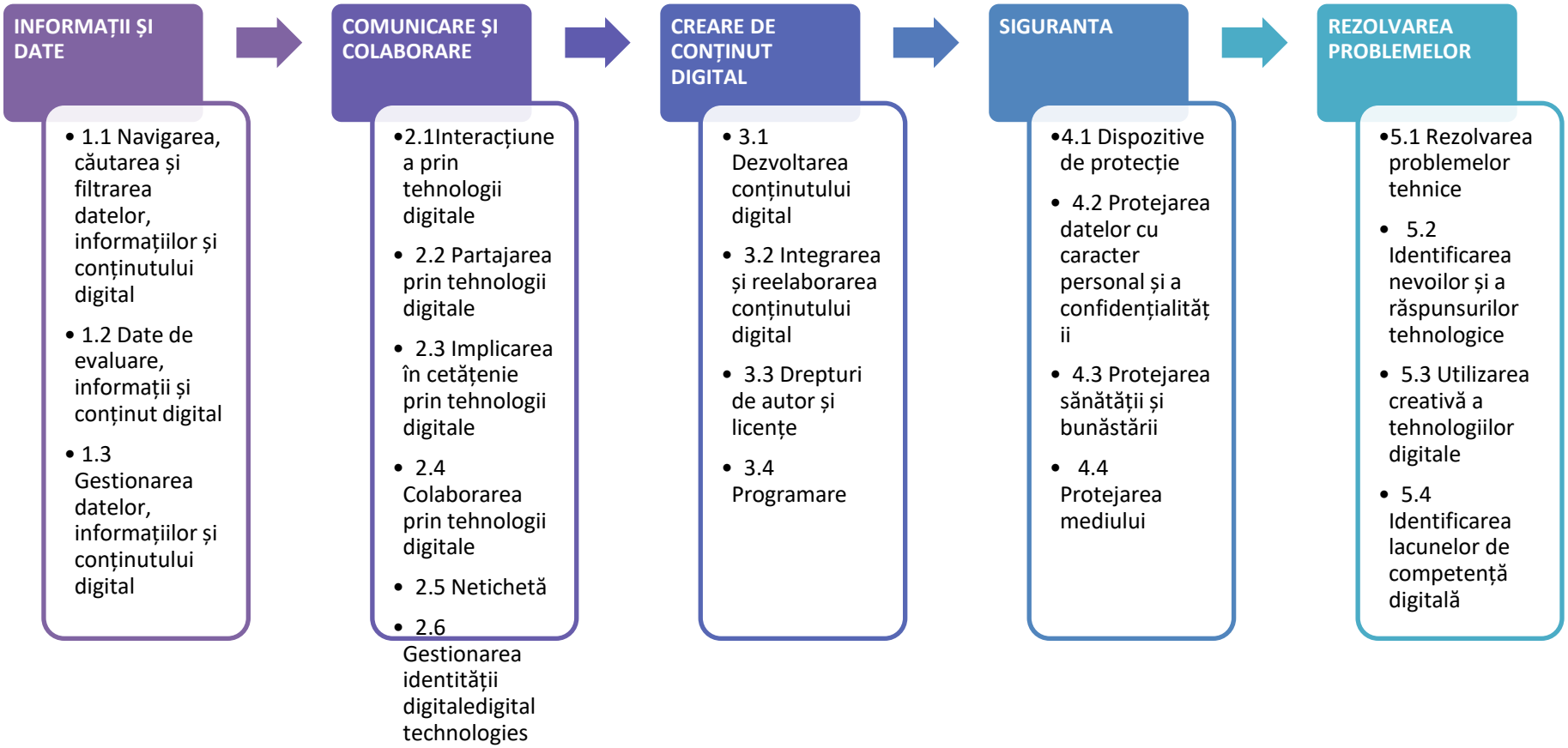


FigurA 2 – Identificarea unitatilor de competente corespunse modulelor de profil pentru un cetatean digital competent.

Aceste unități de competență sunt descrise în documentul Metodologie inovatoare pentru educarea și formarea adulților din mediul rural în vederea îmbunătățirii competențelor lor digitale și TIC în ceea ce privește cunoștințele, aptitudinile și competențele.

No One Behind

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

2 CURRICULA CETATEANULUI COMPETENT DIGITAL

Această secțiune este dedicată curriculumului digital competent pentru cetățeni, la care aveți acces la:

o imagine de ansamblu globală a structurii curriculumului;

scurta prezentare a celor 5 module care cuprind curriculumul;

planuri, activități și resurse specifice legate de unitățile de competență identificate în fiecare modul și care promovează dezvoltarea și consolidarea competențelor digitale ale adulților.

Tabelul 1. Prezintă structura globală a curriculumului pentru **Cetateanul Digital Competent**, astfel cum este structurată în domeniul de aplicare al proiectului **No One Behind**:

Stagiu	**Cetățean digital competent**
Durata	125h
Obiective	Combinație de sesiune față în față cu sesiuni online și studiu individual.
Organizație de instruire	Învățare mixtă, combinând instruirea față în față cu sesiunile online.
Scopul principal	• Acest manual își propune să devină o referință pentru formatori atunci când lucrează cu adulți cu competențe digitale scăzute. Pentru a atinge acest obiectiv, manualul cuprinde conținut teoretic și activități practice pentru a stimula învățarea. • Acest manual își propune să sprijine stagiarii și adulții să își îmbunătățească competențele digitale, prin oferirea de activități pas cu pas.
Planul de instruire	Cursul este structurat în cinci module: • Modulul 1 - Alfabetizarea informației și a datelor (25h) • Modulul 2 - Comunicare și colaborare (25h) • Modulul 3 - Crearea de conținut digital (25h) • Modulul 4 - Siguranță (25h) • Modulul 5 - Rezolvarea problemelor (25h)
Evaluarea învățării	*Fișe de evaluare pentru fiecare modul și unitate (furnizate la sfârșitul manualului)*
Evaluarea instruirii	Fișe de evaluare (furnizate la sfârșitul manualului)

Tabelul 1 – Curicula Cetateanului competent digital - stagii formare.

După cum se poate observa, curriculumul este organizat în 5 module, fiecare cu o propunere specifică și împărțit în unități de competență, după cum se arată în tabelul 2.:

Modul 1 Alfabetizarea în materie de informații și date	
Acest modul introduce instrumentele și competențele necesare pentru a efectua căutarea online, prezentând în același timp diferite strategii și tehnici disponibile pentru a găsi informații fiabile. Până la sfârșitul acestui modul, este de așteptat ca elevii să știe cum să gestioneze informațiile, să le poată salva în dispozitive tehnologice, să le recupereze, deși sunt conștienți de legile privind drepturile de autor și de protecția datelor.	1.1. Navigarea, căutarea și filtrarea datelor
	1.2. Evaluarea datelor, informațiilor și conținutului digital
	1.3. Managing data, information and digital content
Module 2 **Communication and collaboration**	
În acest modul, cursanții își vor dezvolta abilitățile și abilitățile de a interacționa cu alții folosind tehnologia digitală. Ei vor putea interacționa și partaja informații, fiind conștienți de eticheta și identitatea personală online.	2.1.Interacțiunea prin intermediul tehnologiilor digitale
	2.2. Partajarea prin intermediul tehnologiilor digitale
	2.3.Implicarea în cetățenie prin intermediul tehnologiilor digitale
	2.4. Colaborarea prin intermediul tehnologiilor digitale
	2.5. Neticheta
	2.6. Gestionarea identității digitale
Module 3 **Digital content creation**	
Obiectivul acestui modul este de a promova competențele de creare a conținutului digital și a programării, astfel încât cursanții să se simtă încrezători, de exemplu, în promovarea propriei afaceri online.	3.1. Dezvoltarea conținutului digital
	3.2. Integrarea și re-elaborarea conținutului digital
	3.3. Drepturi de autor și licențe
	3.4. Programare
Module 4 **Safety**	
La finalizarea acestui modul, elevii trebuie să devină conștienți de acțiunile pe care le pot lua pentru a proteja dispozitivele, sănătatea lor și mediul înconjurător atunci când utilizează tehnologia. Acest modul are ca scop, de asemenea, creșterea gradului de conștientizare cu privire la confidențialitate și date cu caracter personal.	4.1. Protejarea dispozitivelor
	4.2. Protejarea datelor cu caracter personal și a confidențialității
	4.3. Protejarea sănătății și a bunăstării
	4.4. Protejarea mediului
Module 5 **Problem solving**	
Acest modul evidențiază problemele tehnice și strategiile pentru a face față celor mai actuale probleme atunci când operați un computer. În plus, cursanții vor avea șansa să se	5.1. Rezolvarea problemelor tehnice
	5.2. Identificarea nevoilor și a răspunsurilor tehnologice
	5.3. Utilizarea creativă a tehnologiilor digitale

gândească la metodologii creative atunci când utilizează instrumente digitale.	5.4. Identificarea lacunelor în materie de competențe digitale

Tabelul 2 – Scurtă descriere și identificare a unităților de competențe ale fiecărui modul al cursului de formare.

Urmând această structură, puteți găsi în această secțiune cinci capitole, fiecare corespondent la unul dintre modulele curriculumului. La începutul fiecărui capitol, veți avea un tabel cu o prezentare generală a duratei, obiectivelor și unităților acoperite în modul. Urmează prezentarea către unitățile de competențe în ceea ce privește durata, obiectivele, conținutul, resursele și metodologiile de formare și modul în care unitățile ar putea fi livrate. Pentru fiecare unitate veți găsi atât informații teoretice, cât și activități practice, astfel încât experiența de învățare să curgă ușor și să sperăm că permite o abordare "practică".

Prin urmare, multe activități sunt sugerate pe tot parcursul manualului, făcând uz de diverse metodologii de învățare, cum ar fi:

Metoda	Descriere
Prezentare de către trainer	Participarea cursanților la lecții bazate pe prezentări PowerPoint, vizualizare video, demonstrație, studii de cercetare, cărți, lucrări sau alte resurse și suporturi afișate de formatori într-o sesiune de instruire sau într-o platformă de e-learning. Pot fi utilizate suporturi suplimentare - studii de caz, misiuni și chestionare - care să permită consolidarea expertizei și creșterea cunoștințelor.
Exercițiu de grup Discuție / Dezbatere	Se poate face în grupuri mari sau mai mici, iar ideea este de a promova discuția sau dezbaterea dintre cursanți legată de un anumit subiect lansat de formator. Discuția sau dezbaterea ar trebui monitorizată pentru a permite participarea tuturor cursanților și concentrarea pe subiectele relevante. La sfârșitul discuției sau al dezbaterii este important să se elaboreze și să se împărtășească unele concluzii.
Lucrul în perechi / Grupuri mici	Trainerul trebuie să furnizeze fiecărui grup mic informații exacte despre subiect, rezultatele așteptate ale lucrului în grup (de asemenea, metoda de prezentare a rezultatelor - grupul ar trebui să fie clar cu privire la cine va prezenta aceste rezultate la începutul lucrului) și durata lucrului în grup. Înainte de a începe exercițiul, trainerul și toți cursanții verifică timpul, iar trainerul le spune cursanților când să se întâlnească din nou în grupul mare pentru a evita orice neînțelegeri. În timpul lucrului în grup, trainerul asistă toate grupurile și urmărește calendarul.
Prezentarea de către participanți	Trainerii pot provoca elevii să pregătească o prezentare pe un anumit subiect și să modereze o sesiune de învățare. Cursanții pot alege formatul de prezentare (de exemplu, PowerPoint-uri, activități, videoclipuri,...) și pot implica alți cursanți în diferitele momente ale prezentării.
Simulare / Jocuri de rol	Jocul de rol este o metodă de învățare în care elevii își asumă roluri de personaje și creează în colaborare povești. Această tehnică este un instrument excelent pentru implicarea cursanților și pentru a le permite să interacționeze cu colegii lor în timp ce încearcă să finalizeze sarcina care le-a fost atribuită în rolul lor specific. Această activitate se poate face în grupuri de cooperare și / sau cursanții pot menține persona rolului lor pe tot parcursul perioadei de clasă. Elevii sunt mai implicați pe măsură ce încearcă să răspundă materialului din perspectiva caracterului lor.
Învățarea bazată pe proiecte (PBL)	PBL este o predare bazată pe proiecte sau sarcini integrate. Pornind de la o problemă concretă, elevii sunt provocați să dezvolte proiecte care să răspundă la problemele din viața reală, permițându-le să se implice activ în învățarea lor, să învețe făcând și să dobândească / să-și consolideze abilitățile.
Învățarea prin cooperare	Este o metodologie bazată pe discuții, în care un grup mic de cursanți discută un subiect lansat de formator. Trei roluri principale trebuie distribuite între cursanți:) scribul ia notițe cu privire la dezbatere, astfel încât toți ceilalți cursanți să poată fi pe deplin implicați în conversație; 2) micul sertar de hartă monitorizează cine vorbește și când și desenează evoluția conversației; 3) moderatorul se asigură că conversația nu rămâne pe un singur subiect prea mult timp sau se mișcă prea repede și că toată lumea vorbește. Trainerii intervin doar atunci când este necesar.
Sala de clasă răsturnată	Este o abordare pedagogică în care elementele tradiționale ale lecției predate de formator sunt inversate: materialele educaționale primare sunt studiate de elevi acasă și, apoi, lucrate în sesiune.
Stație de învățare	Cu ajutorul metodei de învățare a stației, conținutul este procesat individual și orientat spre nevoi. Trainerul pregătește o stație de învățare pentru fiecare componentă a aplicației, la care sunt disponibile sarcini de lucru și materiale de lucru. Elevii pot alege stațiile care îi interesează în ceea ce privește conținutul și pe care le evaluează ca fiind importante pentru aplicarea lor individuală. Trainerul este întotdeauna disponibil pentru întrebări. Elevii

	iau notițe și ulterior vor avea acces și la materialele/eșantioanele etc. ale tuturor stațiilor. Ei își pot alege propria cale de învățare de la o stație la o stație.

Tabelul 3 – Identificarea și descrierea succintă a metodelor luate în considerare în prezentul manual.

Modulul 1: Alfabetizarea în domeniul informației și al datelor

Primul modul vă va prezenta procedurile de căutare online, concentrându-vă, de asemenea, în modul de evaluare a informațiilor, cum să le stocați, să le preluați și să le utilizați în mod responsabil.

Vă rugăm să rețineți că activitățile practice descrise în fiecare unitate ar putea implica sprijinul unui formator cu experiență. Deși informațiile prezentate în manual sunt scrise într-un mod ușor de înțeles, unele acțiuni, adiacente informațiilor prezentate, pot necesita supravegherea și sprijinul persoanelor cu experiență.

Modulul 1	**Alfabetizarea în materie de informații și date**		
Durata	25h		
Obiectivele	Pentru a căuta informații fiabile online folosind diferite browsere și motoare de căutare Efectuați căutarea online într-un mod sigur și sigur Identificați posibilele știri false și informații înșelătoare pe site-uri Web Organizați, stocați și preluați informații		
Unităţi	1.1 Navigarea, căutarea și filtrarea datelor, informațiilor și conținutului digital	1.2 Evaluarea datelor, informațiilor și conținutului digital	1.3 Gestionarea datelor, a informațiilor și a conținutului digital
Organizație de instruire	E-learning Față în față	E-learning Față în față	E-learning Față în față
Durată	9h	8h	8h

Tabelul 4 – Structura globală a modulului 1 – Alfabetizarea informației și a datelor.

1.1. Navigarea, căutarea și filtrarea datelor

Unitatea 1.1	Navigarea, căutarea și filtrarea datelor, informațiilor și conținutului digital
Durată	9 ore
Obiective	Pentru a utiliza diferite browsere și motoare de căutare pentru căutarea online; Pentru a efectua o căutare online pe un anumit subiect, selectând surse sigure de informații; Pentru a identifica site-uri web suspecte și informații greșite; Pentru a salva și a prelua date precum documente, imagini, site-uri web; Pentru a gestiona mediul digital ținând cont de setările de confidențialitate și confidențialitate
Conţinut	1.1.1 Concepte principale: IT, TIC și Internet 1.1.2 Introducere în căutarea online 1.1.3 Protecție la utilizarea TIC 1.1.4 Activități practice
Resurse	Manual de instruire Computer cu acces la internet Hârtii de flipchart Markere Studiu de caz 1 și 2
Metodologii de instruire	Prezentare de către trainer Exercițiu de grup Discuție / Dezbatere Lucrul în perechi/grupuri mici Prezentare de către participanți

Masa 5– Structura unităţii de competenţă 1.1. - Navigarea, căutarea și filtrarea datelor din Modulul 1 – Informații și alfabetizare de date.

1.1.1. Concepte principale: IT, TIC și Internet

Pentru a vă prezenta acest modul, am dori să vă prezentăm două concepte principale pe care probabil le auziți mult când vorbiți despre tehnologia computerelor. Acestea sunt:

IT (tehnologia informației) - cuprinde toată tehnologia pe care o folosim pentru a colecta, procesa, proteja și stoca informații. Se referă la hardware, software (programe de calculator) și rețele de computere.

TIC (tehnologia informației și comunicațiilor) - acest concept presupune transferul si utilizarea a tot felul de informatii. TIC este fundamentul economiei și o forță motrice a schimbărilor sociale în secolul XXI. Distanța nu mai este o problemă când vine vorba de accesarea informațiilor; de exemplu, lucrul de acasă, învățarea la distanță, e-banking și e-guvernarea sunt acum posibile din orice loc cu o conexiune la internet și un dispozitiv de calcul.

Ia-ti notite:
TIC include toate mijloacele tehnice care sunt utilizate pentru manipularea informațiilor și facilitarea comunicării, inclusiv calculatoarele, hardware-ul de rețea, liniile de comunicație și tot software-ul necesar. Cu alte cuvinte, TIC este compus din tehnologia informației, telefonie, media electronică și toate tipurile de procese și transfer de semnale audio și video și toate funcțiile de control și management bazate pe tehnologiile de rețea.

Internet
Internetul („rețeaua tuturor rețelelor") este un sistem global format din calculatoare interconectate și rețele de calculatoare, care comunică prin utilizarea protocoalelor TCP/IP. Deși, la începuturile sale, a apărut din necesitatea unui simplu schimb de date, astăzi afectează toate domeniile societății, de exemplu:

- **Economie**: Internet banking (plata facturilor, transferul de fonduri, acces la cont, acces la datorii creditare etc.), tranzacționare electronică (acțiuni, diverse bunuri, servicii intelectuale etc.), etc.
- **Socializarea**: rețele sociale, forumuri...
- **informație**: portaluri de știri, bloguri etc.
- **Sănătate**: diagnosticarea bolii, examene medicale (pentru persoanele care locuiesc pe o insulă sau în alte locuri îndepărtate, unele examinări, care necesită un specialist, se pot face de la distanță), programare pentru examene medicale, schimbul de date medicale între spitale și institute, intervenții chirurgicale și monitorizare chirurgicală de la distanță
- **Educație**: universități online cu webinarii (web + seminar), site-uri web cu tutoriale, sfaturi de specialitate, training online etc.

Internetul are într-adevăr multe aplicații și un impact social uriaș. Poate că cea mai importantă trăsătură este schimbul de informații, deoarece schimbul de informații între oameni permite colaborarea, colaborarea unor oameni cu gânduri similare duce la idei și acțiuni în viața reală, iar acțiunile coordonate ale oamenilor au ca rezultat schimbarea socială.

Acum că ați învățat mai multe despre tehnologie și potențialul internetului de a schimba lumea, gândiți-vă la modul în care vă poate afecta pe dvs. și viața personală.

S-ar putea să vă întrebați chiar acum... ok, această idee de a vă conecta cu ceilalți într-un mod atât de ușor sună uimitor, dar cum folosesc aceste instrumente? Acesta este primul subiect din acest manual: căutarea online și învățarea să răsfoiți, căutarea și filtrarea informațiilor.

1.1.2. Introducere în căutarea online

Abilitatea de a căuta informații online este una dintre cele mai importante abilități de alfabetizare digitală pe care le puteți poseda. Vă permite să găsiți rapid ceea ce căutați, fără a fi nevoie să parcurgeți paginile cu rezultate irelevante.

Cel mai important instrument în acest proces este motorul de căutare, care este un site web specializat care caută informații pe internet. Probabil ați auzit de cele mai populare, inclusiv Google, Yahoo! și Bing și, deși fiecare dintre ele este utilă, ele pot da, de asemenea, rezultate diferite.

În general, Google este cel mai popular motor de căutare. Este atât de popular, de fapt, încât a devenit chiar un verb obișnuit, ca atunci când cineva spune: „Buc adresa pe google chiar acum".

Cum să începeți căutarea

Pentru a începe o căutare, va trebui să faceți clic pe a **browser**. Un browser este un software care permite unui utilizator de computer să găsească și să vizualizeze informații pe Internet și există diferite disponibile pentru utilizatori. Internet Explorer, Mozilla Firefox și Chrome sunt doar câteva dintre ele și de obicei le găsiți în partea de jos a desktopului computerului.

Figura 3 – Pictograme ale unor browsere.

Apoi accesați pagina de pornire a motorului de căutare, de exemplu **google.com**, și introduceți termenii de căutare în caseta de text. Pentru a vedea rezultatele, puteți apăsa tasta Enter sau puteți face clic pe o pictogramă, cum ar fi butonul Căutare Google sau o lupă.

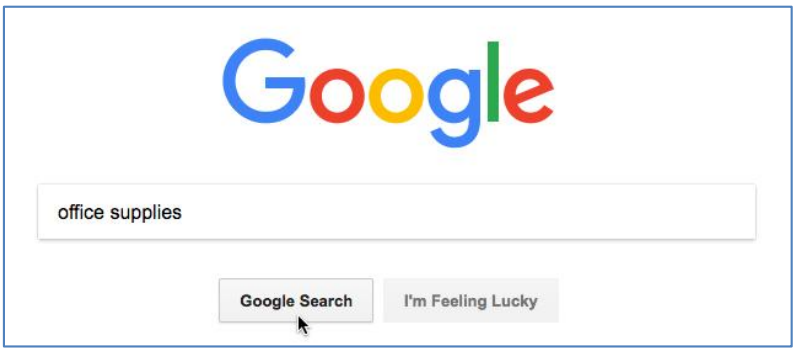


Figura 4 – Pagina de pornire Google.

În funcție de browser, este posibil să puteți efectua o căutare direct din interfața browserului. De exemplu, în Chrome, puteți introduce termenul de căutare direct în bara de adrese. În Internet Explorer (imaginea de mai jos), puteți utiliza fie bara de adrese, fie bara de căutare încorporată pentru a începe o căutare.

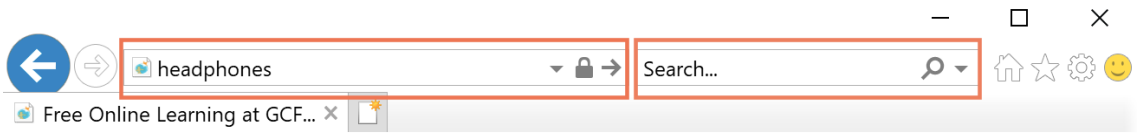


Figura 5 – Pagina de pornire Chrome.

Strategii de căutare

Cu câteva strategii de căutare de bază, puteți găsi de obicei aproape orice doriți. Nu contează dacă utilizați Google sau orice alt motor de căutare, deoarece aceste tehnici sunt eficiente indiferent unde căutați.

- **Nu te complica:**Faceți căutările dvs. scurte concentrându-vă pe cuvinte cheie, apoi păstrați numărul acestor cuvinte cheie la un nivel minim. În acest fel, este mai probabil să obțineți rezultate relevante.
- **Luați în considerare sugestiile:**Pe măsură ce introduceți termenul, motoarele de căutare vă vor sugera cele mai populare rezultate care implică termenul, așa că nu vă fie teamă să selectați unul, deoarece adesea vă pot oferi o mulțime de idei noi.
- **Folosește limbajul natural:**Nu trebuie să folosiți cuvinte sau expresii complicate pentru a obține rezultate. Motoarele de căutare pot recunoaște limba pe care o utilizați în mod natural în viața de zi cu zi, așa că nu ezitați să încercați orice vă trece prin minte.

În funcție de căutarea dvs., formatul rezultatelor dvs. poate varia în funcție de ceea ce motorul de căutare consideră că va fi cel mai util. Aceasta înseamnă că rezultatele dvs. pot include hărți, o parte dintr-un articol Wikipedia, liste și multe altele.

Motoarele de căutare pot găsi multe alte tipuri de conținut pe lângă paginile web. Cu doar un clic sau două, puteți căuta și imagini, videoclipuri, știri și multe altele.

Înainte de a vă începe experiența online, am dori să vă atragem atenția asupra unui lucru de cea mai mare importanță: **setări de securitate și confidențialitate online.**

1.1.3. Protecție la utilizarea TIC

Securitatea informațiilor este definită ca păstrarea confidențialității, integrității și disponibilității informațiilor. **Măsuri de securitate a informațiilor** sunt regulile de protecție a datelor la nivel fizic, tehnic și organizatoric. Autentificarea utilizatorului implică identificarea utilizatorului, astfel încât persoanele fizice pot obține acces la un anumit conținut (date). De exemplu, pentru a vă verifica e-mailul prin browser, adică pentru a accesa un cont, este necesar să introduceți un nume de utilizator și o parolă. Dacă informațiile solicitate sunt introduse corect, accesul este acordat. Parolele ar trebui, din motive de securitate, să fie păstrate confidențiale. O parolă este o cheie (cum ar fi o cheie de acces la casa ta sau la o mașină) care permite accesul.
Deoarece nu ați împărtăși cheile de la apartament sau de la mașină cu nimeni, nu ar trebui să vă împărtășiți nici parola. În prezent, multe persoane au uși de securitate cu încuietori ale căror chei sunt greu de copiat, cu scopul de a bloca pătrunderea neautorizată în locuință. Parolele trebuie create cu aceeași precauție. Cu cât parola dvs. este mai complexă, cu atât va fi mai greu să spargeți (spărgeți-o), prin urmare, este mai puțin probabil ca cineva să obțină acces neautorizat la datele dvs.

Atunci când alegeți o parolă, este recomandabil să utilizați semne de punctuație, cifre și un amestec de litere mari și mici. Se recomandă o lungime minimă de 8 caractere (parolele mai scurte sunt mai ușor de parcurs).
Din când în când, este necesar să schimbați parola. În acest fel, posibilitatea de detectare a acestuia scade.

Unele dintre cele mai frecvente greșeli la alegerea parolelor sunt:

- folosind cuvinte dintr-un dicționar
- parole bazate pe informații personale, cum ar fi numele sau data nașterii, locul de muncă etc.
- caractere care urmează ordinea dată pe o tastatură: 123, qwert etc.

Siguranța site-ului: pentru a vedea dacă un site web este sigur de vizitat, puteți verifica informațiile de securitate despre site. Verificați în stânga adresei web pentru starea de securitate:

- Dacă vedeți o pictogramă de lacăt lângă adresa unui site web înseamnă că traficul către și de la site este criptat.

De asemenea, este verificat, ceea ce înseamnă că compania care administrează site-ul are un certificat care dovedește că îl deține. Selectând pictograma de blocare, puteți vedea mai multe informații despre site, cum ar fi cine îl deține și cine l-a verificat.
Dacă nu vedeți pictograma de lacăt, conexiunea dvs. nu este privată și orice trafic ar putea fi interceptat.

Figura 6 – Identificarea pictogramei de lacăt.

Informații personale – câteva lucruri de avut în vedere!

Trebuie să fii atent la câte informații personale dezvăluiți online. Împărtășirea adresei, a numărului de telefon, a zilei de naștere și a altor informații personale poate însemna că aveți un risc mai mare de furt de identitate, urmărire și hărțuire. Acestea includ informațiile pe care le postați pe rețelele sociale.
Criminalii cibernetici vă pot strânge identitatea din informațiile care sunt disponibile public despre dvs., așa că gândiți-vă la informațiile pe care le distribuiți online.

Prin urmare, iată câteva lucruri de luat în considerare atunci când utilizați internetul:

- Utilizați o adresă de e-mail separată pentru cumpărături, grupuri de discuții și buletine informative. Dacă este necesar, puteți schimba această adresă fără a întrerupe activitățile de afaceri online.
- Partajați adresa dvs. de e-mail principală numai persoanelor pe care le cunoașteți.
- Dacă utilizați rețelele sociale, ajustați setările de confidențialitate pentru a controla cantitatea și tipul de informații pe care le partajați.
- Când creați un cont, acordați-vă timp pentru a vă familiariza cu politicile de confidențialitate ale rețelelor sociale.
- Faceți achiziții online numai de la companii care au o politică de confidențialitate clară și opțiuni de plată sigure
- Gândiți-vă înainte de a completa formulare online și aveți grijă cu cine și cum vă împărtășiți informațiile. Întrebați-vă, chiar trebuie să dau informațiile mele acestui site?

1.1.4. Activitati practice

După fiecare descriere teoretică a conținutului, vă sugerăm câteva dinamici de grup pentru a îmbunătăți învățarea. Aceste activități sunt descrise pas cu pas.

Atunci când oferă instruire, este important ca formatorii și cursanții să se simtă confortabil în cadrul grupului, astfel încât să se simtă fericiți să împărtășească experiențe, întrebări și așa mai departe. Cu cât oamenii se simt mai în largul lor cu colegii lor, cu atât experiența de învățare este mai bună. Prin urmare, sugerăm ca fiecare

activitate să înceapă cu un spărgător de gheață, dacă este posibil ceva distractiv care să le permită oamenilor să se prezinte grupului fără să se simtă intimidați.

La etapa de prezentare, trainerul ar putea dori să invite oamenii să împărtășească ceea ce ar dori să învețe, ce animal ar dori să fie, care este felul lor de mâncare preferat, ce culoare are periuța de dinți și orice alt subiect, având în vedere că este ceva care nu este prea personal.

Pasul 1: Spărgătorul de gheață „Sunt singurul"

Toată lumea se răspândește prin cameră formând un cerc închis. Antrenorul explică că o minge se va opri oprindu-se pe fiecare persoană din cerc. Cine are mingea trebuie să-și spună numele și un singur lucru pe care îl știu sau îl fac în grup. Ei pot vorbi, de asemenea, despre un interes sau un gust rafinat. Dacă un alt membru al grupului are aceeași abilitate, persoana care a vorbit trebuie să găsească altceva care este diferit.

Mingea nu trebuie să urmeze o comandă, așa că oamenii ar putea să o arunce oricui din grup, asigurându-se doar că fiecare persoană are șansa de a vorbi.

Puteți ajusta acest spărgător de gheață la un format online, indicând oamenilor să nominalizeze un coleg să vorbească în loc să arunce mingea.

Pasul 2: începerea brainstormingului

Pentru a introduce subiectul căutării online dar și pentru a vă aduna o idee despre unde se află oamenii din punct de vedere al cunoștințelor comune, începeți această unitate cu un brainstorming.

Asigurați-vă că aveți o tablă albă pregătită pentru a înregistra intrările tuturor. Dacă activitatea se desfășoară online, puteți folosi o platformă online pentru a vă sprijini cu înregistrarea (ex.https://padlet.com) sau chiar partajați un document Word cu grupul, unde puteți doar să tastați răspunsurile acestora.

Informați participanții că nu există răspunsuri corecte/greșite, deoarece ideea este să împărtășim grupului ceea ce știm deja/s-ar putea să nu știm. Întrebări posibile:

- Ce este o căutare online?
- Cum poate această cunoaștere să fie de ajutor în viața noastră de zi cu zi?
- Cum ajung informațiile pe internet?
- Ce fel de riscuri poti întâmpina în timpul căutării online?

Pasul 3: Căutare online – practic!

Arătați participanților diferite browsere web: Google Chrome, Safari, Mozilla Firefox, Edge, Internet Explorer, explicând că acestea sunt programe software pentru a accesa World Wide Web și a naviga prin diferite pagini; arătați participanților unde pot găsi browserele într-un computer; (10 minute)

De asemenea, puteți folosi următorul tutorial pentru a introduce subiectul cum să utilizați un motor de căutare: https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/

Formatorul arată cum să căutați „îngrășământ organic" (acesta este un exemplu, dar este recomandabil să alegeți un subiect semnificativ pentru grupul dvs.); Arătați grupului cum să caute pe diferite pagini și cum să folosească diferite „expresii de căutare"; (10 minute)

Acum, invitați fiecare participant să caute online informații despre pericolele știrilor false și să noteze trei fapte principale pe care le-au găsit; (20 de minute)

Discuție de grup: fiecare participant prezintă rezultatele căutării sale. (20 de minute)

Pasul 4: Analiza, stocarea și prezentarea informațiilor

Pregătiți o listă cu diferite subiecte pentru ca participanții să le exploreze online. Ex: sănătatea mintală în perioada pandemiei, cele mai bune rețete din lume, sporturile extreme, importanța albinelor, bolile copacilor, revoluția industrială, roboții în tehnologie, stilul de viață sănătos etc.

Cereți grupului să se organizeze în perechi și să aleagă un subiect pe care să se lucreze. Scopul principal al acestei activități este 1) de a compila informații de încredere cu privire la subiectul ales, 2) de a selecta și stoca informațiile pe desktop (într-un folder creat de student) și 3) de a crea o prezentare scurtă (10 minute) asigurându-se că au folosit surse de încredere. Cursanții trebuie să înregistreze site-urile web și referințele utilizate, deoarece acestea vor fi evaluate la sfârșit.

Pentru acei cursanți care ar putea să nu poată folosi software-ul pentru a lucra la prezentare, formatorul trebuie să furnizeze hârtie de flipchart și markere. Chiar dacă nu folosesc computerul pentru a prezenta informații, aceștia trebuie să poată căuta imagini, grafice sau videoclipuri pentru a-și ilustra căutarea și să le stocheze în folderul de pe desktop. (4 ore)

Odată terminată această sarcină, fiecare grup trebuie să prezinte lucrarea colegilor. (90 minute)

Pasul 5: Setări de confidențialitate online

Oferiți cursanților Studiul de caz 1 și 2. În plus, vă recomandăm să-i invitați să urmărească un tutorial rapid despre confidențialitate și securitate pe Chrome: https://www.youtube.com/watch?v=zMXI6waGFp4

- Împărțiți cursanții în două grupuri pentru a lucra la fiecare caz. Aceștia trebuie să citească și să răspundă la întrebări, susținute de informații online despre securitatea cibernetică. (30 minute).
- Fiecare grup va produce o fișă informativă[4], subliniind zece pași pentru a evita încălcarea confidențialității în timpul utilizării internetului (20 de minute)
- Dezbatere de grup (40 minute)

[4] Stagiarii pot face acest lucru pe computer sau pe o hârtie de flipchart, în funcție de abilitățile lor digitale preexistente.

Studiu de caz 1 - Jane

Citiți următoarea situație și discutați în cadrul grupului dumneavoastră ce sa întâmplat și răspundeți la întrebările de mai jos pentru a ghida dezbaterea. Apoi, notează concluziile principale pentru a-ți putea prezenta ideile grupului.

„Jane se conectează la internet, pregătindu-se pentru ceea ce majoritatea ar considera o experiență tipică, inofensivă de navigare pe Web. Jane cumpără niște haine pentru ea și copiii ei de doi și cinci ani de pe site-ul web al unui magazin universal. Ea urmează apoi cu o revizuire extinsă a unui site web care prezintă planuri de slăbire. Deși majoritatea ar considera această experiență de navigare o litanie de tranzacții banale, un agent de marketing direct priceput, cu capacitatea de a monitoriza în mod ascuns aceste activități, consideră informațiile obținute neprețuite. Oricât de surprinzător ar fi prea mulți navigatori, asamblarea unui profil alarmant de detaliat al lui Jane, fără știrea sau consimțământul ei, este foarte posibilă cu o singură activitate de navigare precum cea prezentată anterior. Deși acest scenariu necesită unele inferențe, un profil de marketing al tranzacțiilor lui Jane s-ar putea dezvolta după cum urmează: Jane este o mamă cu doi copii mici, cumpără niște bunuri de lux și este serios îngrijorată de greutatea și sănătatea ei. Pe baza ei, un comerciant sau vânzător ar putea dori să îi trimită lui Jane reclame, e-mailuri, bannere, reclame sau reclame pop-up care oferă echipamente scumpe pentru exerciții fizice. Echipamentul i-ar permite să stea acasă cu copiii ei, să-și ajute la atingerea obiectivelor de fitness și să fie accesibil, pe baza modelului ei de cheltuieli de consum observat. O reclamă pentru echipamentul de exerciții poate să nu o deranjeze deloc pe Jane. De fapt, ea ar putea fi de fapt interesată de echipamentul de exerciții de acasă în loc de un alt reclam care ar fi fost postat aleatoriu pe ecranul computerului ei în timp ce naviga pe web. In orice caz,

Groemminger, BK (2003). Confidențialitatea personală pe internet: ar trebui să fie un drept pentru spațiul cibernetic[5].

1) **Ce setări de confidențialitate sau ce acțiuni ar putea lua Jane pentru a evita ca informațiile ei să fie răspândite prin intermediul companiilor comerciale?** (Raspunsuri posibile mai jos)
- Ar trebui să fie atentă la permisiunile cookie-urilor, permițându-le doar pe cele necesare
- Ea ar putea șterge istoricul căutării odată ce a terminat sau să se conecteze ca anonim - acest lucru este deosebit de relevant dacă folosește un computer public
- Trebuie să se deconecteze de la e-mail sau de la alte conturi la care s-ar fi putut conecta.

2) **Ce fel de măsuri de siguranță ați lua în considerare atunci când faceți cumpărături online?**(Raspunsuri posibile mai jos)
- Verificați siguranța site-ului web - vedeți dacă este o conexiune sigură
- Creați un card virtual cu o anumită sumă de bani
- Utilizați platforme credibile pentru plăți precum PayPal
- Asigurați-vă că executați o scanare antivirus și computerul este securizat
- Evitați utilizarea unei conexiuni la rețea publică în timpul cumpărăturilor

[5] Accesibil Aici.

Studiu de caz 2 - Mary

Citiți următoarea situație și discutați în cadrul grupului dumneavoastră ce sa întâmplat și răspundeți la întrebările de mai jos pentru a ghida dezbaterea. Apoi, notează concluziile principale pentru a-ți putea prezenta ideile grupului.

Mary are 22 de ani și cunoaște foarte bine rețelele de socializare, deoarece se autointitulează „o influență". Ea crede că exercițiile fizice regulate și o alimentație bună sunt pilonii unui trai sănătos și scrie multe postări și sugestii pe Instagram despre asta. A ajuns la puțin peste 10000 de urmăritori și este foarte mândră de asta. Recent, unele persoane i-au scris, plângându-se că au căzut într-un atac cibernetic din cauza mesajelor trimise în numele ei. La început, ea nu știe cum să explice acest lucru, dar apoi își dă seama că a fost piratată. În urmă cu două zile, ea a primit un mesaj prin care se informa că a câștigat un concurs online. La început ea a găsit mesajul puțin suspect, deoarece nu a putut recunoaște expeditorul, dar apoi a dat clic pe link și a completat un formular cu detalii personale. Deoarece nu exista premiu, apoi a aflat că a fost o înșelătorie. Fiind conștientă de acest lucru, ea a postat o alertă pe rețelele de socializare prin care îi informează pe toți să nu deschidă mesaje de la ea.

1) **Ce altceva ar putea face Mary odată ce și-a dat seama ce s-a întâmplat?**(Raspunsuri posibile mai jos)
   - resetați parolele (e-mail, telefon, rețele sociale, servicii bancare etc.) și asigurați-vă că acele parole sunt puternice (minim 8 caractere cu majuscule, numere etc.)
   - asigurați-vă că antivirusul este actualizat / executați o scanare antivirus
   - face o copie de rezervă a datelor ei
   - duceți dispozitivul la un profesionist IT

2) **Ce ar putea face Maria pentru a evita această situație?** (Raspunsuri posibile mai jos)
   - Ar fi trebuit să verifice de două ori expeditorul și să nu deschidă niciodată mesajul/linkul dacă era suspect

1.2. Evaluarea datelor, informațiilor și conținutului digital

Unitatea 2 este legată de evaluarea informațiilor, evaluarea credibilității și a surselor acesteia.

Unitatea 1.2	Evaluarea datelor, informațiilor și conținutului digital
Durată	8 ore
Obiective	Să analizeze și să evalueze credibilitatea informațiilor online Să ia măsuri pentru a evalua diferite surse de informații Pentru a înțelege responsabilitatea fiecăruia atunci când împărtășesc informații greșite online Pentru a fi conștienți de modul în care valorile și judecățile personale influențează înțelegerea informațiilor
Conţinut	1.2.1 Cum se evaluează sursele și informațiile online 1.2.2 Evaluarea surselor dvs 1.2.3 Evaluarea site-urilor web 1.2.4 Site-uri web de verificare a faptelor 1.2.5 Activități practice
Resurse	Manual de instruire, calculatoare cu acces la internet, carduri True sau False
Metodologii de instruire	Prezentare de către trainer Exercițiu de grup Discuție / Dezbatere Lucrul în perechi/grupuri mici Prezentare de către participanți Selecția media

Masa 6- Structura unităţii de competenţă 1.2. Evaluarea datelor, informațiilor și conținutului digital al Modulului 1 – Informații și alfabetizare a datelor

1.2.1. Cum se evaluează sursele și informațiile online?

Când ați ajuns la această parte a manualului, aveți deja o idee clară despre informațiile pe care le puteți găsi online: aproape totul! Această afirmație introduce următoarea unitate, în care veți învăța cum să evaluați datele, astfel încât să puteți căuta surse de încredere și, prin urmare, să contribui la partajarea online a informațiilor faptice.

Spre deosebire de informații similare găsite în ziare sau emisiuni de televiziune, informațiile disponibile pe Internet nu sunt reglementate pentru calitate sau acuratețe. Prin urmare, este deosebit de important ca utilizatorul individual de internet să evalueze resursa sau informația. Rețineți că aproape oricine poate publica orice dorește pe Web. Adesea este dificil să se determine autoritatea surselor Web, așadar**este cu adevărat responsabilitatea ta să judeci acuratețea surselor tale**. În ciuda principalelor resurse pentru a face acest lucru este judecata și raționamentul dvs., există câteva acțiuni care vă pot ajuta să creșteți șansele în favoarea unor informații fiabile.

Pune-ți aceste întrebări înainte de a folosi resurse de pe internet:

1. Cine este autorul? Este autorul calificat să scrie pe această temă? În cazul în care este o organizație, este credibilă? Am auzit despre asta?
2. Care este scopul site-ului? Cine este publicul vizat?
3. Informația și limbajul sunt obiective, imparțiale și lipsite de expresii care stârnesc emoții?
4. Sunt enumerate sursele faptice pentru ca informațiile să poată fi verificate?
5. Informația este susținută de dovezi?
6. Câți ani au această informație? Când a fost actualizat ultima dată site-ul?

Ultimul, dar nu cel din urmă…Verifică-ți emoțiile!

Fii atent când un tittle are puterea de a-ți schimba starea emoțională. Aceasta nu este doar o tehnică foarte veche pentru a vă atrage atenția, dar a fost folosită ca un clickbait pentru răspândirea știrilor false. Înclinația noastră normală este să ignorăm nevoile de verificare atunci când reacționăm puternic la conținut, iar cercetătorii au descoperit că conținutul care provoacă emoții puternice se răspândește cel mai rapid prin rețelele noastre sociale (Matthew Shaer, 2014). Asa de,**citește dincolo de titluri**!

1.2.2. Evaluarea surselor dvs

În căutarea dvs. de informații, vă confruntați în cele din urmă cu provocarea de a evalua resursele pe care le-ați localizat și de a le selecta pe cele pe care le considerați a fi cele mai potrivite nevoilor dvs. Examinați fiecare sursă de informații pe care o localizați și evaluați sursele folosind următoarele criterii, cunoscute și sub numele de **Metoda TAARP:**

T – Promptitudine

Resursele tale trebuie să fie suficient de recente pentru subiectul tău. Dacă lucrarea dvs. este pe un subiect precum cercetarea cancerului, ați dori cele mai recente informații, dar un subiect precum cel de-al Doilea Război Mondial ar putea folosi informații scrise într-un interval de timp mai larg.

A – Autoritate

Informația provine de la un autor sau organizație care are autoritatea de a vorbi pe tema dvs.? Informațiile au fost revizuite de colegi? (Puteți folosi Ulrichsweb pentru a determina dacă un jurnal este revizuit de colegi). Își citează ei acreditările? Asigurați-vă că există suficientă documentație pentru a vă ajuta să determinați dacă publicația este fiabilă, inclusiv note de subsol, bibliografii, credite sau citate.

A – Publicul

Cine sunt cititorii vizați și care este scopul publicației? Există o diferență între o revistă scrisă pentru publicul larg și o revistă scrisă pentru profesori și experți în domeniu.

R – Relevanță

Acest articol are legătură cu subiectul tău? Ce legătură se poate face între informațiile prezentate și teza dumneavoastră? O modalitate ușoară de a verifica relevanța este prin revizuirea rezumatului sau a rezumatului articolului înainte de a descărca întregul articol.

P – Perspectivă

Sursele părtinitoare pot fi utile în crearea și dezvoltarea unui argument, dar asigurați-vă că găsiți surse care să vă ajute să înțelegeți și cealaltă parte. Sursele extrem de părtinitoare vor denatura adesea informațiile și acestea pot fi ineficiente de utilizat în lucrarea dvs.

1.2.3. Evaluarea site-urilor web

Site-urile web creează o provocare interesantă în evaluarea credibilității și a utilității, deoarece nu există două site-uri web create în același mod. Metoda TAARP descrisă mai sus poate fi utilizată, dar există lucruri suplimentare pe care doriți să le luați în considerare atunci când vă uitați la un site web:

Aspectul site-ului- Site-urile web de încredere au de obicei un aspect mai profesionist decât site-urile web personale.

Adresa URL a rezultatelor dvs- .com, .edu, .gov, .net și .org înseamnă de fapt ceva și vă pot ajuta să evaluați site-ul!

Resursele informaționale sunt cele care prezintă informații concrete. Acestea sunt de obicei sponsorizate de instituții de învățământ sau agenții guvernamentale. (Aceste resurse includ adesea .edu sau .gov.)

Resursele de advocacy sunt cele sponsorizate de o organizație care încearcă să vândă idei sau să influențeze opinia publică. (Aceste resurse pot include .org în adresa URL.)

Resurse de afaceri sau de marketing sunt cele sponsorizate de o entitate comercială care încearcă să vândă produse. Aceste pagini sunt adesea foarte părtinitoare, dar pot oferi informații utile. (De obicei, veți găsi .com în adresa URL a acestor resurse.

Resursele de știri sunt cele care oferă informații extrem de actuale despre subiecte fierbinți. De cele mai multe ori, sursele de știri nu sunt la fel de credibile ca jurnalele academice, iar credibilitatea ziarelor variază de la hârtie la hârtie. (Adresa URL va include de obicei .com.)

Paginile web personale/Resursele sunt site-uri precum site-uri de rețele sociale: bloguri, pagini Twitter, Facebook etc. Aceste surse pot fi utile pentru a determina ce spun oamenii despre un subiect și ce discuții au loc. Fiți foarte precauți dacă încercați să încorporați aceste surse direct într-o lucrare academică. Foarte rar, sau vreodată, vor avea vreo greutate în comunitatea academică

Există reclame pe site?- Reclamele pot indica faptul că informațiile pot fi mai puțin fiabile.

Verificați linkurile de pe pagină- Legăturile întrerupte sau incorecte pot însemna că nimeni nu are grijă de site și că alte informații de pe acesta pot fi depășite sau nesigure.

Verificați când pagina a fost actualizată ultima dată- Datele la care paginile au fost actualizate ultima dată sunt indicii valoroase despre actualitatea și acuratețea acesteia.

1.2.4. Site-uri web de verificare a faptelor

Din fericire, puteți utiliza și un site web de verificare a faptelor, unde puteți verifica în continuare dacă informațiile pe care le-ați găsit au fost semnalate ca false. În plus, puteți întreba un bibliotecar. Iată o listă cu câteva site-uri de verificare a faptelor (în funcție de țara dvs. de origine, poate fi interesant să căutați site-uri de verificare a faptelor pe știrile naționale. Cele pe care le prezentăm sunt în mare parte americane):

- FactCheck.org - https://www.factcheck.org/
- PolitiFact: sortarea adevărului în politică - https://www.politifact.com/truth-o-meter/
- Legende urbane: Politică -https://www.snopes.com/fact-check/category/politics/
- Adevar sau fictiune - https://www.truthorfiction.com/
- Observador Fact-Check (Portugalia) - https://observador.pt/seccao/observador/fact-check/

1.2.5. Activități practice

Pasul 1: Adevărat sau Fals?

Pentru a introduce subiectul despre cum să evaluăm veridicitatea informațiilor pe care le întâlnim online, începeți cu un joc rapid Adevărat sau Fals. Va trebui să pregătiți câteva cărți Adevărat/Fals în prealabil și să împărțiți cursanții în grupuri de trei. Veți prezenta câteva afirmații legate de subiect și fiecare grup va trebui să arate cardul Adevărat sau Fals, în funcție de răspunsul său. Poți corecta răspunsurile și oferi câteva informații despre subiecte pe măsură ce mergi.

Lista afirmațiilor:

	Afirmare	T/F
1	Toate informațiile postate online sunt de încredere.	Fals
2	Oricine poate adăuga informații online, chiar și pe enciclopedii	Adevărat
3	Există modalități de a verifica credibilitatea informațiilor.	Adevărat
4	Există un fenomen de „știri false” în întreaga lume.	Adevărat
5	Pentru a descoperi știri false, se poate verifica domeniul web.	Adevărat
6	Cu cât ceva este împărtășit mai mult, cu atât este mai probabil să fie adevăr.	Fals

7	Verificarea datei știrii nu este ceva demn de luat în considerare.	Fals
8	Valorile personale pot influența percepția cuiva a adevărului.	Adevărat
9	De obicei, este foarte ușor să identifici un nou fals.	Fals
10	Există site-uri de verificare a faptelor disponibile.	Adevărat

Masa 7 – Lista de afirmații și răspuns corect.

Pasul 2: Cum se răspândește dezinformarea?

Pentru a sprijini învățarea cum să evaluezi datele online, poți prezenta un videoclip rapid care arată cum se răspândesc știrile false.

Sugestie: https://www.youtube.com/watch?v=cSKGa_7XJkg

După aceasta, fiecare cursant poate implica propria căutare pentru a găsi două știri care pot fi adevărate și două știri care pot fi false. Ținând cont de informațiile oferite de formator cu privire la modul de evaluare a fiabilității datelor, cursanții vor trebui acum să folosească unele dintre aceste strategii pentru a selecta informațiile și a putea explica colegilor ce strategii au folosit.

Pasul 3: Activitate de povestire

Povestea următoare vorbește despre doi fermieri care se străduiesc să-și gestioneze afacerea într-un sat mic. Unul dintre ei cunoaște foarte bine instrumentele digitale, dar celălalt nu este foarte priceput în acest sens. Povestea evidențiază potențialul utilizării internetului pentru a răspândi zvonuri și știri false. Scopul principal al poveștii este de a atrage gânduri personale despre ce este o nouă falsă și cât de ușor poate cineva să o facă, dar și să ne gândim la impactul pe care îl poate avea asupra vieții noastre de zi cu zi și în întreaga lume.

De asemenea, ne propunem să promovăm o dezbatere despre avantajele internetului și cum poate fi util să ne ajute să ajungem rapid la informații, să ne sprijine să ne conectăm cu alții care ar putea să ne ajute etc. Îi sugerăm formatorului să prezinte următoarea poveste :

Erau doi bărbați într-un mic sat: Robert și Peter. Ambii erau oameni foarte muncitori, care conduceau ferme mari și propria lor afacere. Obișnuiau să vorbească foarte mândru despre produsele pe care le vând pe piețe, deoarece au urmat întotdeauna proceduri pentru a garanta standarde de calitate înalte.

Peter și Robert au fost întotdeauna vecini și se cunosc de peste 10 ani. Cu toate acestea, nu putem spune că relația lor a fost întotdeauna bună, deoarece au concurat întotdeauna pentru clienții obișnuiți ai satului și a orășelului din apropiere. Ei cred că nu există loc pentru ambii în afacerile unei zone atât de mici.

Într-una dintre plimbările sale de dimineață, Robert îl găsește pe Peter foarte îngrijorat de plantațiile sale, deoarece salatele sunt ruinate de ceea ce pare a fi o ciumă. Este supărat că nu a observat acest lucru mai devreme și se plânge că săptămâna aceasta nu se va vinde salată verde în piața orașului. El este, de asemenea, îngrijorat de faptul că, dacă clienții află ce s-a întâmplat, ar putea să-l vadă ca incompetent și să-și piardă încrederea în calitatea produselor sale. De asemenea, nu știe cum să facă față acestei ciumă, deoarece pare a fi un virus complet nou pe care nu l-a mai văzut până acum.

Între timp, Robert se gândește că, de fapt, acest eveniment nefericit ar putea fi o șansă pentru el de a distruge afacerea vecinului său odată pentru totdeauna! Deci, el decide să creeze un profil de Facebook al cuiva care ar fi cumpărat produsele lui Peter și este foarte nemulțumit. Pentru a acoperi și mai bine minciuna,

Robert a găsit câteva poze online și le-a adăugat în profil ca și cum ar fi poze cu produsele proaste ale lui Peter. Apoi, începe să trimită cereri de prietenie oamenilor din sat și rapid mesajul este răspândit în jur.

Câteva zile mai târziu, Peter își dă seama că profitul său a scăzut semnificativ, chiar și în vânzarea altor produse care nu au fost afectate de ciumă. Cu toate acestea, nu are idee ce a făcut Robert pe internet la spatele lui...

Întrebări sugerate pentru dezbaterea de grup:

- De ce crezi că profitul lui Peter a început să scadă?
- Dacă ai fi clientul lui Peter, cum crezi că te-ai simți urmărind imagini cu salate putrede? Ai mai cumpăra produsele lui?
- Cât de ușor crezi că este să răspândești un zvon și dezinformare online?
- Având în vedere impactul pe care l-au avut știrile false asupra afacerii lui Peter, cum credeți că ar putea afecta politica, de exemplu, sau problemele de sănătate publică legate de covid-19? Vă puteți gândi la vreo știre despre covid-19 pe care este posibil să le fi auzit și să nu fie adevărată?
- Acum imaginați-vă că erați în locul lui Peter... ați fi folosit internetul pentru a vă ajuta

1.3. Gestionarea datelor, informațiilor și conținutului digital

Unitatea 1.3	Gestionarea datelor, informațiilor și conținutului digital
Durată	8 ore
Obiective	Pentru a salva și stoca informații folosind diferite dispozitive Pentru a gestiona, a localiza și a prelua date Pentru a înțelege regulile privind drepturile de autor și licențele Pentru a fi la curent cu legile privind protecția datelor
Conținut	1.3.1 Dispozitive pentru salvarea și preluarea informațiilor 1.3.2 Drepturi de autor și protecția datelor 1.3.3 Activități practice
Resurse	Manual de instruire, calculatoare cu acces la internet, o pălărie, bucăți de hârtie, scară de la 1 la 5 (puteți folosi 5 lucrări numerotate de la 1 la 5), hârtii de flipchart, blu-tack sau orice material pentru a lipi hârtiile pe perete, markere colorate, scaune, masă, lingură, corn sau orice obiect pentru a produce un sunet de alarmă Acces la platforma de învățare colaborativă dacă se face online (ex: LAMS, Padle)
Metodologii de instruire	Prezentare de către trainer Exercițiu de grup Discuție / Dezbatere Lucrul în perechi/grupuri mici Prezentare de către participanți Învățarea prin cooperare

Masa 8- Structura unității de competență 1.3. Gestionarea datelor, informațiilor și conținutului digital al Modulului 1 – Informații și alfabetizarea datelor.

1.3.1. Dispozitive pentru salvarea și preluarea informațiilor

De-a lungul ultimelor unități, ați învățat cum să utilizați instrumentele computerizate pentru a naviga online, ținând cont de siguranța și confidențialitatea dumneavoastră. De asemenea, am abordat un subiect foarte important care vă permite să fiți un cetățean digital responsabil atunci când împărtășiți informații, evaluând veridicitatea datelor.

Acum scopul nostru este să vă ghidăm prin instrumentele disponibile pentru a vă salva informațiile, a le stoca și a le prelua oricând doriți.

În același mod în care îți ții hainele organizate în sertare, ai multe resurse în computer pentru a stoca informații. Mai jos vă prezentăm câteva dintre ele.

Dispozitive de memorie și stocare

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.

Figura 7 – identificarea și scurta descriere a dispozitivelor de memorie și stocare.

Pentru a stoca informații, există, de asemenea, un dispozitiv numit hard disk intern, care este încorporat în carcasa computerului și o unitate hard disk externă, care este conectată la un computer folosind un cablu adecvat sau un port USB și este de obicei folosită pentru a stoca informații. transfera date de la un computer la altul sau pentru backup.

Când descărcați informații de pe Internet, este important să ne amintim că folosim lucrările altor persoane, cum ar fi articole, cărți, imagini, videoclipuri, compoziții, jocuri video etc. Prin urmare, trebuie să înțelegem conceptele de drepturi de autor, licențiere și protejarea datelor. Cu toate acestea, în era digitală, a fost dificil să se stabilească legi privind drepturile de autor cu privire la informațiile postate online. De exemplu, rețelele sociale precum Facebook nu dețin lucrările postate pe site-ul lor, totuși trebuie să fiți de acord cu o licență prin care Facebook vă poate folosi munca în alte scopuri.

1.3.2. Drepturi de autor și protecția datelor

Drepturi de autor este un drept care este folosit pentru a proteja proprietatea intelectuală a autorului. Dacă cineva dorește să folosească o astfel de lucrare protejată prin drepturi de autor, trebuie să respecte condițiile în care autorul, în calitate de proprietar, a permis utilizarea operei sale (plata taxelor, referirea la original etc.).

Protecția datelor cu caracter personal

Carta drepturilor fundamentale a UE prevede că cetățenii UE au dreptul la protecția datelor lor personale.

„Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc" și „la acces la datele care au fost colectate care o privesc și dreptul de a le rectifica"[6]

Comisia Europeană și-a prezentat reforma UE în domeniul protecției datelor în ianuarie 2012 pentru a face Europa potrivită pentru era digitală. Peste 90% dintre europeni spun că doresc aceleași drepturi de protecție a datelor în întreaga UE – și indiferent de locul în care sunt prelucrate datele lor.

Directiva 95/46/CE este textul de referință, la nivel european, privind protecția datelor cu caracter personal. Acesta stabilește un cadru de reglementare care urmărește să găsească un echilibru între un nivel ridicat de protecție a vieții private a persoanelor și libera circulație a datelor cu caracter personal în Uniunea Europeană (UE). Pentru a face acest lucru, directiva stabilește limite stricte privind colectarea și utilizarea datelor cu caracter personal și cere ca fiecare stat membru să înființeze un organism național independent responsabil cu protecția acestor date. Directiva urmărește să protejeze drepturile și libertățile persoanelor cu privire la prelucrarea datelor cu caracter personal prin stabilirea unor orientări care determină când această prelucrare este legală. Orientările se referă la:

[6] Sursă: 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:
- confirmation as to whether or not data relating to him/her are being processed and communication of the data undergoing processing;
- 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.

Figura 8 – Orientări referitoare la protecția datelor cu caracter personal, astfel cum sunt stabilite în Directiva 95/46/CE.

1.3.3. Activitati practice

Pasul 1: Treci pălăria

Toată lumea se așează în cerc. În mijlocul cercului, antrenorul plasează o scară de la 1 la 5. Poate fi o foaie de hârtie cu numerele scrise sau 5 lucrări, fiecare cu un număr. Apoi, antrenorul explică că o pălărie va trece cu propoziții. Propozițiile descriu informații personale de la persoane reale care au fost postate online. Fiecare persoană trebuie să ia o bucată de hârtie din interiorul pălăriei, citind-o și plasând-o lângă un număr de la 1 la 5, unde 1 înseamnă „nu este o problemă gravă” și 5 înseamnă „problemă foarte gravă”.

Situații posibile:

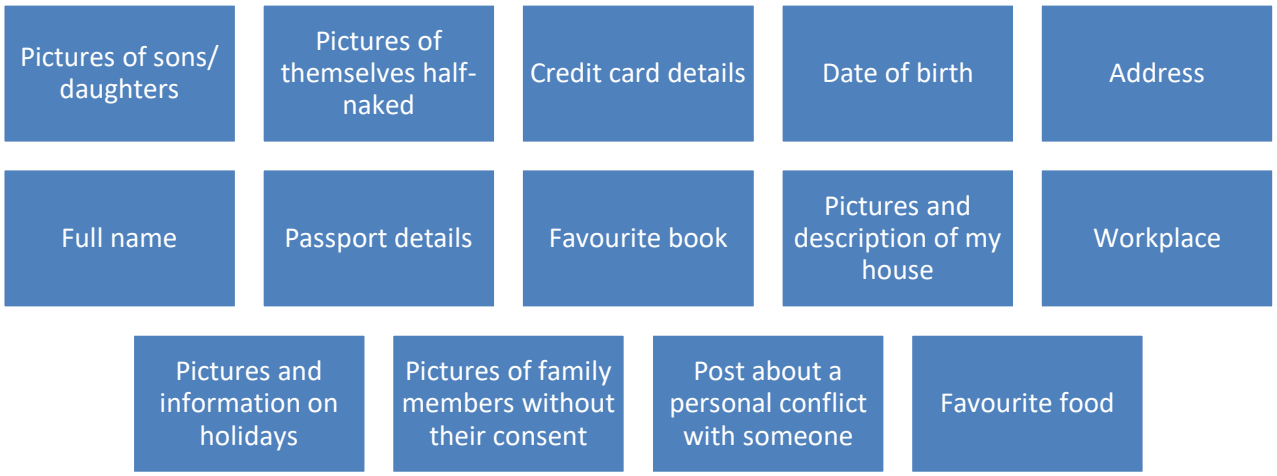


Figura 9 – Identificarea posibilelor situații de luat în considerare în această activitate.

Acestea sunt doar câteva exemple pe care le puteți folosi pentru a începe o conversație despre informațiile personale pe care toată lumea le partajează online, uneori fără să vă gândiți.

La sfârșitul activității, când toate propozițiile sunt sub numerele de la 1 la 5, ar fi interesant să discutăm despre modul în care oamenii le-au judecat pe fiecare dintre ele. De exemplu, de ce împărtășirea unei mâncăruri preferate nu este la fel de serioasă ca a împărtăși fotografii cu membrii familiei fără consimțământul acestora?

Pasul 2: Brainstorming pe jos

Această activitate este o introducere în subiectul regulilor privind drepturile de autor, licențierea și protecția datelor. Formatorul va lipi pe perete trei hârtii de flipchart (vă sugerăm să lipiți hârtiile cu blu-tack) numindu-le cu „copyright”, „licensing” și „data protection”.

Cursanții primesc markere de diferite culori și trebuie să se plimbe prin cameră și să scrie câte un cuvânt sau mai multe în fiecare lucrare, în funcție de ceea ce le vine în minte când se gândesc la fiecare subiect. Este important de subliniat că nu există răspunsuri corecte/greșite.

Odată ce toată lumea a scris cel puțin un cuvânt, puteți începe o discuție și apoi prezentați informații despre subiecte. Puteți adapta această activitate la un format online folosind platforme de învățare colaborativă. Vă sugerăm LAMS (Learning Activities Management System) care este o sursă gratuită și deschisă pentru a dezvolta acest tip de activități online.

Pasul 3: Testează-ți cunoștințele

Această activitate se bazează pe cunoștințele dobândite de cursanți în urma prezentării subiectelor din această unitate.

Formatorul instruiește clasa că va avea la dispoziție 30 de minute pentru a revizui tot ceea ce a fost predat în unitate. După expirarea timpului, clasa este împărțită în două grupe. Antrenorul așează o lingură pe o masă și cele două grupuri se vor așeza pe două rânduri față în față, în direcția mesei (vezi Figura 10).

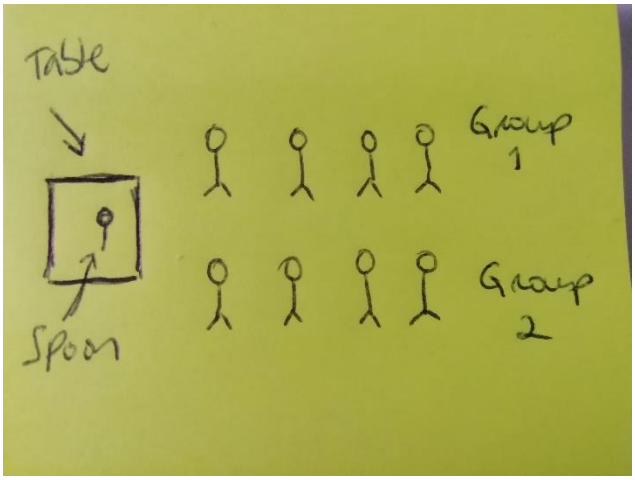


Figura 10 – Împărțirea cursanților în două grupuri.

- Cei doi cursanți cei mai apropiați de masă (trebuie să fie la aceeași distanță) vor fi responsabili de alegerea lingura atunci când aud o alarmă (formatorul va scoate un sunet). Echipa care alege prima lingura are dreptul de a răspunde la o întrebare.
- Formatorii trebuie să pregătească un set de întrebări referitoare la materiile predate.
- Fiecare răspuns corect câștigă 1 punct.
- Fiecare răspuns greșit primește -1 punct.
- Timpul pentru răspunsuri este de 1 minut (formatorul îl poate mări).

- În fiecare rundă, echipa schimbă membrul care alege lingura, astfel încât toată lumea are șansa să o facă. Dacă desfășurați această activitate online, poate fi necesar să o adaptați la un fel de „cine vrea să fie milionar?” joc.

Felicitări, ați finalizat acum Modulul 1.

Nu uitați să verificați Anexele pentru resurse și documente suplimentare furnizate pentru a sprijini auto-studiul!

Modulul 2: Comunicare și colaborare

Al doilea modul conține informații despre platformele colaborative și descrie subiecte legate de comunicare și interacțiune online.

Vă rugăm să rețineți că activitățile practice descrise în fiecare unitate pot presupune sprijinul unui formator cu experiență. Deși informațiile prezentate în manual sunt scrise într-un mod ușor de înțeles, unele acțiuni, adiacente informațiilor prezentate, pot necesita sprijinul unor oameni cu experiență.

Modulul 2	**Comunicare**					
Durată	25h					
Obiective	• A fi capabil să folosească tehnologiile online pentru a colabora cu alte persoane, cum ar fi schimbul de date și informații sau organizarea muncii în echipe. • A fi capabil să se comporte adecvat în mediul online. • A fi conștient de riscurile și beneficiile de a avea o identitate online.					
Unități	2.1 Interacțiunea prin tehnologii digitale	2.2 Partajarea prin tehnologii digitale	2.3 Implicarea în cetățenie prin tehnologii digitale	2.4 Colaborarea prin tehnologii digitale	2.5 Netichetă	2.6 Gestionarea identității digitale
Organizarea instruirii[7]	Față în față E-Learning	Față în față E-Learning	Față în față E-Learning	Față în față E-Learning	Față în față E-Learning	Față în față E-Learning
Durată	4h	4h	5h	3h	5h	4h

Masa 9 - Structura globală a Modulului 2 – Comunicare și colaborare.

[7]Poate fi: față în față, E-Learning. Învățare combinată sau auto-studiu.

2.1. Interacționând prin tehnologii digitale

Unitatea 2.1	Interacționând prin tehnologii digitale
Durată	4 ore
Obiective	• Fundamentele comunicării (Cum să comunici mai bine) • Cursanții vor lua în considerare importanța e-mailului, a căutării pe internet și a documentelor digitale • Cursanții vor folosi instrumente digitale pentru sarcinile de zi cu zi pe diferite platforme • Cursanții se vor familiariza cu rețelele sociale
Conţinut	2.1.1 Procesul de comunicare și stiluri de comunicare 2.1.2 Comunicare eficientă prin e-mail 2.1.3 Training Social Media pentru începători 2.1.4 Activități practice
Resurse	Proiector pentru prezentare Power-point (descărcați prezentarea de pe site) Dispozitive mobile/Statii de calculator/tablete Căști Exemple de proiecte
Metodologii de instruire	• Prezentare de către trainer • Exercițiu de grup Discuție / Dezbatere • Lucrul în perechi/grupuri mici • Prezentare de către participanți • Selecția media • Învățare bazată pe proiecte (PBL) • Clasa intoarsa

Masa 10- Structura unităţii de competenţă 2.1. – Interacțiunea prin tehnologii digitale ale Modulului 2 – Comunicare și colaborare.

2.1.1 Procesul de comunicare și stiluri de comunicare

Fundamentele comunicării

Canale și medii digitale

Un CANAL digital poate fi definit ca o interfață conectată la World Wide Web prin care se poate face comunicare.

- Pe Web – site-uri web
- Pentru căutare - rezultatele motorului de căutare
- Comunicare – aplicații de e-mail și mesagerie
- Evenimente online – webinar
- Media digitală - Site-uri de streaming video și muzică
- Jocuri – Jocuri virtuale

Un MEDIUM digital este o modalitate fizică de a stoca medii sau de a le arhiva și poate păstra

- Date
- Grafică
- Audio și video

Mediile digitale sunt bine cunoscute ca media digitale, adică forma de media care poate fi creată, vizualizată, modificată și distribuită de dispozitive electronice.

Stiluri de comunicare

- **Pasiv:**Comunicatorii pasivi acționează adesea cu indiferență și nu reușesc să-și exprime sentimentele sau nevoile, permițând altora să se exprime.

„Chiar nu contează atât de mult.”

- **Agresiv:**Comunicatorii agresivi se exprimă adesea într-un mod „tare” și tind să emită comenzi, să pună întrebări într-un mod nepoliticos și să nu-i asculte pe ceilalți.

„Am dreptate și tu greșești.”

- **Pasiv agresiv:**Acești comunicatori comunică cel mai probabil cu limbajul corpului și par să fie conștienți de nevoile lor, dar uneori se luptă să le exprime.

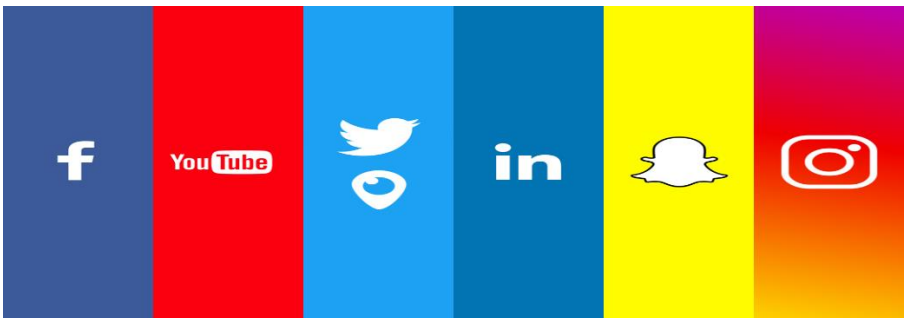
„Este în regulă pentru mine, dar să nu fii surprins dacă altcineva se enervează.”

- **asertiv:**Comunicatorii asertivi își pot exprima propriile nevoi, dorințe, idei și sentimente, luând în considerare și nevoile celorlalți.

„Respect drepturile altora.”

Social Media

Social Media se referă la mijloacele de interacțiune între oameni prin care aceștia creează, împărtășesc și schimbă informații și idei în comunități și rețele virtuale. Cele mai bune aplicații de socializare Facebook, Instagram, Twitter, LinkedIn, YouTube.



Activități practice

Modul	2
Unitate	2.1
Durată	3-4 ore
Tip de activitate	Activitate practică
Obiective	La sfârșitul activității, cursanții vor fi capabili: ♦ Comunicați și interacționați mai bine prin instrumente digitale ♦ Utilizarea platformelor online în funcție de destinatar și de conținutul pe care utilizatorul dorește să-l comunice ♦ Înțelegeți cum să utilizați toate instrumentele digitale și să vă familiarizați cu rețelele sociale
Setare	Pentru desfasurarea acestei activitati este nevoie de: ♦ Un proiector ♦ Slide-uri Powerpoint (descărcare de pe site) ♦ Hârtie și pixuri ♦ Dispozitive mobile ♦ Calculatoare ♦ O tablă ♦ Cretă
Activitate de debriefing	La sfârșitul activității, cursanții trebuie să se gândească la: ♦ Ce înseamnă să comunici și să interacționezi prin tehnologiile digitale. ♦ Ce avantaje aduce? Ce dezavantaje? ♦ Cum au schimbat aceste instrumente comunicarea personală și de grup în ultimii ani?

Pasul 1: 40-50 min

- Educatorul, după ce a cunoscut toți cursanții, începe prin a introduce modulul în diapozitive PowerPoint, dând o definiție generală a ceea ce este comunicarea și interacțiunea și a ceea ce este definit ca instrumente digitale.
- Educatorul va atribui fiecărui cursant un partener și apoi fiecărui cuplu o stație de calculator.
- Educatorul va cere fiecărui cuplu de cursanți să aleagă o aplicație, cum ar fi Word, pentru a scrie o scrisoare scurtă sau un paragraf.
- Discutați cu cursanții ce tip de comunicare sau ce interacțiune este o scrisoare.

Pasul 2: 30-40 min

Educatorul va prezenta prin diapozitive PowerPoint Fundamentele comunicării.

Educatorul va cere tuturor cursanților scrisoarea sau paragraful pe care l-au scris pentru a identifica cine este

a. Expeditorul
b. Destinatarul
c. Mesajul
d. Codul

Activitate de debriefing

- Educatorul va discuta cu toți cursanții și îi va întreba ce consideră ei drept canale de comunicare și le va cere să ofere câteva exemple
- Educatorul va enumera pe tablă toate exemplele de canale și medii de comunicare oferite de cursanți.
- Educatorul va prezenta prin diapozitive PowerPoint canale și medii de comunicare
- Educatorul va întreba cum ar clasifica ei canalele, formale, informale, neoficiale.

Pasul 3: 60 min

Această activitate este mai practică decât primele două activități, dar va combina și o anumită teorie, deoarece educatorul va introduce instrumentele digitale și va pune accent pe utilizarea unui cont online.

- Educatorul va introduce termenul nume de utilizator, parolă și cont online
- Educatorul va ghida cursanții către google.com pe stațiile lor de computer pentru a-și crea contul online
- Cursanții prin această activitate vor lucra în perechi și fiecare cuplu va împărți un cont
- Odată ce cursanții și-au creat contul Google, educatorul le va ghida și le va arăta pe Gmail și va explica formatul și aspectul acestui instrument.

- Cereți cursanților să compună o literă mică sau un paragraf mic în noua fereastră de mesaj

Activitate de debriefing

Educatorul va propune câteva întrebări de debriefing

- Cui ai trimite un e-mail? Ce ton ar folosi și de ce?
- Pentru ce tip de comunicare este cel mai bine e-mailul?
- Ce fel de media sau fișiere se poate atașa unui e-mail?

Pasul 4: 30-40 min

- Educatorul pe baza activității anterioare de debriefing va prezenta prin diapozitive PowerPoint stilurile de comunicare și stilurile de comunicare utilizate prin instrumente digitale
- Educatorul va prezenta și va numi toate rețelele sociale
- Educatorul va ghida cursanții pas cu pas pentru a crea un cont Facebook folosind adresa lor de e-mail Gmail și pentru a se conecta
- Educatorul va ghida cursanții să verifice toate funcțiile de pe Facebook și să trimită mesaje instantanee celorlalți colegi.
- De asemenea, educatorul îi va ghida pas cu pas în crearea unui mic post

2.2. Partajarea prin tehnologii digitale

Unitatea 2.2	Partajarea prin tehnologii digitale
Durată	4 ore
Obiective	• Conectarea cu ceilalți prin instrumente digitale • Configurarea folderelor partajate pe o anumită platformă • Utilizarea și editarea unui fișier partajat
Conţinut	2.2.1 Utilizați contul online pe o platformă digitală 2.2.2 Configurați un fișier partajat pe o platformă 2.2.3 Utilizați comentarii sau faceți ajustări pe un fișier partajat 2.2.4 Activități practice
Resurse[8]	Calculatoare/Tablete cu acces la internet Prezentare power point (descărcare de pe site) proiector PowerPoint Căști
Metodologii de instruire	• Prezentare de către trainer • Exercițiu de grup Discuție / Dezbatere • Lucrul în perechi/grupuri mici • Selecția media • Învățare bazată pe proiecte (PBL) • Stația de învățare

Masa 11- Structura unității de competență 2.2. – Partajarea prin tehnologii digitale a Modulului 2 – Comunicare și colaborare.

Partajarea prin tehnologii digitale

[8] Materiale si echipamente.

Tehnologiile digitale sunt instrumente, sisteme, dispozitive și resurse care generează, stochează sau procesează date. Unele dintre cele mai comune tehnologii digitale includ rețelele sociale, jocurile online, multimedia și dispozitivele mobile.

Ce înseamnă partajarea cu tehnologiile digitale?

Conform Cadrului de competență digitală 2.0, înseamnă a partaja date, informații și conținut digital cu alții prin tehnologii digitale adecvate, așa cum s-a menționat mai sus.

Instrumente digitale

- **Programe**: Word, Paint, Note
- **Site-uri web:** Google.com (Google drive)
- **Surse online:**Podcasturi, videoclipuri, rețele sociale

Să vedem cum poate cineva să partajeze un fișier pe Google Drive...

Ce este Google Drive?
Google Drive este o locație de stocare a fișierelor dezvoltată de Google. Este un serviciu pe internet disponibil ca site web și aplicație și permite stocarea fișierelor în „nor” și sincronizarea fișierelor pe dispozitive.
Acum hai să verificăm!!

1. Pe computerul dvs. accesați drive.google.com
2. Conectați-vă cu numele dvs. de utilizator și parola Google
3. Încărcați fișierul pe care l-am creat mai devreme pe Google Drive
4. Faceți clic pe fișierul încărcat și faceți clic pe Partajare
5. Sub „Oameni” introduceți adresa de e-mail a colegului dvs
6. Faceți clic pe trimite

Activități practice

Modul	2
Unitate	2.2
Durată	2 – 3 ore
Tip de activitate	Activitate practică
Obiective	La sfârșitul activității cursanții vor fi capabili: ♦ Conectarea cu ceilalți prin instrumente digitale ♦ Configurarea folderelor partajate pe o anumită platformă ♦ Utilizarea și editarea unui fișier partajat
Setare[9]	Pentru desfasurarea acestei activitati este nevoie de: ♦ Un proiector ♦ Slide-uri Powerpoint (descărcați prezentarea de pe site) ♦ Hârtie și pixuri ♦ Dispozitive mobile ♦ Calculatoare
Activitate de debriefing	La sfârșitul activității, cursanții trebuie să se gândească la: ♦ Ce înseamnă a împărtăși prin tehnologii digitale. ♦ Ce avantaje aduce? Ce dezavantaje? ♦ Cum au schimbat aceste instrumente schimbul de informații în ultimii ani?

Pasul 1: 10 min

Educatorul va prezenta cursanților conceptul de împărtășire și le va oferi, de asemenea, definiția acestuia.

Activitate de debriefing

Educatorul va propune câteva întrebări de debriefing:

- Ce tip de informații partajați de obicei?

[9]Vă rugăm să identificați echipamentele, materialele, documentele și orice suport necesar pentru realizarea acestei activități. În cazul în care creați un document justificativ, îl puteți adăuga și aici.

- Cum împărtășiți aceste informații?
- Ce instrumente sau platforme digitale ar putea fi folosite pentru a partaja aceste informații?

Pasul 2: 30-40 min

- Educatorul va introduce prin diapozitive PowerPoint instrumente digitale simple precum Word, Note sau Paint pentru a crea conținut
- Educatorul va cere cursanților de pe fiecare dintre stațiile lor computerizate să selecteze una dintre aplicațiile demonstrate pentru a crea conținut specific, fie pe bază de cuvinte, fie pe bază de imagini.
- Odată ce toți cursanții și-au creat fișierele, educatorul le va cere să salveze local pe stația lor de computer.
- Educatorul va prezenta cele mai comune platforme de partajare a conținutului, Facebook, Instagram, mail, YouTube, Google Drive, Dropbox

Pasul 3: 20 min

- Educatorul va cere cursanților să deschidă un instrument digital specific, cum ar fi Dropbox și să-i ghideze pas cu pas pentru a localiza fișierul pe care l-au creat înainte și a-l partaja prin Dropbox cu restul cursanților.
- Educatorul va cere apoi cursanților să deschidă o aplicație de social media, cum ar fi Facebook, și le va cere cursanților să partajeze fișierul creat ca postare.

Pasul 4: 10-20 min

- Educatorul va prezenta prin diapozitive pași simpli despre cum să editați un fișier partajat pe Dropbox.
- Educatorul va cere apoi cursanților să editeze toate fișierele care au fost partajate în folderul comun al platformei Dropbox

2.3. Implicarea în cetățenie prin tehnologii digitale

Această unitate vă va prezenta două concepte principale:

- Cetățenia digitală
- Conștientizarea securității cibernetice

Ne vom concentra pe înțelegerea modului de identificare a riscurilor de securitate cibernetică, a modului de prevenire și rezolvare a acestora.

Unitatea 2.3	**Implicarea în cetățenie prin tehnologii digitale**
Durată	5 ore
Obiective	- Înțelegeți conceptul de cetățenie digitală și de conștientizare a securității cibernetice - Identificați riscurile de securitate cibernetică - Cum să preveniți atacurile cibernetice
Conţinut	2.3.1 Cetățenia digitală 2.3.2 Concepte de bază 2.3.3 Securitate și confidențialitate 2.3.4 Activități practice
Resurse	Calculatoare și dispozitive mobile cu acces la internet Căști Proiector Powerpoint Prezentare power point (descărcare de pe site) Tabla de scris
Metodologii de instruire	- Prezentare de către trainer - Exercițiu de grup Discuție / Dezbatere - Simulare / Jocuri de rol - Selecția media - Învățare bazată pe proiecte (PBL) - Învățarea prin cooperare - Clasa intoarsa

Masa 12- Structura unităţii de competenţă 2.2. – Implicarea în cetățenie prin tehnologiile digitale din Modulul 2 – Comunicare și colaborare.

2.3.1 Cetățenia digitală

Cetățenia digitală se referă la comportamentul, implicarea pozitivă pe care o impun indivizii atunci când intră în lumea digitală. Mai detaliat, un cetățean digital este o persoană care are cunoștințele și abilitățile necesare pentru a utiliza eficient tehnologiile digitale pentru a comunica cu ceilalți, a participa în societate și a crea și consuma conținut prin instrumente digitale.

2.3.2 Concepte de bază

E-Safety

Acest concept a devenit un subiect fundamental în lumea digitală și include cunoștințele unui individ despre confidențialitatea pe Internet și modul în care comportamentul unui individ poate contribui la o interacțiune sănătoasă cu utilizarea internetului.
Pericole comune: phishing, programe malware, hărțuire cibernetică, accesarea și postarea de informații private.

Reputatie

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.

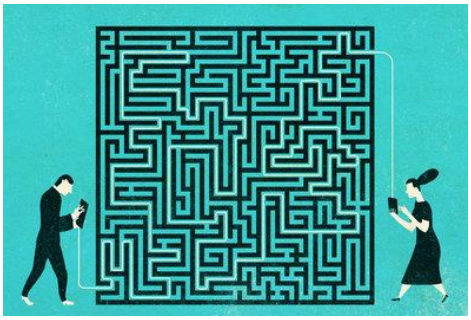
Digital Reputation is a concept that has shaped in such a way that has become more permanent than ever before since we as individuals have placed more trust in search results than any other source.

Relații

Relațiile digitale implică utilizarea tehnologiilor pentru a dezvolta o interacțiune mai interactivă și mai relevantă între indivizi.

Aceste tehnologii pot contribui atât pozitiv, cât și negativ în mod specific în relațiile personale, în funcție de modul în care indivizii folosesc tehnologia și pot crea probleme între parteneri care pot stârni conflicte și nemulțumiri în relație.

SAU



Etică

Etica digitală este studiul modului de a te gestiona etic profesional și într-o manieră prin medii online și digitale.

Câteva exemple de comportament etic sunt atunci când o persoană:

1. Solicită permisiunea de a colecta și stoca date despre utilizatori
2. Solicită permisiunea de a vinde orice date cu caracter personal care au fost stocate
3. I s-a oferit dreptul de a solicita ca datele despre acestea să fie șterse.
4. A primit acces la datele personale care au fost colectate și stocate

Urme digitale

Digital Footprints sau Digital Trails sunt înregistrări ale ceea ce o persoană caută, vizitează, creează, partajează, postează, instalează prin instrumente digitale pe un dispozitiv mobil sau pe o stație de computer.

Un cetățean bun

- Avocați pentru egalitatea drepturilor omului
- Îi tratează pe ceilalți cu respect
- Nu fură sau deteriora bunurile altora
- Comunică clar cu respect și empatie
- Vorbește sincer și nu repetă zvonuri nefondate
- Se protejează pe sine și pe ceilalți de vătămări
- Proiectează o imagine de sine pozitivă

Un bun cetățean digital

- Pledează pentru drepturi digitale egale pentru toți
- Încearcă să înțeleagă toate perspectivele
- Respectă confidențialitatea digitală, proprietatea intelectuală și alte drepturi ale oamenilor online
- Comunică și acționează cu empatie pentru umanitatea altora prin canale digitale
- Aplică gândirea critică tuturor surselor online, inclusiv știrilor false
- Este atent la sănătatea fizică, emoțională și mentală în timp ce folosește instrumente digitale.
- Înțelege permanența lumii digitale și gestionează în mod proactiv identitatea digitală.

2.3.3 Securitate și confidențialitate

Securitate- Numeroase procese care protejează informațiile personale ale unei persoane de alte persoane. Acest lucru se poate realiza prin diferite moduri:

- VPN, rețele private virtuale
- Programe antivirus
- Parole puternice

confidențialitate - Dreptul unei persoane de a-și păstra și proteja identitatea și de a menține un spațiu sigur și protejat în jurul integrității, prezenței fizice, gândurilor, sentimentelor și activităților intime.

În lumea digitală, confidențialitatea trebuie privită ca un drept de importanță crucială pentru indivizi, ca societate și ca colectiv.

2.3.4 Activități practice

Modul	2
Unitate	2.3
Durată	5 ore
Tip de activitate	Activitate practică
Obiective	La sfârșitul activității cursanții vor fi capabili: ♦ Înțelegeți conceptul de cetățenie digitală și de conștientizare a securității cibernetice ♦ Identificați riscurile de securitate cibernetică ♦ Cum să preveniți atacurile cibernetice
Setare[10]	Pentru desfasurarea acestei activitati este nevoie de: ♦ Calculatoare și dispozitive mobile cu acces la internet ♦ Căști ♦ Proiector Powerpoint ♦ Tabla de scris ♦ Cretă
Activitate de debriefing	La sfârșitul activității, cursanții trebuie să se gândească la: ♦ Cum interacționează oamenii online. ♦ Ca și online, trebuie să fii foarte atent cum comunici cu ceilalți. ♦ Cum să preveniți atacurile cibernetice ♦ Cum să protejați o stație de computer sau un dispozitiv mobil în timp ce navigați pe internet ♦ Cum se filtrează informațiile de pe internet și conținutul partajat
Pasul 1: 30-40 min	

[10]Vă rugăm să identificați echipamentele, materialele, documentele și orice suport necesar pentru realizarea acestei activități. În cazul în care creați un document justificativ, îl puteți adăuga și aici.

- Educatorul va avea o diapozitivă a agendei pentru a ajuta la menținerea lecției pe drumul cel bun și pentru a se asigura că cursanții vor ști și vor înțelege la ce să se aștepte în timpul instruirii
- Educatorul va prezenta modulul tuturor cursanților prin diapozitivele PowerPoint și va explica conceptul de cetățenie digitală.
- Cereți cursanților care își folosesc posturile să vizioneze două videoclipuri bazate pe probleme care se concentrează pe motivul pentru care este importantă cetățenia digitală.

Activitate de debriefing

- Educatorul va discuta cu cursanții ce au înțeles ei până acum prin termenul de cetățenie digitală
- Educatorul va discuta, de asemenea, cu cursanții, amenințările și riscurile cu care se confruntă atunci când nu caută site-uri web sigure și cum să gestionezi problemele legate de rețelele sociale.

Pasul 2: 60 min

- Educatorul va introduce conceptele de bază ale Cetățeniei Digitale
- Educatorul va oferi exemple cursanților și îi va ajuta să devină alerti pe internet
- Educatorul va încuraja cursanții să facă schimb de idei între ei și să demonstreze conștientizarea pericolelor, oferind scenarii de caz.
- Educatorul va ilustra cele două scenarii de caz și va discuta punctele cheie ale fiecărui scenariu
- Odată ce cele două scenarii sunt elaborate, educatorul va crea apoi pe tablă o diagramă cu trei coloane cu termenii „Sigur”, „Responsabil” și „Respectuos” înscriși în partea de sus a fiecărei coloane.
- Invitați cursanții să furnizeze cuvinte sau expresii care descriu modul în care oamenii pot acționa online în siguranță, responsabil și respectuos și scrieți-le în coloana corespunzătoare
- Rugați-i pe fiecare dintre cursanți să folosească câte o bucată de plastic și să îl sfărâmă în bucăți, să explice ce va cauza acest lucru mediului înconjurător și să o coreleze cu amprenta digitală atunci când aceștia nu acționează într-o manieră sigură, responsabilă și respectuoasă.

Pasul 3: 50 min

- Educatorul va introduce conceptul și definiția traseului și amprentei digitale
- Educatorul va oferi tuturor cursanților fișe pentru a nota ceea ce știu deja, ceea ce doresc să știe și ceea ce au învățat.
- Educatorul va cere doi voluntari să participe la un joc de rol

  Spuneți: „Imaginați-vă că mergeți pe o stradă aglomerată și un străin complet se apropie de tine și spune că tocmai ai câștigat o excursie gratuită – tot ce trebuie să-i dai este numele tău, vârsta, adresa, numărul de telefon și parolele pentru rețeaua ta de socializare. conturi (Google+, Facebook etc). L-ai crede?”

Activitate de debriefing

Educatorul va distribui o evaluare ulterioară care va fi discutată între cursanți

Pasul 4: 45 min

- Educatorul va începe prin a întreba cât de importantă este confidențialitatea lor pentru ei sau o va evalua de la 1 la 5 și va înregistra informațiile pe tablă.
- Educatorul va întreba apoi cursanții care spun că nu este important să aibă intimitate și îi va încuraja pe ceilalți cursanți să dezbată pe această temă.
- Folosind câteva exemple oferite din dezbatere, discutați cu toți cursanții ce înțeleg ei prin termenul de securitate și confidențialitate
- Educatorul va oferi definiția confidențialității și securității și va oferi exemple utilizate pe instrumentele digitale

La sfârșit, educatorul va depăși ceea ce s-a discutat în unitate și va explica drepturile pe care fiecare le are ca cetățean digital și va cere setările de securitate și confidențialitate ale conturilor de rețele sociale pe stațiile lor de computer.

2.4. Colaborarea prin tehnologii digitale

Unitatea 2.4	Colaborarea prin tehnologii digitale
Durată	3 ore
Obiective	• Învățarea cursanților cum să folosească instrumentele digitale pentru a colabora online cu alții.
Conținut	2.4.1 Colaborarea prin tehnologii digitale – concepte principale 2.4.2 Activități practice
Resurse	Tabla de scris Bucăți de hârtie Pixuri Borcan Calculatoare
Metodologii de instruire	• Prezentare de către trainer • Exercițiu de grup Discuție / Dezbatere • Lucrul în perechi/grupuri mici • Selecția media

Masa 13- Structura unității de competență 2.5. – Colaborarea prin tehnologii digitale a Modulului 2 – Comunicare și colaborare.

2.4.1 Colaborarea prin tehnologii digitale – concepte principale

Scopul acestei unități este de a-i învăța pe elevi ce înseamnă să colaborezi prin tehnologii digitale, să cunoască cele mai comune instrumente de colaborare online și să poată identifica instrumentul potrivit pentru o anumită nevoie.

Definiția Colaborării prin tehnologii digitale:

Conform definiției din Cadrul Competenței Digitale 2.0, colaborarea prin tehnologii digitale înseamnă: „a folosi instrumente și tehnologii digitale pentru procese colaborative și pentru co-construcție și co-creare de resurse și cunoștințe”.

De ce este atât de importantă colaborarea prin tehnologii digitale?

În zilele noastre suntem din ce în ce mai obișnuiți să folosim tehnologiile digitale, în viața privată și profesională pentru a interacționa cu ceilalți.

Schimbul de documente, fotografii, informații sau folosirea mediului online pentru a organiza munca sau studiul a devenit din ce în ce mai important, mai ales că pandemia de Covid 19 ne-a obligat să trăim, să muncim și să studiem acasă. Există o serie de instrumente care ne permit să schimbăm informații în mediul online, într-un mod rapid și ușor.

Mai ales într-un mediu de lucru, a devenit esențial să putem interacționa cu colegii sau cu alte persoane online, să facem schimb de documente și informații și să putem gestiona sarcini, organiza întâlniri etc. Instrumentele digitale ne vor ajuta să gestionăm munca (nu doar de la distanță).), accelerează schimbul de informații și crește productivitatea echipei.

Care sunt cele mai utile instrumente de colaborare într-un mediu online?

După cum am menționat deja, există multe instrumente care ne ajută să colaborăm online cu alții. Mai jos am dori să împărtășim și să recomandăm câteva dintre ele:

Skype; Mergi la sedinta; Întâlniri Zoom; Google Meet; Echipe Microsoft: Toate aceste instrumente sunt instrumente de conferințe web și de întâlniri online care permit oamenilor să organizeze întâlniri de la distanță sau să se vadă cu ușurință atunci când oamenii sunt departe. De asemenea, puteți să partajați ecranul și să afișați prezentări și fișiere altor participanți.

Google Drive; Dropbox: Cu aceste aplicații, puteți salva fișiere și le puteți stoca într-un spațiu online, separat de dispozitivele dvs. Acest lucru este util deoarece puteți recupera fișierul chiar dacă dispozitivele dvs. au unele probleme, presupunând că le-ați arhivat aici. Mai mult, datorită acestor instrumente veți putea lucra și colabora cu alte persoane având posibilitatea de a vă împărtăși spațiul sau documentele cu colegii, prietenii sau membrii familiei sau oricine doriți.

Google Calendar; Echipa sus: Acestea sunt aplicații concepute ca o agendă. Arată ca un calendar pe care îl poți organiza și personaliza. Interfața este foarte simplă în ambele și puteți decide să afișați o singură zi, o săptămână sau chiar intervale de timp mai lungi. Puteți să vă marcați întâlnirile, să programați întâlnirile și chiar să le împărtășiți altor persoane.

Trello; Redbooth; Asana: Acestea sunt instrumente de management de proiect care ajută în activitățile de lucru. Puteți să creați liste, să atribui sarcini altor membri ai echipei dvs. care împart același spațiu, să stabiliți termene limită și să personalizați totul cât mai eficient posibil.

Formular Google: Aplicația google vă permite să creați sondaje liber și foarte ușor. Vă puteți personaliza sondajele și puteți utiliza diferite moduri de a pune întrebări: răspunsuri multiple, răspunsuri deschise, scoruri de satisfacție etc.

2.4.2 Activități practice

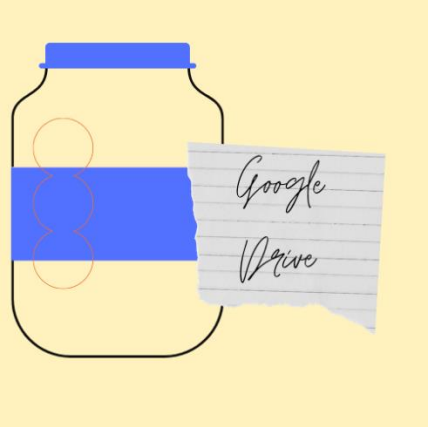
Pasul 1: Borcanul cu unelte

Educatorul enumeră mai multe instrumente care ar putea fi propuse cursanților.

Toate instrumentele pe care le sugerăm sunt instrumente digitale open-source. Educatorul poate introduce câte instrumente dorește (cel puțin unul per elev).

Vă sugerăm următoarele: Google Drive, Trello, Dropbox, Google Calendar Google Form etc.).

Educatoarea scrie numele instrumentului pe o bucată de hârtie și o introduce în borcan.



În acest moment, este rândul cursanților: pe rând, cursanții iau o bucată de hârtie în borcan și spun cu voce tare numele instrumentului pe care l-au găsit.

Educatorul propune elevului și clasei câteva întrebări:

- La ce se folosește acest instrument?
- Ați folosit vreodată acest instrument?
- Știți cum funcționează?
- Cunoașteți și alte instrumente care funcționează în același mod?
- Credeți că acest instrument este util pentru a stimula colaborarea?

Educatorul va conduce discuția, dar va încerca să stimuleze conversația dintre cursanți.

Când toate notele din borcan sunt terminate, educatorul va nota pe o tablă toate numele instrumentelor care au apărut și va explica mai bine cursanților cum funcționează.

La finalul activității, educatorul va propune câteva întrebări de debriefing:

- Știi ce înseamnă să colaborezi prin tehnologii digitale?
- Cum pot instrumentele pe care le-am văzut să ajute oamenii să colaboreze mai rapid și mai ușor?

Pasul 2: Să încercăm!

Această activitate este mai practică decât prima și servește la punerea în practică a cunoștințelor mai teoretice dobândite în prima parte.

Cursanții lucrează în perechi.

Educatorul le atribuie un instrument pentru a fi testat dintre cele menționate în prima activitate.

În acest moment, în funcție de instrumentul „primit", educatorul va cere cursanților să îndeplinească sarcini mici.

Sarcinile pot fi multe și diferite și depind de instrumentele pe care educatorul decide să le prezinte cursanților săi.

Crearea unui folder partajat, trimiterea unui fișier greu, stabilirea unei întâlniri online și invitarea unor persoane de contact etc.

Cursanții vor încerca timp de 30 de minute un instrument și se pot roti cu alții pentru a permite tuturor să încerce cât mai multe instrumente posibil.

La finalul activității, educatorul va propune câteva întrebări de debriefing:

- Ți s-au părut utile instrumentele pe care le-ai încercat?
- Le cunoști deja?
- Crezi că sunt utile în contextul muncii și nu numai?
- La ce le-ai folosi?

2.5. Neticheta

Unitatea 2.5	Neticheta
Durată	5 ore
Obiective	Învățarea cursanților comportamentul corect care ar trebui păstrat într-un mediu online.
Conţinut	2.5.1 Ce înseamnă netichetă? 2.5.2 Activități practice
Resurse	O tablă; Cretă; Postează; Hârtie și pixuri Studiu de caz 1 Studiu de caz 2
Metodologii de instruire	Exercițiu de grup Discuție / Dezbatere Lucrul în perechi/grupuri mici

Masa 14- Structura unităţii de competenţă 2.6. – Neticheta Modulului 2 – Comunicare și colaborare.

2.5.1 Ce înseamnă netichetă?

Scopul acestei unități este de a învăța cursanții să păstreze un comportament corect în mediul online. Respectarea celorlalți și a locurilor în care ne aflăm este la fel de importantă în mediul fizic ca și în cel online. Predarea acestor subiecte este foarte importantă, mai ales că oamenii online devin mai agresivi sau mai răutăcioși față de ceilalți. Există multe exemple de fenomene legate de comportamentul rău online, cyberbullying, body-shaming sunt doar câteva exemple de comportamente la care asistăm zilnic pe web, ca să nu mai vorbim de episoade de rasism și ură față de minorități în general. Educația pentru a-i respecta pe ceilalți este esențială pentru a preveni un astfel de comportament.

Definiţia Netiquette

Conform definiției din Digital Competence Framework 2.0, netiquette înseamnă: „A fi conștient de normele comportamentale și de know-how în timp ce utilizați tehnologii digitale și interacționați în medii digitale. Să adapteze strategiile de comunicare la publicul specific și să fie conștient de diversitatea culturală și generațională în mediile digitale”.

Ce comportamente sunt considerate un exemplu prost de netichetă?

În general, putem considera drept exemplu prost de netichetă toate acele comportamente online care sunt lipsite de respect față de ceilalți. Aceste atitudini pot fi de diferite caractere.

Nerespectarea proprietății intelectuale:partajarea de conținut, fotografii, materiale ale altora fără a cita sursa este considerată greșită și un exemplu de netichetă proastă (Pe lângă faptul că implică obligații legale pe care nu le vom discuta aici).

Ar trebui să verificăm întotdeauna de unde obținem acest conținut și să vedem dacă este open source sau dacă trebuie să citățm sursa atunci când îl folosim.

Nerespectarea opiniilor altora:nerespectarea opiniilor altora și, prin urmare, adoptarea de atitudini ostile și jignitoare față de acești oameni este un exemplu de netichetă proastă. Ar trebui să încercăm întotdeauna să stabilim un dialog cu ceilalți, fără a folosi cuvinte sau tonuri care sunt nepotrivite sau care îi pot jigni pe alții.

Exprimându-ne într-un mod lipsit de respect:Când scriem un mesaj, un e-mail sau o postare trebuie să fim conștienți de modul în care scriem și cum ne exprimăm ideile. Amintiți-vă întotdeauna că oamenii de cealaltă parte nu văd expresiile noastre sau ne aud tonul vocii și acest lucru poate duce la neînțelegeri. De aceea este important să fii atent când te exprimi online. Folosirea unui limbaj ambiguu sau ostil, folosirea majusculelor, nesemnarea, necontextualizarea conținutului mesajului dvs. sunt doar câteva exemple de netichetă proastă. Amintiți-vă, de asemenea, să folosiți un limbaj formal sau informal, în funcție de persoana cu care aveți de-a face, fie că este un prieten, o cunoștință, un coleg sau un străin.

Nerespectarea intimității celorlalți: Mulți oameni împărtășesc o mulțime de fotografii sau informații private despre ei înșiși pe rețelele sociale, dar aveți grijă să respectați întotdeauna confidențialitatea celorlalți și să nu distribuiți niciodată date sensibile fără permisiunea celeilalte persoane.

2.5.2 Activități practice

Pasul 1: Care dintre ele nu aparține?

Educatorul scrie pe o tablă diferite comportamente online care au legătură cu neticheta, câteva exemple pozitive și câteva exemple negative.

În această primă activitate, cursanții ar trebui să afle care elemente nu au nicio legătură cu celelalte într-un grup de exemple bune și rele de netichetă.

Scopul exercițiului este de a identifica comportamentele rele din interiorul celor bune.

Sunați câte un elev la tablă și cereți-i să încercuiască exemple proaste de netichetă.

În final, educatorul va corecta răspunsurile date de cursanți.

La finalul acestei activități, educatorul invită cursanții să reflecteze asupra comportamentului pe care oamenii îl păstrează online. Educatorul va propune câteva întrebări de debriefing:

- Care sunt comportamentele care te fac să fii inconfortabil online?
- În mediul online, ați observat vreodată folosirea unui comportament rău de către utilizatori?
- Ai încercat vreodată să explici altora ce este neticheta?

Sfaturi:

- Această activitate se poate face și folosind note post-it de agățat pe un perete.
- Această activitate se poate face și online, folosind un instrument precum jamboard (https://jamboard.google.com/).

Pasul 2: războinic cu tastatura

Pentru acest exercițiu, educatorul propune cursanților diferite texte în care oamenii interacționează între ei online (adică, chat, e-mail, întrebări frecvente, comentarii etc.).

Două studii de caz pot fi utilizate în această activitate.

Studiu de caz 1

Un schimb de e-mail între doi colegi

Anna și Elisabeth sunt două colege care lucrează în aceeași companie. Anna lucrează în departamentul administrativ de vânzări în timp ce Elizabeth gestionează relația cu clientul și organizarea evenimentelor. Elisabetta a comandat niște fluturași și afișe pentru a face publicitate evenimentului, dar au existat întârzieri la livrare.

Obiect: Festivalul de vară_întârzieri de livrare

Anna:

Dragă Elizabeth, îți scriu cu referire la ordinea de fluturași și afișe pentru petrecerea de vară pe care ai cerut-o. Din păcate, din cauza pandemiei de Covid 19, tipografia noastră ne-a informat că va exista o întârziere în livrare.

Vă voi anunța imediat ce primim materialele.

Cu sinceritate,

Anna

Elisabeta:

Bună Anna. Înțeleg că Covid a creat multe probleme, dar aceasta este o problemă foarte serioasă pentru organizarea festivalului. Eu sunt cel care trebuie să vorbească cu clientul, ce să-i spun?

CUM PROMOVEZ EVENIMENTUL ACUM?

Clientul dorește materialele până la sfârșitul săptămânii. FĂRĂ SCUZE.

SCHIMBATI GRAMATUL daca este necesar! MĂ ÎNȚELEGI?

Anna:

Draga Elisabeta,

Îmi pare foarte rău că această întârziere cauzează probleme cu munca dvs.

Din păcate, am plătit deja materialul în avans și nu putem primi banii înapoi în acest moment. Vă rugăm să încercați să explicați situația clientului dvs., sunt sigur că va înțelege.

Încrezător în cooperarea dumneavoastră,

Îți doresc o zi bună.

Cu sinceritate,

Anna

Elisabeta:

Voi încerca să-i explic situația și voi cere mai mult timp, dar nu vreau să îmi asum responsabilitatea pentru această problemă, dacă este cazul, voi da numărul directorului de servicii.

AȘA VOI GESTIONA ACEASTA PROBLEMA.

Elisabeta

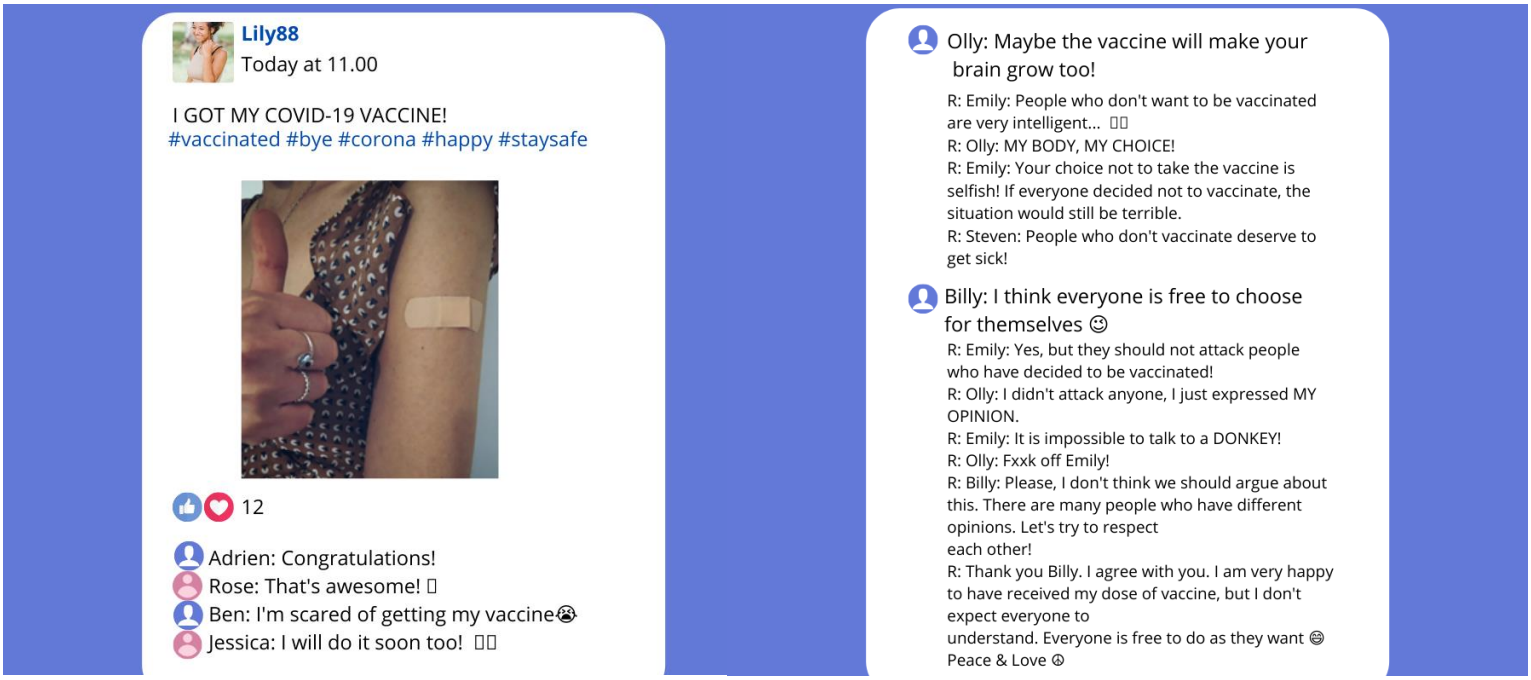
Educatorul invită cursanții să reflecteze asupra textului:

- Cum apare Anna? Are sau nu o atitudine drăguță față de Elisabeth?
- Și Elisabetta la Anna?
- Care este atitudinea Elisabetei față de problemă? Este cuprinzătoare pentru colegul ei sau nu?
- În text, există câteva exemple de netichetă proastă. Poți afla care sunt acestea?

După ce au răspuns la întrebările educatorului, participanții ar trebui să încerce să rescrie textul transformând comportamentele din negative în pozitive.

Studiu de caz 2

O fată (Lily) postează pe profilul ei de Facebook o fotografie după ce a primit prima doză de vaccin împotriva Covid 19:



Educatorul invită cursanții să reflecteze asupra textului:

- Ce crezi că este neticheta proastă în aceste comentarii?
- Cum ai fi reacționat la comentariul lui Olly?
- Crezi că Emily i-a răspuns corect lui Billy?
- Cine crezi că a acţionat corespunzător în aceste comentarii?
- Puteți găsi exemple proaste și bune de netichetă în text?
- De ce crezi că este mai ușor să fii răutăcios online?
- Ai fost vreodată un războinic cu tastatura?
- Ce faci când recunoști că cineva folosește un comportament răutăcios online?

După ce au răspuns la întrebările educatorului, participanții ar trebui să încerce să rescrie textul transformând comportamentele din negative în pozitive.

Pasul 3: Manifestul Netiquette

În ultima activitate, educatoarea merge la tablă și le cere cursanților să scrie împreună „Manifestul Netiquette", adică toate comportamentele pozitive pe care le consideră că ar trebui păstrate online.

Cursanții ar trebui să discute care sunt regulile principale și apoi să enumere aproximativ zece exemple de netichetă bună.

Acesta este „Manifestul Netiquette" al clasei și toată lumea trebuie să se angajeze să-l respecte.

Odată ce manifestul a fost decis, educatorul poate explica cursanților o scurtă explicație a teoriei netichetei.

La sfârșitul activității, educatorul invită cursanții să reflecte cu atenție modul în care oamenii ar trebui să interacționeze online și modul în care cursanții ar dori să răspândească și să predea altora regulile pe care le-au scris (folosind rețelele sociale? Partajarea manifestului? Etc.)

2.6. Gestionarea identității digitale

Unitatea 2.6	Gestionarea identității digitale
Durată	4 ore
Obiective	Învățarea cursanților ce înseamnă să ai o identitate digitală și cum ar trebui să aibă grijă de ea.
Conţinut	2.6.1 Definiții și protejarea identității 2.6.2 Activități practice
Resurse	Hârtie și pixuri Calculatoare
Metodologii de instruire	Exercițiu de grup Discuție / Dezbatere Lucrul în perechi/grupuri mici Simulare / Jocuri de rol

Masa 15- Structura unităţii de competenţă 2.7. – Gestionarea identității digitale a Modulului 2 – Comunicare și colaborare.

2.6.1 Definiții și protejarea identității

Acest modul își propune să îi facă pe cursanți să conștientizeze toate informațiile pe care le lăsăm online despre noi înșine și care reprezintă identitatea noastră digitală. Identitatea digitală este ceva care se referă la noi, la persoana noastră. De exemplu, atunci când folosim un ID și o parolă pentru a ne autentifica pe un site web, ne folosim identitatea digitală. În zilele noastre, trăim într-o lume în care tot mai multe servicii ne impun să ne logăm de pe dispozitive, atât private, cât și publice. Comerțul electronic, serviciile bancare, serviciile de sănătate, serviciile fiscale sunt doar câteva exemple. De fiecare dată când ne înregistrăm identitatea digitală sau facem anumite acțiuni online, datele noastre private sunt preluate și înregistrate, adesea fără ca utilizatorul să-și dea seama. Acesta este motivul pentru care trebuie să fim conștienți și să învățăm cum să ne gestionăm cel mai bine identitatea digitală online.

Definiția managementului identității digitale

Conform definiției din Digital Competence Framework 2.0, gestionarea identității digitale înseamnă: „A crea și gestiona una sau mai multe identități digitale, a-ți putea proteja propria reputație, a face față datelor pe care le produce prin mai multe instrumente digitale, medii. și servicii”.

De ce trebuie să ne facem griji pentru datele noastre?

De fiecare dată când suntem de acord cu confidențialitatea pentru a accesa un site, a descărca o aplicație, a răspunde la sondaje pe rețelele sociale sau pentru a intra pe un site folosind informațiile noastre, generăm date. Aceste date sunt relevante pentru multe companii, deoarece dezvăluie comportamentul consumatorilor. Adesea dăm datele noastre sau ne consimțăm pentru utilizarea lor, fără măcar să fim conștienți de acest lucru.

Dar online nu lăsăm doar urme din ceea ce ne place și nu ne place ca consumatori, lăsăm și informații private foarte importante care, dacă sunt folosite de alții, ne pot fi foarte dăunătoare. Gândiți-vă doar la detaliile cardului nostru de credit sau la conturile noastre sociale cu fotografii și informații personale.

Furt de identitate

Când identitatea noastră digitală este piratată și datele personale sau financiare ne sunt furate, putem vorbi de infractori cibernetici. Sunt oameni specializați în furturi online. Ne sparg sistemele sau folosesc trucuri pentru a ne face să credem că ne pot oferi datele noastre pe site-uri sau aplicații securizate, când de fapt ni le fură.

Usurându-vă identitatea, acești criminali vă fură banii și informațiile. De exemplu, unii influenți (oameni foarte celebri pe rețelele de socializare) au anunțat că le-a fost furată identitatea de către un hacker, care le-a furat conturile de pe rețelele de socializare și a cerut o răscumpărare pentru a le restitui.

Cum să ne apărăm de infractorii cibernetici?

În primul rând cu conștientizare. A ști cum funcționează infractorii cibernetici și cum îți pot fura identitatea digitală este un factor cheie pentru prevenirea acestora.

Atunci trebuie să fii foarte atent. De exemplu, nu deschideți niciodată e-mailuri sau mesaje suspecte care ajung la noi. Adesea, acești criminali cibernetici pretind a fi organizații cu care avem un serviciu (de exemplu, o bancă), așa că trebuie să fim capabili să recunoaștem dacă informațiile pe care le primim pot fi sau nu adevărate. este scris corect in limba ta? Există semne ciudate? Vorbește despre operațiuni de care nu știi? Dacă aveți cea mai mică suspiciune, nu faceți clic, nu descărcați și nu atingeți nimic. Dacă este banca dvs., de exemplu, sunați la sucursala dvs. și cereți o explicație. Nu faceți niciodată clic pe linkuri suspecte.

Acest fenomen se numește atac de tip phishing și este cu adevărat periculos pentru persoanele care sunt afectate de acesta.

Care sunt câteva modalități de a ne proteja identitatea digitală?

- **Utilizați autentificarea cu doi factori:** Autentificarea identității tale nu se face doar printr-un singur pas (de exemplu, parola), ci și prin pași suplimentari precum introducerea unui cod sau autorizarea prin telefon.
- **Schimbați și diversificați parolele:** Nu utilizați aceleași parole pentru toate conturile și încercați să le schimbați des.
- **Evitați partajarea informațiilor sensibile**: aveți grijă la tipul de date pe care le partajați și încercați să partajați online doar elementele esențiale, cum ar fi adresa de domiciliu (ai grijă la geolocalizarea pe fotografiile pe care le postezi pe rețelele de socializare!).

Drepturile unui cetățean digital

- Cetățenia digitală conform Consiliului Europei se referă la capacitatea de a se angaja pozitiv, critic și competent în mediul digital, bazându-se pe abilitățile de comunicare și creație eficiente, dar se referă și la capacitatea pe care un cetățean o aplică atunci când participă într-o manieră respectuoasă față de drepturile omului și demnitatea prin utilizarea responsabilă a tehnologiei.
- Un cetățean digital are dreptul să se bucure de drepturile la confidențialitate, securitate, evaluare și incluziune și libertatea de exprimare. Cu toate acestea, în calitate de cetățean cu aceste drepturi, cetățeanul digital are anumite responsabilități, cum ar fi etica și empatia și alte responsabilități pentru a garanta un mediu digital sigur și responsabil pentru toți cetățenii digitali.

2.6.2 Activități practice

Pasul 1: Jocul cu personalul privat

Imaginează-ți că vorbești cu o prietenă care îți spune că a cunoscut un coleg de-al tău din liceu.

Ești curios să afli mai multe despre acea persoană cu care erai atât de apropiată când erai adolescent.

Încercați să vă alăturați numelui și prenumelui pe internet și apoi extindeți cercetarea (puteți face cercetarea și asupra dvs. sau asupra unei persoane pe care o cunoașteți).

- Ce ai aflat despre acea persoană?
- Ce instrumente ai folosit pentru a te ajuta în cercetarea ta?
- Ce platforme ați consultat?
- Încercați să răspundeți la următoarele întrebări:
  - În ce oraș locuiește el/ea?
  - El/ea este căsătorit?
  - Ce a studiat el/ea?
  - Care este meseria lui/ei?

La sfârșitul activității, educatorul invită cursanții să reflecteze cu atenție asupra informațiilor pe care le distribuim online.

Pasul 2: Cât de sigură este parola ta?

În această activitate, educatorul dorește să învețe cursanții importanța de a avea o parolă sigură pe conturile lor.

Educatorul le cere cursanților să-și imagineze că trebuie să pregătească parole pentru una dintre următoarele persoane:

1.Helen Smith	1.Alejandro Garcia	1.María Ivanov
• Born: 25th June 1988 • Live in: Los Angeles (USA) • Married • She has got a dog named Oliver	• Born: 11th March 1965 • Live in: Madrid (Spain) • Single • He loves motorbikes	• Born: 1st December 1952 •Live in: Sofia (Bulgaria) • Married • She has three children

Figura 11 – Profiluri de luat în considerare la pregătirea parolelor.

- **Încercați să scrieți o parolă diferită pentru fiecare persoană care se joacă cu cuvinte (cel puțin 5). T**sugerează o parolă diferită, în funcție de contul pentru care trebuie să o creezi (ei, bancă; Facebook; e-mail privat; e-mail de serviciu, comerț electronic etc.).
- Acum testați online nivelul de securitate al parolei (există mai multe platforme pe care le puteți utiliza, de exemplu https://howsecureismypassword.net/).

La finalul activității, educatorul invită cursanții să reflecte cu atenție cum să creeze o parolă bună pentru a garanta un nivel de securitate online.

Educatorul va propune câteva întrebări de debriefing:

- Cum îți creezi parolele? Întotdeauna folosești același pentru toate site-urile sau ai altele diferite?
- Credeți că există site-uri unde aveți nevoie de un nivel mai ridicat de securitate a parolei decât altele?

- Ce trucuri ar trebui folosite pentru a crea parole online sigure?
- Cât de des ar trebui schimbate parolele?
- Știți cum hoții de identitate vă pot fura parolele?

Felicitări, acum ați finalizat Modulul 2.

Nu uitați să verificați Anexele pentru resurse și documente suplimentare furnizate pentru a sprijini auto-studiul!

Modulul 3: Crearea de conținut

Modulul 3 se concentrează pe crearea de conținut pentru cetățeanul competent din punct de vedere digital. Ne propunem să creăm o înțelegere comună a ceea ce înseamnă să fii un cetățean competent din punct de vedere digital, precum și să dezvoltăm și să testăm materiale care creează o cale clară spre îmbunătățirea competențelor în principalele domenii digitale relevante.

În cadrul acestui modul vom acoperi:

- Dezvoltarea conținutului digital - Pentru a crea și edita conținut digital în diferite formate, pentru a se exprima prin mijloace digitale.

- Integrarea și reelaborarea conținutului digital - Pentru a modifica, rafina, îmbunătăți și integra informații și conținut într-un corp de cunoștințe existent pentru a crea conținut și cunoștințe noi, originale și relevante.

- Drepturi de autor și licențe - Pentru a înțelege modul în care drepturile de autor și licențele se aplică datelor, informațiilor și conținutului digital

- Programare - Pentru a planifica și dezvolta o secvență de instrucțiuni ușor de înțeles pentru un sistem de calcul pentru a rezolva o anumită problemă sau a îndeplini o anumită sarcină.

Vom sublinia modul în care puteți crea și edita conținut digital pentru a vă îmbunătăți și integra informațiile într-un corp de materiale existent, subliniind în același timp problemele importante legate de drepturile de autor și licențierea în sfera digitală. De asemenea, vom aborda pe scurt aspectele de programare ale modului de utilizare a sistemelor informatice.

Vă rugăm să rețineți că activitățile practice descrise în fiecare unitate pot presupune sprijinul unui formator cu experiență. Deși informațiile prezentate în manual sunt scrise într-un mod ușor de înțeles, unele acțiuni, adiacente informațiilor prezentate, pot necesita sprijinul unor oameni cu experiență.

Modulul 3	Crearea de conținut			
Durată	10 ore			
Obiective	Pentru a înțelege nuanțele și a vă dezvolta abilitățile de creare de conținut			
Unități	3.1.Dezvoltarea continutului digital	3.2 Integrarea și reelaborarea conținutului digital	3.3 Drepturi de autor și licențe	3.4 Programare
Organizarea instruirii	E-Learning	E-Learning	E-Learning	E-Learning
Durată	2,5 ore	2,5 ore	2,5 ore	2.5 ore

Masa 16 - Structura globală a Modulului 3 – Crearea conținutului.

Notă: Activitățile practice ale Modulului 3 sunt prezentate în diapozitive Power Point, pe care le puteți descărca din secțiunea de resurse a site-ului proiectului.

3.1 Dezvoltarea continutului digital

Unitatea 3.1	Dezvoltarea continutului digital
Durată	2,5 ore
Obiective	Cunoștințe sporite despre echipamentul Mojo, modalități practice de filmare, precum și înțelegere a poziționării, luminii și unghiurilor. Prezentare generală a Facebook live, aplicații mobile pentru dezvoltarea conținutului digital. În sfârșit, o perspectivă asupra programelor de editare pe computer pentru conținutul dvs. digital
Conţinut	Resurse autonome, flexibile, care pot fi utilizate în deplasare - E-Learning
Resurse	PC/ mobil sau tabletă pentru e-learning Prezentare power point (descărcare de pe site)
Metodologii de instruire	Prezentare de către trainer Clasa intoarsa

Masa 17 - Structura unității de competență 3.1.- Dezvoltarea conținutului digital al Modulului 3 – Crearea conținutului.

3.1 Dezvoltarea conținutului digital

5 tipuri de conținut digital

Blogging

Postările de blog sunt o modalitate de bază de a crea conținut captivant pentru utilizatorii dvs. online! La fel ca ziarul de modă veche, multor oameni le place să se așeze și să se bucure de un articol sau un articol bine scris și perspicace. Puteți partaja o mulțime de informații într-un cadru non-formal, prezentându-vă cititorilor dvs. și creând un raport cu aceștia și agățându-i pentru a reveni pentru mai multe! Menținerea unui blog de succes poate fi consumatoare de timp, așa că este recomandat să creați o bancă de materiale înainte de a începe totul. Veniți cu câteva idei pentru primele 2-3 luni de conținut de postare pe blog, precum și implementarea unui program de încărcare pentru a menține cititorii implicați, acest lucru vă va ajuta să fiți un poster obișnuit și consecvent!

Inspirat să începi propriul blog - găsiți mai multe informații aici:

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=CjwKCAjwh5qLBhALEiwAioods-cylXXhYEWcT_ZrqTbAeIxQDqSkTV_pdKfnoxlptSsbyl02Iw87MxoC6dwQAvD_BwE

Conținut de formă lungă

În lumea instantanee în care trăim astăzi, conținutul lung poate fi un pic de noroc. Majoritatea oamenilor le place să primească informațiile în bucăți scurte și dulci, de mărimea unei mușcături, totuși definiția formei lungi se adaptează pentru a reflecta acest lucru. Unii oameni definesc conținutul lung ca articole mai lungi de 700 de cuvinte, în timp ce alții cred că trebuie să depășească 1800 de cuvinte. Aceste tipuri de articole de conținut în formă lungă pot atrage cititorii tăi pasionați, îi implică și le oferă o evadare pe care o doresc.

Acest tip de conținut poate funcționa deosebit de bine datorită concentrării pe optimizarea motoarelor de căutare, inclusiv optimizarea cuvintelor cheie. Indicând cuvintele pe care le folosiți des și care vor fi de interes pentru publicul țintă, vă puteți asigura că conținutul ajunge pe ecranul lor! Fii inteligent și priceput cu conținutul tău, iar acest lucru poate funcționa excepțional de bine.

Sfaturi pentru a vă face conținutul lizibil și valoros- https://medium.com/swlh/10-tips-to-make-long-form-content-readable-and-valuable-5b6e117965ae

Infografice

Atrăgător, captivant și ușor de creat! Infograficele sunt acolo sus cu cel mai folosit conținut digital din sfera online, motivul pentru care acesta atrage atenția utilizatorului și îl atrag, dorind să afle mai multe. Ele pot fi cu adevărat captivante, oferind imagini de înaltă calitate, multe informații într-un instantaneu rapid. În plus, sunt foarte ușor de făcut!

Puteți folosi instrumente precum Canva sau chiar Microsoft PowerPoint pentru a crea imagini de marcă frumoase, cu concizie, pentru a le partaja publicului dvs. Nu vă fie teamă să le distribuiți pe rețelele dvs. de socializare pentru un impact mai mare al evenimentului!

Faceți clic aici pentru a încerca Canva- https://www.canva.com/

Podcasturi

În ultimii cinci ani, prevalența podcast-urilor a crescut de zece ori. Dacă stați astăzi în jurul mesei de prânz, întrebați cine ascultă conținutul podcastului și vă putem garanta că veți avea o rată de feedback pozitiv de cel puțin 50%! Podcasturile sunt modalitatea nouă și inovatoare de a prelua informații de toate tipurile. De la crime adevărate, la comedie, la istoria naturală, dacă aveți un interes ciudat sau nenorocit, sunt șanse să existe deja un podcast care o acoperă în detaliu!

Acest tip de conținut permite oamenilor să absoarbă conținut digital chiar și atunci când sunt în mișcare, de exemplu, la alergare sau în timpul navetei de dimineață, puteți intra cu ușurință într-un podcast, vă puteți concentra în continuare asupra sarcinii în cauză cu o doză utilă de divertisment sau educație.

Faceți clic aici pentru a afla cum să începeți cu podcastul dvs. - https://www.thepodcasthost.com/planning/how-to-start-a-podcast/

În sfârșit, Video!

Videoclipul este REGELE conținutului digital, în societatea vizuală de astăzi, videoclipul este modalitatea ideală de a intra în contact cu publicul într-un mod care va avea un impact uriaș! Se estimează că YouTube are peste 2 miliarde de utilizatori activi LUNAR. Dacă aveți de gând să alegeți un conținut digital pentru a vă dedica timpul

și resursele pentru a-l lăsa să fie creație video. Conținutul video este foarte divers, adaptabil și poate fi captivant pentru utilizator. Cu toții cunoaștem senzația de a derula prin rețelele de socializare dincolo de postări lungi, imagini și de a ne fi atras atenția de un videoclip frumos conceput, cu imagini, muzică și mesaje captivante.

Marketingul video mulțumește imediat publicul, YouTube a generat venituri de 19,7 miliarde de dolari începând cu ianuarie 2021.[11]Și TikTok a preluat de la Facebook, Instagram și Snapchat ca cea mai populară platformă de socializare. Scurte videoclipuri introductive sau explicative pot fi mult mai eficiente în a-ți atrage utilizatorii, ocupându-le puțin din timp, dar lăsându-le cu multe informații în schimb!

În cadrul acestui modul, vom discuta în continuare despre cum să filmați conținutul dvs. video, utilizând cea mai bună poziție, iluminare și unghiuri, precum și aplicațiile mobile care vă pot face viața mai ușoară atunci când creați conținut de marketing video de înaltă calitate!

3.2 Integrarea și reelaborarea conținutului digital

Unitatea 3.2	Integrarea și reelaborarea conținutului digital
Durată	2,5 ore
Obiective	Prezentarea formelor tipice de creare a conținutului și stocarea acestuia. Indicarea care sunt modalitățile de publicare și menținere a conținutului pe internet.
Conţinut	Resurse Power Point (descărcare de pe site) Resurse autonome, flexibile, care pot fi utilizate în deplasare - E-Learning
Resurse	PC/ mobil sau tabletă pentru e-learning
Metodologii de instruire	Prezentare de către trainer Prezentare de către participanți

Masa 18Structura unității de competenţă 3.2. – Integrarea și reelaborarea conținutului digital al Modulului 3 – Crearea conținutului.

3.2 Integrarea și reelaborarea conținutului digital

Crearea și integrarea conținutului. Pentru a modifica, rafina și integra informații și conținut noi într-un corp de cunoștințe și resurse existente pentru a crea conținut și cunoștințe noi, originale și relevante.

[11] https://www.globalmediainsight.com/blog/youtube-users-statistics/

Am abordat crearea de conținut extrem de captivant pentru publicul dvs., ținând cont de contextul utilizării dvs. La cine încerci să ajungi? Folosiți-vă punctele forte pentru a vă atinge grupul țintă, efectuați o cercetare de piață pentru a vă asigura că faceți alegerea potrivită pentru dvs.! Vom acoperi, de asemenea, publicarea și stocarea conținutului online. În cadrul integrării conținutului dvs. în resursele deja existente, vă vom arăta cum să utilizați software-ul și aplicațiile de productivitate pentru a realiza acest lucru într-un mod eficient și util! Folosind instrumente care există deja înseamnă că veți cheltui mai puțin capital și energie, în timp ce atingeți obiectivul final, care este de a crea conținut extrem de captivant, care să răspundă nevoilor dvs. și ale publicului țintă!

După cum am atins înainte ca YouTube să aibă o bancă masivă de materiale, disponibile public, care poate fi extrem de util, conținutul podcast este, de asemenea, disponibil gratuit și poate ajuta la completarea resurselor pe care le creați.

Pe parcursul versiunii 3.2, veți primi o serie de instrumente utile care vă vor face călătoria de integrare și elaborare a conținutului mult mai interesantă și mai simplă.

- O nota
- Evernote
- Desenează.io
- PIXLR
- Adobe Spark
- documente Google

Stocarea Conținutului dvs

Când ți-ai petrecut timpul și energia creând și integrând conținutul digital, este de o importanță vitală să ai abilitățile și cunoștințele despre unde este cel mai sigur să salvezi acest conținut pentru ușurință de acces, dar și securitate.

Partajarea fișierelor în cloud poate fi o platformă utilă care oferă utilizatorilor posibilitatea de a-și accesa conținutul de pe orice dispozitiv, această flexibilitate înseamnă că nu sunteți legat de un computer fizic și este

de cea mai mare importanță într-un spațiu de lucru dinamic și în schimbare. Descoperiți Dropbox, Google Drive și One Drive și schimbați modul în care vă partajați materialele.

Publicare și partajare

Partajarea online a creațiilor dvs. este un proces de publicare a conținutului pe platforme online, fie că este un canal YouTube, propriul site web și pagina de blog sau contul dvs. de social media. Conținutul publicat poate include text, imagini, videoclipuri și alte tipuri de medii digitale.

Publicarea online poate fi un cost redus, foarte eficient și eficient pentru utilizarea dvs., așa că vă putem ajuta să găsiți cele mai bune instrumente pentru a publica. Aflați mai multe despre WIX, Wordpress, Linkedin și Pinterest.

3.3 Drepturi de autor și licențe

Unitatea 3.3	Drepturi de autor și licențe
Durată	2,5 ore
Obiective	Dreptul de autor este un tip de drepturi de proprietate intelectuală (DPI) care oferă protecție asupra a ceva: • ai putea crea • deținut de una sau mai multe persoane sau întreprinderi
Conținut	Resurse autonome, flexibile, care pot fi utilizate în deplasare - E-Learning
Resurse	Resurse Power Point (descărcare de pe site) PC/ mobil sau tabletă pentru e-learning
Metodologii de instruire	Prezentare de către trainer

Masa 19 - Structura unității de competență 3.3.- Drepturi de autor și licențe ale Modulului 3 – Crearea conținutului.

3.3 Drepturi de autor și licențe

Ce este dreptul de autor?

Dreptul de autor îi conferă proprietarului dreptul exclusiv de a utiliza lucrarea, cu unele excepții. Când o persoană creează o lucrare originală, fixată într-un mediu tangibil, el sau ea deține în mod automat drepturile de autor asupra operei.

Multe tipuri de lucrări sunt eligibile pentru protecția dreptului de autor, de exemplu:

- Lucrări audiovizuale, cum ar fi programe TV, filme și videoclipuri online
- Înregistrări sonore și compoziții muzicale
- Lucrări scrise, cum ar fi prelegeri, articole, cărți și compoziții muzicale
- Lucrări vizuale, cum ar fi picturi, afișe și reclame
- Jocuri video și software de calculator
- Lucrări dramatice, cum ar fi piese de teatru și muzicale

Este posibil să utilizați o lucrare protejată prin drepturi de autor fără a încălca?

Da, în anumite circumstanțe, este posibil să utilizați o lucrare protejată prin drepturi de autor fără a încălca drepturile de autor ale proprietarului. Unii creatori de conținut aleg să își facă munca disponibilă pentru reutilizare cu anumite cerințe. Pentru mai multe despre acest lucru, poate doriți să aflați despreLicență Creative Commons.[12]

Legea drepturilor de autor a Uniunii Europene

Legea drepturilor de autor a Uniunii Europene estedrepturi de autorlegea aplicabilă în cadrulUniunea Europeana. Legea drepturilor de autor este în mare măsură armonizată în Uniune, deși există diferențe de la țară la țară. Corpul legislativ a fost implementat în UE printr-o serie dedirective, pe care statele membre trebuie să le introducă în legislația lor națională. Principalele directive privind drepturile de autor suntDirectiva privind termenii drepturilor de autor, celDirectiva Societății InformaționalesiDirectiva privind drepturile de autor în piața unică digitală.[13]

Legea drepturilor de autor a UE constă din 11 directive și 2 reglementări, care armonizează drepturile esențiale ale autorilor, interpreților, producătorilor și radiodifuzorilor. Prin stabilirea de standarde armonizate, legislația UE privind drepturile de autor reduce discrepanțele naționale și garantează nivelul de protecție necesar pentru a stimula creativitatea și investițiile în creativitate. Standardele armonizate promovează diversitatea culturală și aduc un acces mai bun pentru consumatori și întreprinderi la conținutul și serviciile digitale din întreaga Europă.[14]

[12] https://support.google.com/legal/answer/3463239?hl=ro

[13] https://en.wikipedia.org/wiki/Copyright_law_of_the_European_Union

[14] https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation

În 3.3, vom aprofunda cerințele privind drepturile de autor, cum să utilizați licențe creative commons și cum aceste tipuri de licențe pot fi utile conținutului dvs.!

3.4 Programare

Unitatea 3.4	Programare
Durată	2,5 ore
Obiective	Obiectivul acestui modul este de a obține o înțelegere a structurilor de bază ale limbajului Python.
Conţinut	Resurse autonome, flexibile, care pot fi utilizate în deplasare - E-Learning
Resurse	Resurse Power Point (descărcare de pe site) PC/ mobil sau tabletă pentru e-learning
Metodologii de instruire	Prezentare de către trainer Flipped Classroom

Masa 20- Structura unităţii de competenţă 3.4. - Programarea Modulului 3 – Crearea Conținutului.

3.4 Noțiuni de bază pentru programare și codare

Ce este programarea la nivel de bază?

Codarea este o cunoaștere de bază în era digitală și este important ca fiecare persoană să înțeleagă și să fie capabilă să codifice simplu și să folosească tehnologia din jurul său. Există multe limbaje de codare diferite. Am ales Python. Python este un simplu și ușor de învățat datorită sintaxei și lizibilității sale clare.

Python este un limbaj de programare puternic, ușor de învățat.

Python este un limbaj de programare ușor de învățat și puternic în funcționare. În timp ce scrieți codul, vă veți concentra în principal pe rezolvarea problemei, nu pe sintaxa și structura limbajului în care programați.

Variabile Python

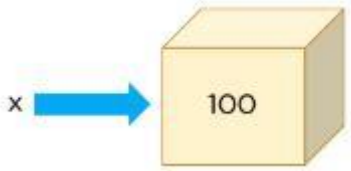
1. Atribuire variabilă

O variabilă este un concept fundamental în orice limbaj de programare. Este o locație de memorie rezervată care stochează și manipulează date. Gândiți-vă la o variabilă ca la un nume atașat unui anumit obiect. În Python, variabilele nu trebuie declarate sau definite în prealabil, așa cum este cazul în multe alte limbaje de programare. Pentru a crea o variabilă, îi atribuiți o valoare și apoi începeți să o utilizați. Atribuirea se face cu un singur semn egal (=):

Variabilele sunt entități ale unui program care dețin o valoare. Iată un exemplu de variabilă:

x=100

În diagrama de mai jos, caseta conține o valoare de 100 și este numită x. Prin urmare, variabila este x, iar datele pe care le deține sunt valoarea.



Tipul de date pentru o variabilă este tipul de date pe care le deține.15

În exemplul de mai sus, x conține 100, care este un număr, iar tipul de date al lui x este un număr.

În Python, există trei tipuri de numere: Integer, Float și Complex.

Numerele întregi sunt numere fără zecimale. Flotantele sunt numere cu zecimale. Numerele complexe au părți reale și părți imaginare.

Un alt tip de date care este foarte diferit de un număr se numește șir, care este o colecție de caractere.

[15] https://www.simplilearn.com/tutorials/python-tutorial/python-variables

Să vedem o variabilă cu un tip de date întreg:

x=100

Pentru a verifica tipul de date al lui x, utilizați funcția type():

tip (x)

Python vă permite să atribuiți variabile în timp ce efectuați operații aritmetice.

x=654*6734

tip (x)

Pentru a afișa rezultatul variabilei, utilizați funcția print().

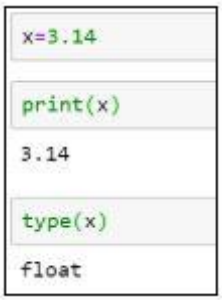
print(x) #Oferă produsul celor două numere

Acum, să vedem un exemplu de număr în virgulă mobilă:

x=3,14

print(x)

type(x) #Aici tipul variabilei este float



Șirurile sunt declarate între ghilimele simple sau duble.

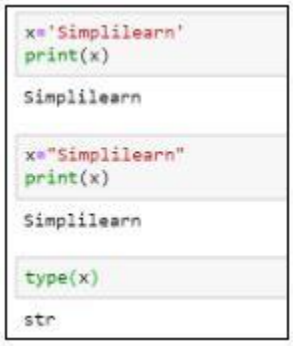
x='Simplilearn'

print(x)

x = „Învățare simplă.”

print(x)

tip (x)



Pentru a afla mai multe, am legat o pagină interesantă cu infografice excelente:

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

Felicitări, ați finalizat acum Modulul 3.

Nu uitați să verificați Anexele pentru resurse și documente suplimentare furnizate pentru a sprijini auto-studiul!

Modulul 4: Siguranță

Modulul 4 este axat pe siguranța online și își propune să vă atragă atenția asupra acestei probleme, alături de a vă oferi informații despre cum să reduceți riscurile și să vă păstrați siguranța.

Vă rugăm să rețineți că activitățile practice descrise în fiecare unitate pot presupune sprijinul unui formator cu experiență. Deși informațiile prezentate în manual sunt scrise într-un mod ușor de înțeles, unele acțiuni, adiacente informațiilor prezentate, pot necesita sprijinul unor oameni cu experiență.

Modulul 4	**Siguranță**			
Durată	**25h**			
Obiective	În cadrul acestei unități, participantul va fi instruit să: • pentru a proteja dispozitivele, conținutul, datele personale și confidențialitatea în medii digitale; • să protejeze sănătatea fizică și psihologică și să fie conștienți de tehnologiile digitale pentru bunăstarea socială și incluziunea socială; • să fie conștienți de impactul asupra mediului al tehnologiilor digitale și de utilizarea acestora.			
Unități	4.1 Dispozitive de protecție	4.2 Protejarea datelor cu caracter personal și a confidențialității	4.3 Protejarea sănătății și bunăstării	4.4 Protejarea mediului
Organizarea instruirii	Față în față E-Learning B-learning	Față în față E-Learning B-learning	Față în față E-Learning B-learning	Față în față E-Learning B-learning
Durată	6h	9h	5h	5h

Masa 21 - Structura globală a Modulului 4 – Siguranță.

4.1 Dispozitive de protecție

Unitatea 4.1	Dispozitive de protecție
Durată	6h
Obiective	Pentru a înțelege că un computer este predispus la atacuri cibernetice în rețea Pentru a ști cum să configurați o parolă puternică Pentru a putea instala un browser de internet Chrome și a-l actualiza periodic Pentru a înțelege efortul pe care ochiul uman îl face pentru a citi informațiile de pe dispozitive electronice Înțelegeți că o poziție incorectă de lucru poate duce la probleme medicale cu coloana vertebrală Pentru a înțelege costurile de funcționare ale echipamentului Pentru a înțelege că componentele electronice fizice nu sunt „prietenoase cu mediul”
Conţinut	4.1.1 Dispozitive de protecție 4.1.2 Actualizări software 4.1.3. Securitate și parole 4.1.4 Creșterea securității 4.1.5 Ce este un cod rău intenționat? 4.1.6 Activități practice
Resurse	Manual de instruire Computer cu acces la internet Program de editare Hârtii Pixuri
Metodologii de instruire	Prezentare de către trainer Selecția media

Masa 22- Structura unităţii de competenţă 4.1. – Dispozitive de protecție ale Modulului 4 – Siguranță.

4.1.1 Dispozitive de protecție

De ce este importantă securitatea computerului?

Deoarece computerele joacă roluri atât de importante în viața noastră și pentru că introducem și vedem atât de multe informații de identificare personală pe ele, este imperativ să implementăm și să menținem securitatea computerului. Securitatea computerizată puternică asigură procesarea și stocarea în siguranță a informațiilor noastre.

Cum pot îmbunătăți securitatea computerului meu?

Următorii sunt pași importanți pe care ar trebui să îi luați în considerare pentru a vă face computerul mai sigur. Deși niciun pas individual nu va elimina toate riscurile, atunci când sunt utilizate împreună, aceste practici de apărare în profunzime vor consolida securitatea computerului și vor ajuta la minimizarea amenințărilor.

➢ Asigurați-vă rețeaua de acasă

Când conectați un computer la internet, acesta este, de asemenea, conectat la milioane de alte computere - o conexiune care ar putea permite atacatorilor accesul la computerul dvs. Deși modemurile prin cablu, liniile digitale de abonat (DSL) și furnizorii de servicii de internet (ISP) au un anumit nivel de monitorizare a securității, este esențial să vă securizați routerul - primul dispozitiv securizat care primește informații de pe internet. Asigurați-vă că îl securizați înainte de a vă conecta la internet pentru a consolida securitatea computerului.
Ce este securitatea rețelei de acasă și de ce ar trebui să-mi pese?

➢ Securitatea rețelei de acasă

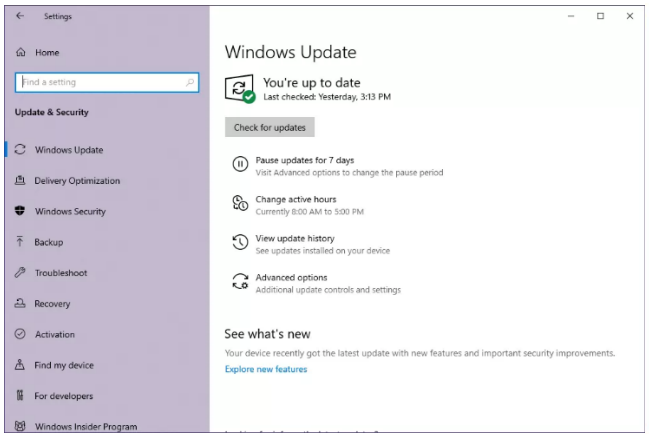
Securitatea rețelei de acasă se referă la protecția unei rețele care conectează dispozitive, cum ar fi routere, computere, smartphone-uri, electrocasnice, monitoare pentru bebeluși compatibile Wi-Fi, camere foto, între ele și la internetul din locuință.
Mulți utilizatori casnici împărtășesc două concepții greșite despre securitatea rețelelor lor:

- Rețeaua lor de domiciliu este prea mică pentru a fi expusă riscului unui atac cibernetic.
- Dispozitivele lor sunt „suficient de sigure” imediat scoase din cutie.

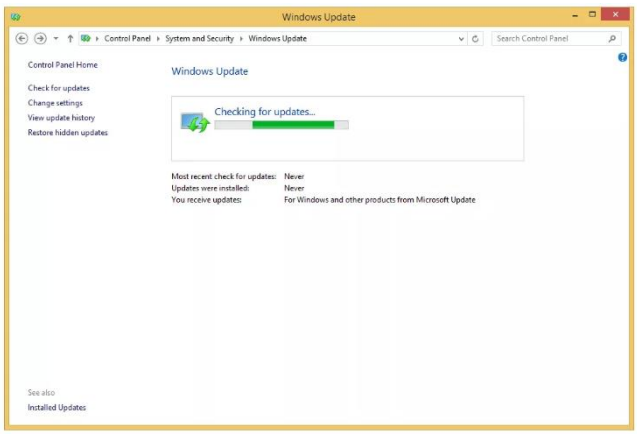
Majoritatea atacurilor nu sunt de natură personală și pot apărea pe orice tip de rețea - mare sau mică, acasă sau în afaceri. Dacă o rețea se conectează la internet, este în mod inerent mai vulnerabilă și mai susceptibilă la amenințările externe.
Cum pot îmbunătăți securitatea rețelei mele de acasă?
Urmând unele dintre tehnicile de atenuare simple, dar eficiente de mai jos, puteți reduce în mod semnificativ suprafața de atac a rețelei dvs. de acasă și puteți îngreuna ca un actor cibernetic rău intenționat să lanseze un atac de succes.

➢ Actualizați-vă software-ul în mod regulat

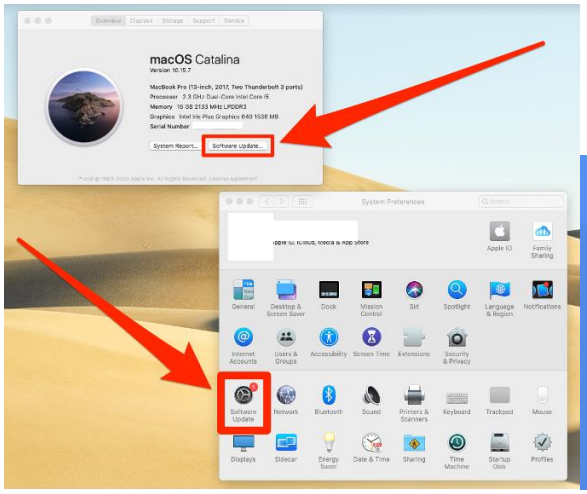
Actualizările regulate ale software-ului sunt unul dintre cei mai eficienți pași pe care îi puteți lua pentru a îmbunătăți postura generală de securitate cibernetică a rețelelor și sistemelor dvs. de acasă. Pe lângă adăugarea de noi caracteristici și funcționalități, actualizările software includ adesea patch-uri critice și remedieri de securitate pentru amenințările și vulnerabilitățile nou descoperite. Majoritatea aplicațiilor software moderne vor verifica automat actualizările nou lansate. Dacă nu sunt disponibile actualizări automate, luați în considerare achiziționarea unui program software care identifică și gestionează centralizat toate actualizările software instalate.



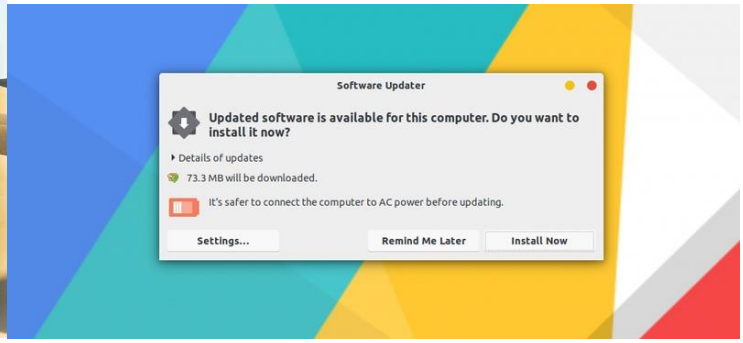
Windows 10



Windows 8,7, Vista



Actualizare MacOS



Actualizare Ubuntu (Linux).

Ce sunt patch-urile?

Patch-urile sunt actualizări ale software-ului și ale sistemului de operare (OS) care abordează vulnerabilitățile de securitate dintr-un program sau produs. Furnizorii de software pot alege să lanseze actualizări pentru a remedia erorile de performanță, precum și pentru a oferi funcții de securitate îmbunătățite.

4.1.2 Actualizări software

Cum afli ce actualizări de software trebuie să instalezi?

Când actualizările de software devin disponibile, vânzătorii le pun de obicei pe site-urile lor web pentru ca utilizatorii să le descarce. Instalați actualizări cât mai curând posibil pentru a vă proteja computerul, telefonul sau alt dispozitiv digital împotriva atacatorilor care ar profita de vulnerabilitățile sistemului. Atacatorii pot viza vulnerabilități timp de luni sau chiar ani după ce actualizările sunt disponibile.

Unele programe software vor verifica automat actualizările, iar mulți furnizori oferă utilizatorilor opțiunea de a primi actualizări automat. Dacă sunt disponibile opțiuni automate, puteți profita de ele. Dacă nu sunt disponibile, verificați periodic site-urile web ale furnizorului dvs. pentru actualizări.

Asigurați-vă că descărcați actualizări software numai de pe site-urile web ale furnizorilor de încredere. Nu aveți încredere într-un link dintr-un mesaj de e-mail – atacatorii au folosit mesaje de e-mail pentru a direcționa utilizatorii către site-uri web care găzduiesc fișiere rău intenționate deghizate în actualizări legitime. De asemenea, utilizatorii ar trebui să fie suspicioși cu privire la mesajele de e-mail care pretind că au atașat un fișier de actualizare a software-ului - aceste atașamente pot conține programe malware.

Dacă este posibil, aplicați actualizări automate numai din locații de încredere din rețea (de exemplu, acasă, serviciu). Evitați actualizarea software-ului (automat sau manual) în timp ce sunteți conectat la rețele nesigure (de exemplu, aeroport, hotel, cafenea). Dacă actualizările trebuie instalate într-o rețea nede încredere, utilizați o conexiune de rețea privată virtuală la o rețea de încredere și aplicați actualizări.

Care este diferența dintre actualizările manuale și automate?

Utilizatorii pot instala actualizările manual sau pot alege ca programele lor software să se actualizeze automat.

Actualizările manuale necesită ca utilizatorul sau administratorul să viziteze site-ul web al furnizorului pentru a descărca și instala fișiere software.

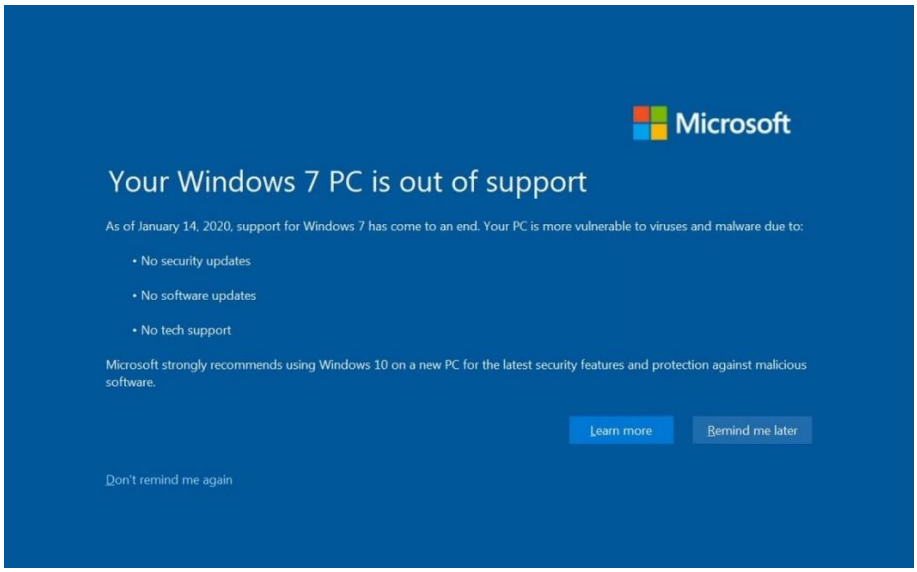
Actualizările automate necesită consimțământul utilizatorului sau al administratorului la instalarea sau configurarea software-ului. Odată ce sunteți de acord cu actualizările automate, actualizările software sunt „împinse” (sau instalate) în sistem automat.

Ce este software-ul la sfârșitul vieții?

Uneori, furnizorii vor întrerupe suportul pentru un program software sau vor emite actualizări de software pentru acesta (cunoscut și ca software la sfârșitul vieții [EOL]). Utilizarea continuă a software-ului EOL prezintă un risc consecvent pentru sistemul dumneavoastră, care poate permite unui atacator să exploateze vulnerabilitățile de securitate. Utilizarea de software neacceptat poate cauza, de asemenea, probleme de compatibilitate software, precum și scăderea performanței și productivității sistemului.

Cele mai bune practici pentru actualizările software

- Activați actualizările automate de software ori de câte ori este posibil. Acest lucru va asigura că actualizările software sunt instalate cât mai repede posibil.
- Nu utilizați software EOL neacceptat.
- Vizitați întotdeauna site-urile furnizorilor direct, în loc să faceți clic pe reclame sau link-uri de e-mail.
- Evitați actualizările de software în timp ce utilizați rețele care nu sunt de încredere.
- Noi vulnerabilități apar în mod continuu, dar cea mai bună apărare împotriva atacatorilor care exploatează vulnerabilități corectate este simplă: mențineți software-ul la zi. Aceasta este cea mai eficientă măsură pe care o puteți lua pentru a vă proteja computerul, telefonul și alte dispozitive digitale.



Windows 7 EOL

Eliminați serviciile și software-ul inutile

Dezactivați toate serviciile inutile pentru a reduce suprafața de atac a rețelei și a dispozitivelor dvs., inclusiv a routerului. Serviciile și software-ul neutilizate sau nedorite pot crea găuri de securitate în sistemul unui dispozitiv, ceea ce ar putea duce la o suprafață de atac crescută a mediului de rețea. Acest lucru este valabil mai ales în cazul sistemelor informatice noi pe care vânzătorii vor preinstala adesea un număr mare de software și aplicații de probă – denumite „bloatware” – pe care utilizatorii ar putea să nu le găsească utile.

Ajustați configurațiile implicite din fabrică pentru software și hardware

Multe produse software și hardware vin „din cutie” cu configurații implicite din fabrică prea permisive menite să le facă ușor de utilizat și să reducă timpul de depanare pentru serviciul clienți. Din păcate, aceste configurații implicite nu sunt orientate spre securitate. Lăsându-le activate după instalare, poate crea mai multe căi de exploatare pentru un atacator. Utilizatorii ar trebui să ia măsuri pentru a consolida parametrii impliciti de configurare pentru a reduce vulnerabilitățile și pentru a proteja împotriva intruziunilor.

4.1.3 Securitate și parole

Schimbați parolele implicite de conectare și numele de utilizator

Majoritatea dispozitivelor de rețea sunt preconfigurate cu parole implicite de administrator pentru a simplifica configurarea. Aceste acreditări implicite nu sunt sigure – pot fi disponibile cu ușurință pe internet sau chiar pot fi etichetate fizic pe dispozitivul însuși. Lăsarea acestora neschimbată creează oportunități pentru actorii cibernetici rău intenționați de a obține acces neautorizat la informații, de a instala software rău intenționat și de a cauza alte probleme.

Utilizați parole puternice și unice

Alegeți parole puternice pentru a vă proteja dispozitivele. În plus, nu utilizați aceeași parolă cu mai multe conturi. În acest fel, dacă unul dintre conturile dvs. este compromis, atacatorul nu va putea încălca niciun alt cont.

De ce ai nevoie de parole puternice?

Probabil că folosiți numere personale de identificare (PIN), parole sau expresii de acces în fiecare zi: de la obținerea de bani de la bancomat sau utilizarea cardului de debit într-un magazin, până la autentificarea la e-mail sau la un comerciant online. Urmărirea tuturor combinațiilor de numere, litere și cuvinte poate fi frustrantă, dar aceste protecții sunt importante deoarece hackerii reprezintă o amenințare reală pentru informațiile dvs. Adesea, un atac nu se referă în mod specific la contul dvs., ci la utilizarea accesului la informațiile dvs. pentru a lansa un atac mai mare.

Una dintre cele mai bune modalități de a proteja informațiile sau proprietatea fizică este să vă asigurați că numai persoanele autorizate au acces la acestea. Următorul pas este verificarea faptului că cei care solicită acces sunt persoanele care pretind că sunt. Acest proces de autentificare este mai important și mai dificil în lumea cibernetică. Parolele sunt cele mai comune mijloace de autentificare, dar funcționează numai dacă sunt complexe și confidențiale. Multe sisteme și servicii au fost încălcate cu succes din cauza parolelor nesecurizate și inadecvate. Odată ce un sistem este compromis, acesta este deschis exploatării de către alte surse nedorite.

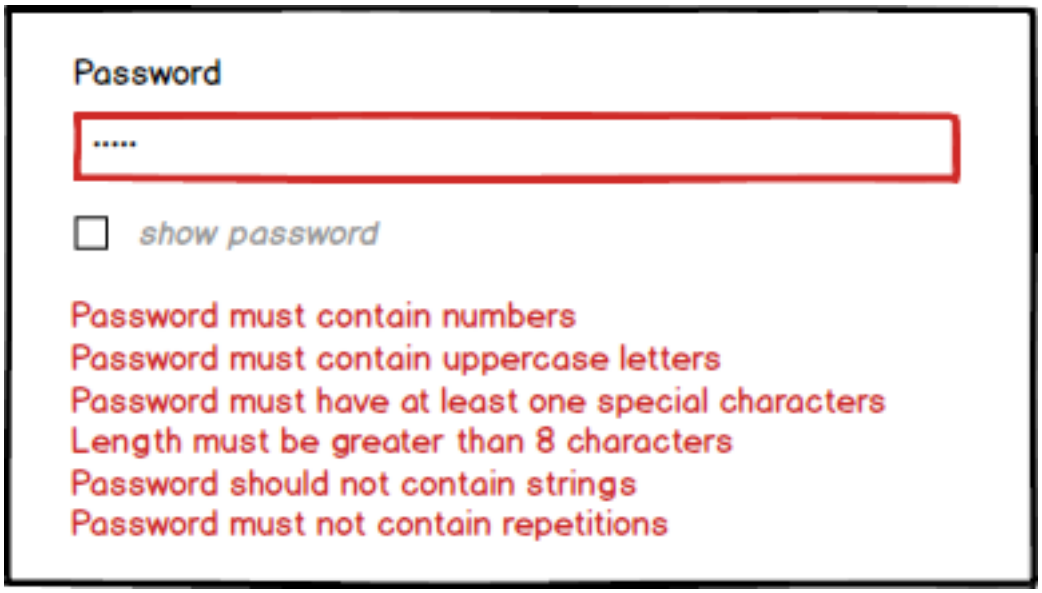
Evitați greșelile comune

Majoritatea oamenilor folosesc parole care se bazează pe informații personale și sunt ușor de reținut. Cu toate acestea, acest lucru face, de asemenea, mai ușor pentru un atacator să le spargă. Luați în considerare un cod PIN din patru cifre. A ta este o combinație a lunii, zilei sau anului zilei tale de naștere? Conține adresa sau numărul dvs. de telefon? Gândiți-vă cât de ușor este să găsiți ziua de naștere a cuiva sau informații similare. Dar parola dvs. de e-mail - este un cuvânt care poate fi găsit în dicționar? Dacă da, poate fi susceptibil la atacuri de dicționar, care încearcă să ghicească parole pe baza unor cuvinte sau expresii obișnuite.

Deși scrierea greșită intenționată a unui cuvânt („daytt” în loc de „data”) poate oferi o anumită protecție împotriva atacurilor din dicționar, o metodă și mai bună este să te bazezi pe o serie de cuvinte și să folosești tehnici de memorie sau mnemonice, pentru a te ajuta să-ți amintești cum să decodești aceasta. De exemplu, în loc de parola „hoops”, utilizați „IlTpbb” pentru „[I] [l]ike [T]o [p]lay [b]asket[b]all”. Folosirea atât a literelor mici, cât și a majusculei adaugă un alt strat de obscuritate. Schimbarea aceluiași exemplu folosit mai sus în „Il!2pBb”. creează o parolă foarte diferită de orice cuvânt din dicționar.

Lungimea și complexitatea

Ar trebui să luați în considerare utilizarea celei mai lungi parole sau expresii de acces permise (8-64 de caractere) atunci când puteți. De exemplu, „Pattern2baseball#4mYmiemale!” ar fi o parolă puternică, deoarece are 28 de caractere și include litere mari și mici, cifre și caractere speciale. Poate fi necesar să încercați diferite variante ale unei fraze de acces — de exemplu, unele aplicații limitează lungimea parolelor, iar altele nu acceptă spații sau anumite caractere speciale. Evitați frazele obișnuite, citatele celebre și versurile cântecelor.



Ce să faci și ce să nu faci

Odată ce ați venit cu o parolă puternică și memorabilă, este tentant să o reutilizați - nu o faceți! Reutilizarea unei parole, chiar și a uneia puternice, vă pune în pericol conturile la fel de mult ca și utilizarea unei parole slabe. Dacă atacatorii vă ghicesc parola, ar avea acces la celelalte conturi ale dvs. cu aceeași parolă. Utilizați următoarele tehnici pentru a dezvolta parole unice pentru fiecare dintre conturile dvs.:

- Utilizați parole diferite pe sisteme și conturi diferite.
- Utilizați cea mai lungă parolă sau expresie de acces permisă de fiecare sistem de parole.
- Dezvoltați mnemonice pentru a reține parolele complexe.
- Luați în considerare utilizarea unui program de gestionare a parolelor pentru a vă urmări parolele. (Vezi mai multe informații mai jos.)
- Nu utilizați parole care se bazează pe informații personale care pot fi ușor accesate sau ghicite.
- Nu folosiți cuvinte care pot fi găsite în orice dicționar din orice limbă.

Cum să vă protejați parolele

După ce ai ales o parolă care este ușor de reținut, dar greu de ghicit pentru alții, nu o nota și lasă-o undeva unde alții o pot găsi. Notând-o și lasând-o pe birou, lângă computer, sau, mai rău, lipită pe computer, îl face ușor accesibil pentru cineva cu acces fizic la birou. Nu spune nimănui parolele tale și urmărește atacatorii care încearcă să te păcălească prin apeluri telefonice sau prin e-mailuri prin care se solicită să-ți dezvălui parolele.

Programele numite manageri de parole oferă opțiunea de a crea parole generate aleatoriu pentru toate conturile dvs. Apoi accesați acele parole puternice cu o parolă principală. Dacă utilizați un manager de parole, nu uitați să utilizați o parolă principală puternică.

Problemele legate de parole pot proveni din capacitatea browserelor dvs. web de a salva parolele și sesiunile online în memorie. În funcție de setările browserului dvs. web, oricine are acces la computerul dvs. poate să vă descopere toate parolele și să obțină acces la informațiile dvs. Nu uitați întotdeauna să vă deconectați atunci când utilizați un computer public (la bibliotecă, un internet cafe sau chiar un computer partajat la birou). Evitați utilizarea computerelor publice și a rețelei Wi-Fi publice pentru a accesa conturi sensibile, cum ar fi servicii bancare și e-mail.

Nu există nicio garanție că aceste tehnici vor împiedica un atacator să vă învețe parola, dar o vor face mai dificilă.

Nu uitați de elementele de bază ale securității

- Țineți-vă actualizat sistemul de operare, browserul și alte programe software.
- Utilizați și întrețineți software antivirus și un firewall.
- Scanați-vă în mod regulat computerul pentru spyware. (Unele programe antivirus încorporează detectarea programelor spion.)

4.1.4 Creșterea securității

Rulați software antivirus actualizat

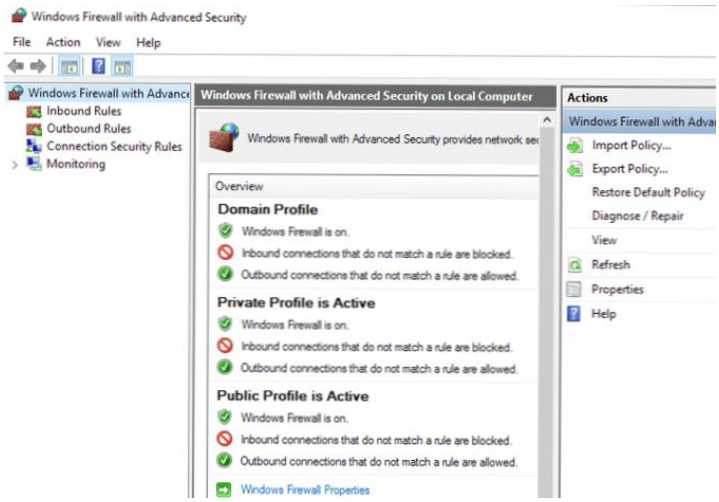
O aplicație software antivirus de renume este o măsură de protecție importantă împotriva amenințărilor rău intenționate cunoscute. Poate detecta, pune în carantină și elimina automat diferite tipuri de malware, cum ar fi viruși, viermi și ransomware. Multe soluții antivirus sunt extrem de ușor de instalat și intuitiv de utilizat. Se recomandă ca toate computerele și dispozitivele mobile din rețeaua dvs. de domiciliu să ruleze software antivirus. În plus, asigurați-vă că activați actualizările automate ale definițiilor de viruși pentru a asigura protecție maximă împotriva celor mai recente amenințări. Notă: deoarece detectarea se bazează pe semnături – modele cunoscute care pot identifica codul ca malware – chiar și cel mai bun antivirus nu va oferi protecție adecvată împotriva amenințărilor noi și avansate, cum ar fi exploit-urile zero-day și virușii polimorfi.

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

Instalați un firewall de rețea

Instalați un firewall la limita rețelei dvs. de acasă pentru a vă apăra împotriva amenințărilor externe. Un firewall poate bloca traficul rău intenționat să intre în rețeaua dvs. de domiciliu și vă poate avertiza cu privire la activități potențial periculoase. Când este configurat corespunzător, poate servi și ca o barieră pentru amenințările interne, împiedicând software-ul nedorit sau rău intenționat să ajungă la internet. Majoritatea routerelor fără fir vin cu un firewall de rețea configurabil, încorporat, care include caracteristici suplimentare - cum ar fi controale de acces, filtrare web și apărare împotriva refuzului serviciului (DoS) - pe care le puteți personaliza pentru a se potrivi mediului dvs. de rețea. Rețineți că unele funcții de firewall, inclusiv firewall-ul în sine, pot fi dezactivate în mod implicit. Asigurarea că firewall-ul este activat și că toate setările sunt configurate corect va întări securitatea rețelei rețelei. Notă:

Pe lângă un firewall de rețea, luați în considerare instalarea unui firewall pe toate computerele conectate la rețeaua dvs. Deseori denumite bazate pe gazdă sau software, aceste firewall-uri inspectează și filtrează traficul de rețea de intrare și de ieșire al unui computer pe baza unei politici predeterminate sau a unui set de reguli. Cele mai multe sisteme de operare Windows și Linux moderne vin cu un firewall încorporat, personalizabil și bogat în funcții. În plus, majoritatea vânzătorilor își îmbină software-ul antivirus cu funcții de securitate suplimentare, cum ar fi controlul parental, protecția e-mailului și blocarea site-urilor web rău intenționate.



Faceți în mod regulat copii de siguranță ale datelor dvs

Efectuați și stocați, folosind fie medii externe, fie un serviciu bazat pe cloud, copii de rezervă regulate ale tuturor informațiilor valoroase care se află pe dispozitivul dvs. Luați în considerare utilizarea unei aplicații de backup terță parte, care poate simplifica și automatiza procesul. Asigurați-vă că ați criptat backup-ul pentru a proteja confidențialitatea și integritatea informațiilor dvs. Copierea de rezervă a datelor este crucială pentru a minimiza impactul în cazul în care datele respective sunt pierdute, corupte, infectate sau furate.

Creșteți securitatea wireless

Este posibil să fie nevoie să consultați manualul de instrucțiuni al routerului sau să contactați furnizorul de servicii de internet pentru instrucțiuni specifice despre cum să modificați o anumită setare pe dispozitiv.

Utilizați cel mai puternic protocol de criptare disponibil. Se recomandă utilizarea standardului de criptare avansat personal (AES) și a protocolului de integritate a cheii temporare (TKIP), care este în prezent cea mai sigură configurație de router disponibilă pentru uz casnic. Încorporează AES și este capabil să utilizeze chei criptografice de 128, 192 și 256 de biți. Acest standard a fost aprobat de Institutul Național de Standarde și Tehnologie (NIST).
Schimbați parola implicită de administrator a routerului. Schimbați parola de administrator a routerului pentru a vă proteja de un atac folosind acreditările implicite.
Schimbați identificatorul implicit al setului de servicii (SSID). Denumit uneori „numele rețelei”, un SSID este un nume unic care identifică o anumită rețea locală wireless (WLAN). Toate dispozitivele fără fir dintr-o rețea locală wireless (WLAN) trebuie să utilizeze același SSID pentru a comunica între ele. Deoarece SSID-ul implicit al dispozitivului identifică de obicei producătorul sau dispozitivul real, un atacator îl poate folosi pentru a identifica dispozitivul și pentru a exploata oricare dintre vulnerabilitățile sale cunoscute. Faceți-vă SSID-ul unic

și nu legat de identitatea sau locația dvs., ceea ce ar face mai ușor pentru atacator să identifice rețeaua dvs. de domiciliu.
Dezactivați Wi-Fi Protected Setup (WPS). WPS oferă mecanisme simplificate pentru ca un dispozitiv fără fir să se alăture unei rețele Wi-Fi fără a fi nevoie să introduceți parola rețelei fără fir. Cu toate acestea, un defect de proiectare în specificația WPS pentru autentificarea PIN reduce semnificativ timpul necesar unui atacator cibernetic pentru a forța un întreg PIN, deoarece îi informează când prima jumătate a codului PIN de opt cifre este corectă. Multe routere nu au o politică de blocare adecvată după un anumit număr de încercări eșuate de a ghici PIN-ul, ceea ce face ca un atac cu forță brută să fie mult mai probabil să apară. Vedeți Atacurile cu forță brută conduse de actori cibernetici.
Reduceți puterea semnalului wireless. Semnalul dvs. Wi-Fi se propagă frecvent dincolo de perimetrele casei dvs. Această emisie extinsă permite interceptarea cu urechea intrușilor din afara perimetrului rețelei dvs. Prin urmare, luați în considerare cu atenție plasarea antenei, tipul de antenă și nivelurile de putere de transmisie. Experimentând cu plasarea routerului și nivelurile de putere a semnalului, puteți reduce acoperirea de transmisie a rețelei dvs. Wi-Fi, reducând astfel acest risc de compromis. Notă: deși acest lucru vă reduce riscul, un atacator motivat poate fi în continuare capabil să intercepteze un semnal care are o acoperire limitată.
Opriți rețeaua când nu este utilizată. Deși poate fi imposibil să dezactivați și să porniți frecvent semnalul Wi-Fi, luați în considerare dezactivarea acestuia în timpul călătoriilor sau în perioadele prelungite când nu va trebui să fiți online. În plus, multe routere oferă opțiunea de a configura un program wireless care va dezactiva automat Wi-Fi la anumite ore. Când conexiunea Wi-Fi este dezactivată, împiedicați atacatorii externi să poată exploata rețeaua dvs. de acasă.
Dezactivați Universal Plug and Play (UPnP) atunci când nu este necesar. UPnP este o caracteristică la îndemână care permite dispozitivelor din rețea să descopere și să stabilească fără probleme între ele în rețea. Cu toate acestea, deși caracteristica UPnP ușurează configurarea inițială a rețelei, este, de asemenea, un risc de securitate. Recentele atacuri de rețea la scară largă demonstrează că programele malware din rețeaua dvs. pot folosi UPnP pentru a ocoli firewall-ul routerului dvs., pentru a permite atacatorilor să preia controlul asupra dispozitivelor dvs. de la distanță și să răspândească malware pe alte dispozitive. Prin urmare, ar trebui să dezactivați UPnP, cu excepția cazului în care aveți o nevoie specifică de el.
Actualizați firmware-ul. Verificați site-ul web al producătorului routerului pentru a vă asigura că rulați cea mai recentă versiune de firmware. Actualizările de firmware îmbunătățesc performanța produsului, remediază defecțiunile și abordează vulnerabilitățile de securitate. Notă: unele routere au opțiunea de a activa actualizările automate.
Dezactivează gestionarea de la distanță. Majoritatea routerelor oferă opțiunea de a-și vizualiza și modifica setările pe internet. Dezactivați această funcție pentru a vă proteja împotriva accesului persoanelor neautorizate și a modificării configurației routerului.
Monitorizați pentru conexiuni necunoscute la dispozitiv. Utilizați site-ul web al producătorului routerului pentru a monitoriza dispozitivele neautorizate care se conectează sau încearcă să se alăture rețelei dvs. Consultați, de asemenea, site-ul web al producătorului pentru sfaturi despre cum să împiedicați conectarea dispozitivelor neautorizate la rețeaua dvs.

Reduceți amenințările prin e-mail

E-mailurile de tip phishing continuă să fie unul dintre cei mai obișnuiți vectori de atac inițial folosiți de către livrarea de programe malware și colectarea acreditărilor. Atacarea elementului uman – considerat cea mai slabă componentă din fiecare rețea – continuă să fie extrem de eficientă. Pentru a infecta un sistem, atacatorul trebuie pur și simplu să convingă un utilizator să facă clic pe un link sau să deschidă un atașament. Vestea bună este că există mulți indicatori pe care îi puteți folosi pentru a identifica rapid un e-mail de phishing. Cea mai bună apărare împotriva acestor atacuri este să devii un utilizator educat și precaut și să te familiarizezi cu cele mai comune elemente ale unui atac de tip phishing.

---------- 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

citi

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

Evitarea ingineriei sociale și a atacurilor de phishing

Nu oferiți altora informații sensibile decât dacă sunteți sigur că aceștia sunt într-adevăr cine pretind că sunt și că ar trebui să aibă acces la informații.

Ce este un atac de inginerie socială?

Într-un atac de inginerie socială, un atacator folosește interacțiunea umană (abilități sociale) pentru a obține sau a compromite informații despre o organizație sau sistemele sale informatice. Un atacator poate părea modest și respectabil, posibil pretinzând că este un nou angajat, reparator sau cercetător și chiar oferind acreditări pentru

a susține acea identitate. Cu toate acestea, punând întrebări, el sau ea poate fi capabil să strângă suficiente informații pentru a se infiltra în rețeaua unei organizații. Dacă un atacator nu este capabil să adune suficiente informații dintr-o sursă, el sau ea poate contacta o altă sursă din cadrul aceleiași organizații și se poate baza pe informațiile din prima sursă pentru a spori credibilitatea sa.

Ce este un atac de tip phishing?

Phishingul este o formă de inginerie socială. Atacurile de tip phishing folosesc e-mailuri sau site-uri web rău intenționate pentru a solicita informații personale, dându-se drept o organizație de încredere. De exemplu, un atacator poate trimite e-mailuri aparent de la o companie de card de credit reputată sau o instituție financiară care solicită informații despre cont, sugerând adesea că există o problemă. Când utilizatorii răspund cu informațiile solicitate, atacatorii le pot folosi pentru a obține acces la conturi.

Atacurile de tip phishing pot părea să provină și de la alte tipuri de organizații, cum ar fi organizațiile caritabile. Atacatorii profită adesea de evenimentele curente și de anumite perioade ale anului, cum ar fi

- Dezastre naturale (de exemplu, uraganul Katrina, tsunami indonezian)
- Epidemii și înfricoșări de sănătate (de exemplu, H1N1, COVID-19)
- Preocupări economice (de exemplu, escrocherii IRS)
- Alegeri politice majore
- Sărbători

Ce este un atac vishing?

Vishing este abordarea de inginerie socială care valorifică comunicarea vocală. Această tehnică poate fi combinată cu alte forme de inginerie socială care atrage o victimă să sune la un anumit număr și să divulge informații sensibile. Atacurile avansate de vishing pot avea loc complet prin comunicații vocale prin exploatarea soluțiilor Voice over Internet Protocol (VoIP) și a serviciilor de difuzare. VoIP permite cu ușurință falsificarea identității apelantului (ID), ceea ce poate profita de încrederea nepotrivită a publicului în securitatea serviciilor de telefonie, în special a serviciilor de telefonie fixă. Comunicarea prin telefon fix nu poate fi interceptată fără acces fizic la linie; totuși, această trăsătură nu este benefică atunci când comunicați direct cu un actor rău intenționat.

Ce este un atac zdrobitor?

Smishing este o formă de inginerie socială care exploatează mesajele SMS sau text. Mesajele text pot conține link-uri către lucruri precum pagini web, adrese de e-mail sau numere de telefon care, atunci când se fac clic, pot deschide automat o fereastră de browser sau un mesaj de e-mail sau pot forma un număr. Această integrare a funcției de e-mail, voce, mesaj text și browser web crește probabilitatea ca utilizatorii să fie victime ale activităților rău intenționate proiectate.

Care sunt indicatorii comuni ai încercărilor de phishing?

Adresa expeditorului suspect. Adresa expeditorului poate imita o afacere legitimă. Infractorii cibernetici folosesc adesea o adresă de e-mail care seamănă mult cu una de la o companie de renume, modificând sau omițând câteva caractere.

Salutări generice și semnătură. Atât o salutare generică, cum ar fi „Stimată client valoros” sau „Domnule/Doamnă”, cât și lipsa informațiilor de contact în blocul de semnătură sunt indicatori puternici ai unui e-mail de phishing. O organizație de încredere vă va adresa în mod normal pe nume și vă va furniza informațiile de contact.

hyperlinkuri și site-uri web falsificate. Dacă treceți cursorul peste orice link din corpul e-mailului, iar linkurile nu se potrivesc cu textul care apare atunci când treceți cu mouse-ul peste ele, este posibil ca linkul să fie falsificat. Site-urile web rău intenționate pot arăta identice cu un site legitim, dar adresa URL poate folosi o variație de ortografie sau un domeniu diferit (de exemplu, .com vs. .net). În plus, infractorii cibernetici pot folosi un serviciu de scurtare URL pentru a ascunde adevărata destinație a link-ului.

Ortografie și aspect. Structura proasta de gramatică și propoziție, greșelile de ortografie și formatarea inconsecventă sunt alți indicatori ai unei posibile încercări de phishing. Instituțiile de renume au personal dedicat care produce, verifică și corectează corespondența clienților.

Atașamente suspecte. Un e-mail nesolicitat care solicită unui utilizator să descarce și să deschidă un atașament este un mecanism comun de livrare pentru malware. Un infractor cibernetic poate folosi un fals sentiment de urgență sau de importanță pentru a ajuta un utilizator să descarce sau să deschidă un atașament fără a-l examina mai întâi.

Cum eviți să fii o victimă?

Fiți suspicios față de apelurile telefonice, vizitele sau mesajele de e-mail nesolicitate de la persoane care întreabă despre angajați sau alte informații interne. Dacă o persoană necunoscută pretinde că este dintr-o organizație legitimă, încercați să-i verificați identitatea direct la companie.

Nu furnizați informații personale sau informații despre organizația dvs., inclusiv structura sau rețelele acesteia, decât dacă sunteți sigur de autoritatea unei persoane de a deține informațiile.

Nu dezvăluie informații personale sau financiare prin e-mail și nu răspunde la solicitările prin e-mail pentru aceste informații. Aceasta include următoarele link-uri trimise prin e-mail.

Nu trimiteți informații sensibile pe internet înainte de a verifica securitatea unui site web. (Consultați Protejarea confidențialității pentru mai multe informații.)

Acordați atenție URL-ului (Uniform Resource Locator) al unui site web. Căutați adrese URL care încep cu „https" – o indicație că site-urile sunt sigure – și nu „http".

Căutați o pictogramă de lacăt închis - un semn că informațiile dvs. vor fi criptate.

Dacă nu sunteți sigur dacă o solicitare prin e-mail este legitimă, încercați să o verificați contactând direct compania. Nu utilizați informațiile de contact furnizate pe un site web conectat la cerere; în schimb, verificați declarațiile anterioare pentru informații de contact.

Instalați și întrețineți software antivirus, firewall-uri și filtre de e-mail pentru a reduce o parte din acest trafic.

Profitați de toate funcțiile anti-phishing oferite de clientul dvs. de e-mail și browserul web.

Implementați autentificarea cu mai mulți factori (MFA).

Ce faci dacă te crezi o victimă?

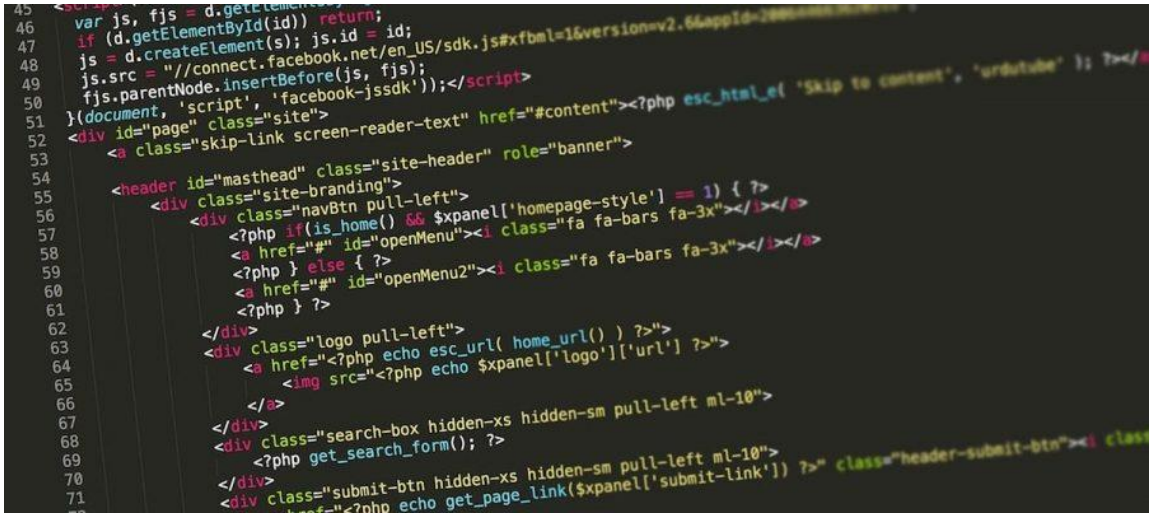
Dacă credeți că ați dezvăluit informații sensibile despre organizația dvs., raportați-le persoanelor corespunzătoare din cadrul organizației, inclusiv administratorilor de rețea. Ei pot fi atenți pentru orice activitate suspectă sau neobișnuită.

Dacă credeți că conturile dvs. financiare ar putea fi compromise, contactați imediat instituția dvs. financiară și închideți toate conturile care ar fi putut fi compromise. Urmăriți orice debitări inexplicabile pentru contul dvs.

Schimbați imediat orice parole pe care le-ați dezvăluit. Dacă ați folosit aceeași parolă pentru mai multe resurse, asigurați-vă că o schimbați pentru fiecare cont și nu utilizați acea parolă în viitor.

4.1.5 Ce este codul rău intenționat?

Codurile rău intenționate sunt fișiere sau programe nedorite care pot provoca daune unui computer sau pot compromite datele stocate pe un computer. Diverse clasificări ale codurilor rău intenționate includ viruși, viermi și cai troieni.



Viruși au capacitatea de a deteriora sau distruge fișiere de pe un sistem informatic și sunt răspândite prin partajarea unui mediu amovibil deja infectat, deschiderea atașamentelor de e-mail rău intenționate și vizitarea paginilor web rău intenționate.

Viermi sunt un tip de virus care se autopropaga de la computer la computer. Funcționalitatea sa este de a utiliza toate resursele computerului, ceea ce poate face ca computerul să nu mai răspundă.

Cai troieni sunt programe de calculator care ascund un virus sau un program potențial dăunător. Nu este neobișnuit ca software-ul gratuit să conțină un cal troian care face un utilizator să creadă că folosește software legitim, în schimb programul efectuează acțiuni rău intenționate pe computerul tău.

Fișiere de date rău intenționate sunt fișiere neexecutabile - cum ar fi un document Microsoft Word, un PDF Adobe, un fișier ZIP sau un fișier imagine - care exploatează punctele slabe ale programului software utilizat pentru a-l deschide. Atacatorii folosesc frecvent fișiere de date rău intenționate pentru a instala programe malware pe sistemul victimei, distribuind de obicei fișierele prin e-mail, rețele sociale și site-uri web.

Cum vă recuperați dacă deveniți victima unui cod rău intenționat?

Utilizarea software-ului antivirus este cea mai bună modalitate de a vă apăra computerul împotriva codurilor rău intenționate. Dacă credeți că computerul dvs. este infectat, rulați programul antivirus. În mod ideal, programul

dumneavoastră antivirus va identifica orice cod rău intenționat de pe computer și îl va pune în carantină, astfel încât să nu vă mai afecteze sistemul. De asemenea, ar trebui să luați în considerare acești pași suplimentari:

- Minimizați daunele. Dacă sunteți la serviciu și aveți acces la un departament de tehnologie a informației (IT), contactați-i imediat. Cu cât pot investiga și „curăța" mai devreme computerul dvs., cu atât este mai puțin probabil să provoace daune suplimentare computerului dvs. și altor computere din rețea. Dacă sunteți pe un computer sau laptop de acasă, deconectați-vă computerul de la internet; acest lucru va împiedica atacatorul să vă acceseze sistemul.
- Eliminați codul rău intenționat. Dacă aveți software antivirus instalat pe computer, actualizați software-ul și efectuați o scanare manuală a întregului sistem. Dacă nu aveți software antivirus, îl puteți achiziționa online sau într-un magazin de calculatoare. Dacă software-ul nu poate localiza și elimina infecția, poate fi necesar să vă reinstalați sistemul de operare, de obicei cu un disc de restaurare a sistemului. Rețineți că reinstalarea sau restaurarea sistemului de operare șterge de obicei toate fișierele și orice software suplimentar pe care l-ați instalat pe computer. După reinstalarea sistemului de operare și a oricărui alt software, instalați toate corecțiile adecvate pentru a remedia vulnerabilitățile cunoscute.

Amenințările la adresa computerului dvs. vor continua să evolueze. Deși nu puteți elimina orice pericol, prin utilizarea precauției, prin instalarea și utilizarea software-ului antivirus și urmând alte practici simple de securitate, vă puteți reduce semnificativ riscul și vă puteți consolida protecția împotriva codului rău intenționat.

Ce sunt site-urile de rețele sociale?

Site-urile de rețele sociale, denumite uneori site-uri „prietenul unui prieten", se bazează pe conceptul rețelelor sociale tradiționale în care ești conectat la oameni noi prin intermediul unor persoane pe care deja le cunoști. Scopul unor site-uri de rețea poate fi pur social, permițând utilizatorilor să stabilească prietenii sau relații romantice, în timp ce altele se pot concentra pe stabilirea de conexiuni de afaceri.

Deși caracteristicile site-urilor de rețele sociale diferă, toate vă permit să furnizați informații despre dvs. și să ofere un anumit tip de mecanism de comunicare (forumuri, camere de chat, e-mail, mesaje instant) care vă permit să vă conectați cu alți utilizatori. Pe unele site-uri, puteți căuta persoane pe baza anumitor criterii, în timp ce alte site-uri necesită să fiți „prezentat" unor persoane noi printr-o conexiune pe care o partajați. Multe dintre site-uri au comunități sau subgrupuri care se pot baza pe un anumit interes.

Ce implicații de securitate prezintă aceste site-uri?

Site-urile de rețele sociale se bazează pe conexiuni și comunicare, așa că vă încurajează să furnizați o anumită cantitate de informații personale. Atunci când decid câte informații să dezvăluie, este posibil ca oamenii să nu manifeste aceeași prudență ca atunci când întâlnesc pe cineva în persoană, deoarece

- Internetul oferă un sentiment de anonimat
- lipsa interacțiunii fizice oferă un fals sentiment de securitate
- ei adaptează informațiile pentru ca prietenii lor să le citească, uitând că alții le pot vedea
- doresc să ofere perspective pentru a impresiona potențialii prieteni sau asociați

Deși majoritatea persoanelor care folosesc aceste site-uri nu reprezintă o amenințare, persoanele rău intenționate pot fi atrase de ele din cauza accesibilității și cantității de informații personale disponibile. Cu cât oamenii rău intenționați au mai multe informații despre tine, cu atât le este mai ușor să profite de tine. Prădătorii pot forma relații online și apoi pot convinge persoane nebănuitoare să-i cunoască personal. Asta ar putea duce la o situație periculoasă. Informațiile personale pot fi folosite și pentru a efectua un atac de inginerie socială. Folosind informațiile pe care le furnizați despre locația, hobby-urile, interesele și prietenii dvs., o persoană rău intenționată ar putea uzurpa identitatea unui prieten de încredere sau vă poate convinge că are autoritatea de a accesa alte date personale sau financiare.

În plus, din cauza popularității acestor site-uri, atacatorii le pot folosi pentru a distribui coduri rău intenționate. Site-urile care oferă aplicații dezvoltate de terți sunt deosebit de sensibile. Atacatorii pot crea aplicații personalizate care par a fi nevinovate în timp ce îți infectează computerul sau îți partajează informațiile fără știrea ta.

4.1.6 Activitati practice

Pasul 1: Curățarea prafului de pe computere

1. Această problemă poate fi observată prin zgomotul produs de viteza ventilatoarelor de răcire, atunci când utilizați computerul personal sau laptopul personal.
2. Probabil ați observat că la începutul utilizării computerului, când era nou, ventilatoarele de răcire erau silențioase pentru că ventilatoarele de răcire nu erau pline de praf.
3. După o perioadă mai lungă de utilizare, computerul/laptop-ul devine foarte zgomotos din cauza vitezei mari a ventilatoarelor prăfuite, care nu mai reușesc să asigure debitul de aer necesar răcirii componentelor electronice din computer, ajungând într-un punct de oprire (blocarea).) și duce la distrugerea componentelor interne, a microprocesoarelor din cauza temperaturii ridicate de funcționare.
4. Aspectul negativ al prafului este efectul termic creat de depunerea de praf pe componente (pe și în jurul radiatorului procesorului).
5. Astfel existenta prafului in calculator poate provoca distrugerea componentelor electronice. Din cauza prafului se supraincalzesc ducand la distrugerea lor. Din acest motiv, computerele trebuie curățate regulat de praf.
6. Presupunând că aveți acasă un computer pe care îl utilizați, vă rugăm să răspundeți la următoarea întrebare: „Când ați curățat ultima dată computerul de praf?”
7. Curățarea se poate face la un atelier specializat de depanare computer.
8. Curățarea prafului pe laptopuri necesită operații mai dificile din acest motiv trebuie să apelați la un service specializat.
9. Pentru a înțelege ce înseamnă curățarea unui computer cu praf, poți căuta pe internet, deschizând un motor de căutare pe internet și tastând în câmpul de căutare „cum se curăță praful de pe computere?”. Un site web pe care îl recomandăm este:https://www.wikihow.com/Clean-a-Dusty-Computer
10. Totusi, avand in vedere faptul ca acest curs se adreseaza incepatorilor, cu mai putine cunostinte in acest domeniu, va recomandam ca pentru inceput sa curatati calculatorul pentru a apela la un service specializat.

Pasul 2: Pentru un computer este necesar să instalați un program de protecție antivirus / firewall

1. Pentru a înțelege ce este un software antivirus, vă recomandăm să accesați site-ul web: https://us.norton.com/internetsecurity-malware-what-is-antivirus.html

2. Desigur, există multe software antivirus pe piață. O căutare pe internet, de exemplu, pentru cuvintele cheie „comparare software antivirus" poate găsi nenumărate pagini pentru a găsi informații despre software-ul existent, cum ar fi:https://www.pcmag.com/picks/the-best-antivirus-protection unde în secțiunea „CELE 13 ALEGERII NOASTRE DE TOP" sunt enumerate mai multe software antivirus

3. În computerul dvs., dacă nu aveți alt antivirus instalat, vă recomandăm să căutați într-o pagină de căutare cuvintele cheie „free trial antivirus" și să accesați linkulhttps://www.kaspersky.com/downloads/thank-you/antivirus-free-trial iar în pagina deschisă, faceți clic pe butonul „DOWNLOAD NOW".

4. Computerul pe care îl folosim, de exemplu, are sistem de operare WINDOWS 10 și „Google Chrome" ca browser de internet

5. Recomandarea pentru Kaspersky a fost făcută, datorită faptului că pe computerul pe care îl folosim, aceasta este soluția de securitate antivirus instalată, iar pentru a nu genera conflicte cu alte tipuri de software antivirus, am recomandat această soluție.

6. În partea de jos a ferestrei browser Chrome, după apăsarea butonului „DOWNLOAD NOW", este afișată arhiva executabilă „kav21.3.10.391en_26075.exe" (desigur că numele arhivei poate varia în funcție de versiunea descărcată)

7. Acum, după descărcarea de pe internet și instalarea, ați instalat o soluție de securitate antivirus în computer! Felicitări!

8. Antivirusul funcționează întotdeauna și este activ în fundalul sistemului de operare

9. În partea dreaptă jos a ecranului, lângă ceas, apare o pictogramă cu „K". Este posibil ca această pictogramă să fie ascunsă de sistemul Windows, motiv pentru care va fi necesar să faceți mai întâi clic pe butonul „^", de lângă ceas.

10. Dacă faceți clic pe pictograma „K", se lansează interfața de setări antivirus Kaspersky.

11. În interfața deschisă faceți clic pe zona butonului „SARCINI", iar în fereastra deschisă din zona „SCANARE COMPLETĂ" faceți clic pe START. Observăm că software-ul antivirus începe să scaneze computerul pentru viruși, dacă există.

12. După finalizarea scanării, scanarea poate fi repornită oricând se dorește. Antivirusul poate fi setat să pornească automat procesul de scanare a computerului

13. Tot in aceasta fereastra deschisa cand dai click pe TASKS, deruland mai jos, ajungi in zona UPDATE. Prin apăsarea butonului START din această zonă, aplicația antivirus va fi actualizată la cea mai recentă versiune și la cea mai recentă bază de date furnizată de producător. Se recomandă ca această actualizare să se facă periodic

14. Trebuie remarcat faptul că soluțiile de securitate, pot fi atât pentru protejarea computerului personal împotriva virușilor, cât și pentru protejarea computerului împotriva accesului neautorizat, atunci când computerul se află într-o rețea de calculatoare.

15. Pentru această situație pe site-ul Kaspersky https://www.kaspersky.com/home-security sunt prezentate 3 variante ale softului de protectie, alaturi de fiecare fiind specificate pentru ce poate asigura protectia

16. De exemplu, soluția de protecție „Kaspersky Internet Security" este o soluție integrată care asigură atât protecție antivirus, cât și protecție în rețeaua de calculatoare (firewall).

17. În general, toate programele de protecție antivirus oferă opțiuni integrate atât pentru protecție antivirus, cât și pentru protecție în rețeaua de calculatoare.

18. În mod similar, alte programe antivirus pot fi instalate accesând pagina dedicată a producătorului pentru descărcarea și achiziționarea de licențe aferente.

19. Prezentarea nu se limitează strict la antivirus Kaspersky! La alegere și în funcție de nevoile fiecăruia dintre voi, la fel, se pot instala și alte programe antivirus atât pe computer, cât și pe sisteme electronice portabile.

4.2 Protejarea datelor personale și a confidențialității

Unitatea 4.2	Protejarea datelor personale și a confidențialității
Durată	9h
Obiective	Pentru a fi la curent cu problemele legate de partajarea datelor cu caracter personal Pentru a putea configura setările de securitate pentru a păstra confidențialitatea
Conținut	4.2.1 Protejarea dvs. online 4.2.2 Orientări pentru partajarea informațiilor personale 4.2.3 Activități practice
Resurse	Manual de instruire, calculatoare cu acces la internet
Metodologii de instruire	Prezentare de către trainer Exercițiu de grup Discuție / Dezbatere

Masa 23- Structura unității de competență 4.2. – Protejarea datelor cu caracter personal și a confidențialității Modulului 4 – Securitate.

4.2.1 Protejează-te online

Cum te poți proteja?

Limitați cantitatea de informații personale pe care le postați - Nu postați informații care v-ar face vulnerabil, cum ar fi adresa sau informații despre programul sau rutina dvs. Dacă conexiunile dvs. postează informații despre dvs., asigurați-vă că informațiile combinate nu sunt mai mult decât v-ați simți confortabil să știe străinii. De asemenea, fiți atenți când postați informații, inclusiv fotografii, despre conexiunile dvs.

Amintiți-vă că internetul este o resursă publică - Postați numai informații pe care vă simțiți confortabil cu oricine să le vadă. Acestea includ informații și fotografii din profilul dvs. și din bloguri și alte forumuri. De asemenea, odată ce postați informații online, nu le puteți retrage. Chiar dacă eliminați informațiile de pe un site, versiunile salvate sau stocate în cache pot exista în continuare pe computerele altor persoane.

Ai grijă de străini - Internetul le face mai ușor pentru oameni să își prezinte greșit identitățile și motivele. Luați în considerare limitarea persoanelor cărora li se permite să vă contacteze pe aceste site-uri. Dacă interacționați cu persoane pe care nu le cunoașteți, fiți atenți la cantitatea de informații pe care le dezvăluiți sau sunteți de acord să le întâlniți personal.

Fii sceptic - Nu crede tot ce citești online. Oamenii pot posta informații false sau înșelătoare despre diferite subiecte, inclusiv despre propriile identități. Acest lucru nu se face neapărat cu intenții rău intenționate; ar putea fi neintenționat, o exagerare sau o glumă. Totuși, luați măsurile de precauție adecvate și încercați să verificați autenticitatea oricărei informații înainte de a lua orice măsură.

Evaluează-ți setările - Profitați de setările de confidențialitate ale unui site. Setările implicite pentru unele site-uri pot permite oricui să vă vadă profilul, dar vă puteți personaliza setările pentru a restricționa accesul numai la anumite persoane. Există încă riscul ca informațiile private să poată fi expuse în ciuda acestor restricții, așa că nu postați nimic pe care nu ați dori să vadă publicul. Site-urile își pot schimba opțiunile periodic, așa că revizuiți-vă setările de securitate și confidențialitate în mod regulat pentru a vă asigura că alegerile dvs. sunt în continuare adecvate.

Fiți atenți la aplicațiile de la terți - Aplicațiile de la terțe părți pot oferi divertisment sau funcționalitate, dar aveți grijă când decideți ce aplicații să activați. Evitați aplicațiile care par suspecte și modificați setările pentru a limita cantitatea de informații pe care aplicațiile le pot accesa.

Folosiți parole puternice - Protejați-vă contul cu parole care nu pot fi ghicite cu ușurință. Dacă parola dvs. este compromisă, altcineva poate să vă acceseze contul și să pretindă că sunteți dvs.

Verificați politicile de confidențialitate - Unele site-uri pot partaja informații precum adrese de e-mail sau preferințe ale utilizatorilor cu alte companii. Acest lucru poate duce la o creștere a spam-ului. De asemenea, încercați să găsiți politica de gestionare a recomandărilor pentru a vă asigura că nu vă înscrieți neintenționat prietenii pentru spam. Unele site-uri vor continua să trimită mesaje de e-mail oricărei persoane pe care le trimiteți până când acestea se alătură.

Țineți software-ul, în special browserul dvs. web, actualizat - Instalați actualizări de software, astfel încât atacatorii să nu poată profita de problemele sau vulnerabilitățile cunoscute. (Consultați Înțelegerea corecțiilor.) Multe sisteme de operare oferă actualizări automate. Dacă această opțiune este disponibilă, ar trebui să o activați.

Utilizați și întrețineți software antivirus - Software-ul antivirus vă ajută să vă protejați computerul împotriva virușilor cunoscuți, astfel încât este posibil să puteți detecta și elimina virusul înainte ca acesta să provoace daune. (Consultați Înțelegerea software-ului antivirus.) Deoarece atacatorii scriu continuu viruși noi, este important să vă mențineți definițiile la zi.

Copiii sunt în special sensibili la amenințările pe care le prezintă site-urile de socializare- Deși multe dintre aceste site-uri au restricții de vârstă, copiii pot denatura vârsta lor, astfel încât să se poată înscrie. Învățându-i pe copii despre siguranța pe internet, fiind conștienți de obiceiurile lor online și îndrumându-i către site-uri adecvate, părinții se pot asigura că copiii devin utilizatori siguri și responsabili.

De ce este important să ne amintim că internetul este public?

Internetul este o resursă accesibilă și populară pentru comunicarea cu ceilalți și efectuarea de cercetări. Este posibil să aveți un sentiment de anonimat în timp ce sunteți online, dar ar trebui să vă amintiți că nu sunteți anonim și că este la fel de ușor pentru oameni să găsească informații despre dvs., precum este pentru dvs. să găsiți informații despre ei.

Mulți oameni au devenit atât de familiarizați și confortabili cu internetul încât adoptă practici care îi fac vulnerabili. De exemplu, deși oamenii sunt de obicei precauți în a împărtăși informații personale cu străinii pe care îi întâlnesc pe stradă, este posibil să nu ezite să posteze aceleași informații online. Odată ce este online, poate fi accesat de o lume de străini și nu ai idee ce ar putea face cu aceste informații.

4.2.2 Orientări pentru partajarea informațiilor personale

Ce îndrumări puteți urma atunci când publicați informații pe internet?

Priviți internetul ca pe un roman, nu ca pe un jurnal. Asigurați-vă că vă simțiți confortabil cu oricine care vad informațiile pe care le puneți pe bloguri, site-uri de rețele sociale și site-uri web personale - scrieți-le cu așteptarea că sunt disponibile pentru consumul public și că oamenii pe care nu i-ați întâlnit niciodată vă vor găsi pagina. Deși unele site-uri folosesc parole sau alte restricții de securitate pentru a proteja informațiile, aceste metode nu sunt folosite pentru majoritatea site-urilor web. Dacă doriți ca informațiile să fie private sau limitate la un grup mic și select de persoane, internetul nu este cel mai bun forum.

Limitați cantitatea de informații personale pe care le postați. Nu postați informații care v-ar putea face vulnerabil, cum ar fi adresa, numărul de telefon, e-mailul sau informații despre programul sau rutina dvs. Furnizarea adresei dvs. de e-mail poate crește cantitatea de spam pe care o primiți (consultați Reducerea spamului pentru mai multe informații). Furnizarea de detalii despre hobby-urile dvs., locul de muncă, familia și prietenii sau trecutul dvs. poate oferi atacatorilor suficiente informații pentru a efectua un atac de inginerie socială cu succes (consultați Evitarea atacurilor de inginerie socială și phishing și Menținerea în siguranță pe site-urile de rețele sociale pentru mai multe informații).

Realizați că nu o puteți lua înapoi. Odată ce publicați ceva online, acesta este disponibil pentru alte persoane și pentru motoarele de căutare. Puteți modifica sau elimina informații după ce ceva a fost publicat, dar este posibil ca cineva să fi văzut deja versiunea originală. Chiar dacă încercați să eliminați paginile de pe internet, este posibil ca cineva să fi salvat o copie a paginii sau să fi folosit fragmente dintr-o altă sursă. Unele motoare de căutare „memorează cache" copii ale paginilor web; aceste copii stocate în cache pot fi disponibile după ce o pagină web a fost ștearsă sau modificată. Unele browsere web pot păstra, de asemenea, o memorie cache a paginilor web pe care le-a vizitat un utilizator, astfel încât versiunea originală poate fi stocată într-un fișier temporar pe computerul utilizatorului. Gândiți-vă la aceste implicații înainte de a publica informații – odată ce ceva apare, nu puteți garanta că îl puteți elimina complet.

Ca practică generală, lăsați bunul simț să vă ghideze deciziile cu privire la ce să postați online. Înainte de a publica ceva pe internet, stabiliți ce valoare oferă acesta și luați în considerare implicațiile pe care le are ca informația să fie disponibilă publicului. Furtul de identitate este o problemă din ce în ce mai mare și cu cât un atacator poate aduna mai multe informații despre tine, cu atât este mai ușor să te prefaci că ești tu.

Cât de anonim ești?

S-ar putea să credeți că sunteți anonim în timp ce navigați pe site-uri web, dar informații despre dvs. sunt întotdeauna lăsate în urmă. Puteți reduce cantitatea de informații dezvăluite despre dvs. vizitând site-uri legitime, verificând politicile de confidențialitate și minimizând cantitatea de informații personale pe care o furnizați.

Ce informații sunt colectate?

Când vizitați un site web, o anumită cantitate de informații este trimisă automat către site. Aceste informații pot include următoarele:

- Adresă IP - Fiecărui computer de pe internet i se atribuie o adresă IP specifică, unică (protocol de internet). Computerul dvs. poate avea o adresă IP statică sau o adresă IP dinamică. Dacă aveți o adresă

IP statică, aceasta nu se schimbă niciodată. Cu toate acestea, unii ISP-uri dețin un bloc de adrese și atribuie unul deschis de fiecare dată când vă conectați la internet - aceasta este o adresă IP dinamică. Puteți determina adresa IP a computerului dvs. în orice moment, vizitând www.showmyip.com.

- Nume de domeniu - Internetul este împărțit în domenii, iar contul fiecărui utilizator este asociat cu unul dintre acele domenii. Puteți identifica domeniul uitându-vă la sfârșitul URL-ului; de exemplu, .edu indică o instituție de învățământ, .gov indică o agenție guvernamentală din SUA, .org se referă la organizație și .com este pentru uz comercial. Multe țări au, de asemenea, nume de domenii specifice. Lista numelor de domenii active este disponibilă de la Internet Assigned Numbers Authority (IANA).
- Detalii software - Este posibil ca o organizație să determine ce browser, inclusiv versiunea, pe care l-ați folosit pentru a-și accesa site-ul. De asemenea, organizația poate determina ce sistem de operare rulează computerul dvs.
- Vizite în pagină - Informațiile despre paginile pe care le-ați vizitat, cât timp ați stat pe o anumită pagină și dacă ați ajuns pe site dintr-un motor de căutare sunt adesea disponibile pentru organizația care operează site-ul.
- Dacă un site web folosește cookie-uri, organizația poate să colecteze și mai multe informații, cum ar fi tiparele dvs. de navigare, care includ alte site-uri pe care le-ați vizitat. Dacă site-ul pe care îl vizitați este rău intenționat, fișierele de pe computerul dvs., precum și parolele stocate în memoria temporară pot fi în pericol.

Cum sunt utilizate aceste informații?

În general, organizațiile folosesc informațiile care sunt colectate automat în scopuri legitime, cum ar fi generarea de statistici despre site-urile lor. Analizând statisticile, organizațiile pot înțelege mai bine popularitatea site-ului și care sunt zonele de conținut care sunt cel mai mult accesate. Este posibil ca aceștia să poată folosi aceste informații pentru a modifica site-ul pentru a sprijini mai bine comportamentul persoanelor care îl vizitează.

O altă modalitate de a aplica informațiile adunate despre utilizatori este marketingul. Dacă site-ul folosește cookie-uri pentru a determina alte site-uri sau pagini pe care le-ați vizitat, poate folosi aceste informații pentru a face publicitate anumitor produse. Produsele pot fi pe același site sau pot fi oferite de site-uri partenere.

Cu toate acestea, unele site-uri pot colecta informațiile dvs. în scopuri rău intenționate. Dacă atacatorii pot accesa fișierele, parolele sau informațiile personale de pe computerul dvs., ei pot folosi aceste date în avantajul lor. Atacatorii ar putea să vă fure identitatea, folosind și abuzând de informațiile dumneavoastră personale pentru câștiguri financiare. O practică comună este ca atacatorii să folosească acest tip de informații o dată sau de două ori, apoi să le vândă sau să le schimbe altor persoane. Atacatorii profită de pe urma vânzării sau comerțului, iar creșterea numărului de tranzacții face mai dificilă urmărirea oricărei activități până la ei. Atacatorii pot modifica, de asemenea, setările de securitate de pe computer, astfel încât să poată accesa și utiliza computerul pentru alte activități rău intenționate.

Expuneți și alte informații personale?

În timp ce utilizarea cookie-urilor poate fi o metodă de culegere de informații, cea mai ușoară modalitate prin care atacatorii pot obține acces la informații personale este să le ceară. Reprezentând un site rău intenționat ca fiind unul legitim, atacatorii vă pot convinge să le furnizați adresa, informațiile despre cardul de credit, numărul de securitate socială sau alte date personale.

4.2.3 Activități practice

Pasul 1: Blocați computerul cu parolă

1. Echipamentul de astăzi oferă mai multe modalități de a vă proteja! De exemplu în WINDOWS 10 în secțiunea SETĂRI -> Opțiuni de conectare ai posibilitatea de a-ți parola computerul prin una dintre opțiuni: recunoaștere facială, amprentă, PIN, cheie de securitate, parolă sau recunoaștere a imaginii.
2. Nu vom discuta astăzi despre toate acestea, dar trebuie menționat că orice computer oferă posibilitatea de a seta o parolă (acest lucru se poate face în general din secțiunea SETĂRI a echipamentului dumneavoastră)
3. Astăzi ne concentrăm pe setarea unei parole. Parola este o succesiune de caractere scrise într-o ordine dată, care poate conține: majuscule, litere mici, cifre, caractere speciale
4. De exemplu, dacă în WINDOWS setăm parola „@calculatorMeuDeNota10” la SETĂRI -> Opțiuni de conectare, atunci la accesarea computerului la repornire sau la ieșirea din sistemul de operare din standby, se va solicita parola. Ce parola? @calculatorulMeuDeNota10, literele scrise exact în aceeași ordine și același tip de literă. ATENTIE: calculatorul nu va recunoaste parola @CALCULATORULMEUDENOTA10 sau @calculatorulmeudenota10 sau @ calculatorulMeu De Nota 10. Parola recunoscuta de sistem va fi exact ca cea stabilita, respectiv @ calculatorulMeuDeNota10
5. Atenție: o parolă setată, nu o uitați! Cel mai bine ar fi să-l notați undeva unde îl puteți găsi. Dacă v-ați uitat parola, există diferite modalități de a o recupera, dar acest lucru necesită cunoștințe mult mai avansate și aduce adesea probleme în recuperarea acesteia.
6. O parolă trebuie să conțină caractere speciale (@), litere mici (computer eu e ota), litere mari (MDN), cifre (10).
7. Cu cât o parolă conține mai multe caractere, acea parolă va fi mult mai puternică și va fi mai greu pentru cineva să o găsească.
8. Pentru a înțelege ce este o parolă puternică, vă recomandăm să accesați următorul site:https://ro.safetydetectives.com/password-meter/
9. În partea din dreapta sus, puteți seta limba în care vor fi afișate informațiile de pe site
10. În câmpul de sub titlul „Cât de sigură este parola mea?” puteți tasta și testa modele de parole

11. Cu cât este mai mare numărul de caractere pe care parola conține și mai multe caractere enumerate mai sus, cu atât scorul obținut în partea dreaptă a câmpului va fi mai mare, iar tipul de parolă devine de la FOARTE SLAB la FOARTE PUTERNIC
12. Încercați să găsiți o parolă care să primească nota 100! reusesti? Parola de la acest exercițiu ce punctaj crezi că va obține?
13. În cele din urmă, vă recomandăm să citiți secțiunea Întrebări frecvente din partea de jos a paginiihttps://ro.safetydetectives.com/password-meter/
14. În acest fel veți obține mai multe informații despre cum să creați parole foarte bune și sigure.

Pasul 2: Utilizarea unui browser și actualizări periodice

1. Deschideți o pagină web, introduceți adresa de internet www.google.com și introduceți următoarele cuvinte „chrome download" în câmpul de căutare
2. Pe computer, căutați și descărcați browserul de internet Chrome (dacă nu este deja instalat) lahttps://www.google.com/chrome/
3. Din pagina deschisă apăsați butonul DOWNLOAD CHROME
4. Accesați fișierul descărcat și urmați pașii de instalare
5. Deschideți una sau mai multe pagini web în browserul Chrome (decizia dvs. ce pagini web doriți să accesați)
6. Observați în bara de navigare dacă există sau nu un lacăt în fața adresei de internet accesate
7. Acel lacat reprezinta un certificat de securitate pentru pagina accesata si in lipsa acestuia navigarea pe pagina nu este sigura. Deci o navigare sigură se poate face pe acele pagini de internet atunci când lacătul există
8. Pe o pagină web securizată (unde există acel lacăt), faceți clic pe acel lacăt și observați din informațiile furnizate dacă certificatul este valabil
9. Faceți clic pe Certificat (Valid) și respectați data până la care certificatul este valabil
10. Pictograma „lacăt" este o confirmare că conexiunea la Internet între persoana care accesează acel site și serverul acelui site este o conexiune securizată, este o comunicare criptată (alți utilizatori nu pot accesa, intercepta, conexiunea stabilită a dvs. cu acel site). site web)
11. Închideți fereastra cu informații despre certificat și faceți clic pe cele 3 puncte verticale din dreapta sus (situate sub fereastra de închidere X) pentru a accesa setările Chrome
12. Faceți clic pe „Ajutor" și în noul meniu faceți clic pe „Despre Google Chrome"
13. În acest moment, Google Chrome va încerca să actualizeze la cea mai recentă versiune disponibilă a software-ului cu următorul mesaj:
    „Actualizarea Google Chrome (50%)
    Versiunea 90.0.4430.212 (build oficial) (64 de biți)"
14. După actualizare, Chrome vă poate solicita să reporniți browserul cu un mesaj

„Aproape la zi! Relansați Google Chrome pentru a finaliza actualizarea. Ferestrele incognito nu se vor redeschide.
Versiunea 90.0.4430.212 (build oficial) (64 de biți)”

15. Apăsați butonul „Relunch”
16. Dacă nu este necesară redeschiderea browserului sau browserul este deja actualizat, va apărea un mesaj „Google Chrome este la zi
    Versiunea 91.0.4472.77 (build oficial) (64 de biți)”
17. În acest fel browserul Chrome poate fi actualizat
18. Vă rugăm să rețineți că orice software și nu doar browserul Chrome oferă posibilitatea de a actualiza la versiuni superioare, dar nu toate programele oferă această funcție gratuit
19. Actualizarea la versiuni mai noi oferă securitatea și stabilitatea software-ului în uz

4.3 Protejarea sănătății și a bunăstării

Unitatea 4.3	Protejarea sănătății și a bunăstării
Durată	5h
Obiective	pentru a putea evita riscurile pentru sănătate și amenințările la adresa bunăstării fizice și psihologice în timpul utilizării tehnologiilor digitale; să se poată proteja pe sine și pe ceilalți de posibilele pericole din mediile digitale; să poată controla aspectele care distrag atenția de la muncă și viața digitală; sa poata lua masuri preventive pentru protejarea sanatatii persoanei de care raspunde
Conţinut	4.3.1 Efectele negative ale tehnologiei: ce să știți 4.3.2 Ați auzit de cyberbullying? 4.3.3 Activități practice
Resurse	Manual de instruire, calculatoare cu acces la internet
Metodologii de instruire	Prezentare de către trainer

Masa 24- Structura unităţii de competenţă 4.3. – Protejarea sănătății și bunăstării Modulului 4 – Securitate.

4.3.1 Efectele negative ale tehnologiei: ce să știți

Oamenii sunt mai conectați ca niciodată, datorită în mare parte progreselor rapide ale tehnologiei.

În timp ce unele forme de tehnologie ar fi putut produce schimbări pozitive în lume, există dovezi pentru efectele negative ale tehnologiei și utilizarea excesivă a acesteia.

Rețelele sociale și dispozitivele mobile pot duce la probleme psihologice și fizice, cum ar fi oboseala ochilor și dificultăți de concentrare pe sarcini importante. Ele pot contribui, de asemenea, la afecțiuni mai grave de sănătate, cum ar fi depresia.

Efecte psihologice

Utilizarea excesivă sau dependența de tehnologie poate avea efecte psihologice adverse, inclusiv: Izolarea. Tehnologiile, cum ar fi rețelele sociale, sunt concepute pentru a aduce oamenii împreună, dar pot avea efectul opus în unele cazuri.

Un studiu din 2017 pe adulți tineri cu vârsta cuprinsă între 19 și 32 de ani a constatat că persoanele cu o utilizare mai mare a rețelelor sociale aveau mai mult de trei ori mai multe șanse de a se simți izolați social decât cei care nu folosesc rețelele sociale la fel de des.

Găsirea unor modalități de reducere a utilizării rețelelor sociale, cum ar fi stabilirea limitelor de timp pentru aplicațiile sociale, poate ajuta la reducerea sentimentelor de izolare la unii oameni.

Depresie și anxietate

Autorii unei revizuiri sistematice din 2016 Trusted Source au discutat legătura dintre rețelele sociale și problemele de sănătate mintală, cum ar fi depresia și anxietatea.

Cercetările lor au găsit rezultate mixte. Persoanele care au avut mai multe interacțiuni pozitive și sprijin social pe aceste platforme păreau să aibă niveluri mai scăzute de depresie și anxietate.

Cu toate acestea, era adevărat și invers. Oamenii care au perceput că au mai multe interacțiuni sociale negative online și care au fost mai predispuși la comparații sociale au experimentat niveluri mai ridicate de depresie și anxietate.

Deci, deși pare să existe o legătură între rețelele sociale și sănătatea mintală, un factor determinant semnificativ îl reprezintă tipurile de interacțiuni pe care oamenii simt că le au pe aceste platforme.

Efecte asupra sănătății fizice

Utilizarea tehnologiei poate crește și riscul de probleme fizice, inclusiv:

Oboseala ochilor

Tehnologiile, cum ar fi tabletele portabile, smartphone-urile și computerele, pot reține atenția unei persoane pentru perioade lungi de timp. Acest lucru poate duce la oboseala ochilor.

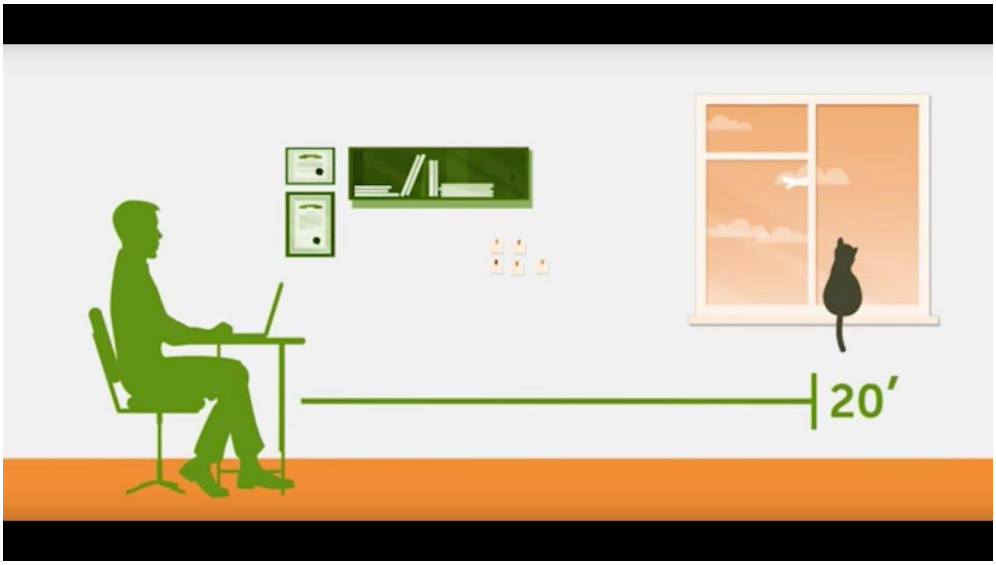
Simptomele oboselii oculare digitale pot include vedere încețoșată și ochi uscați. Oboseala ochilor poate duce, de asemenea, la dureri în alte zone ale corpului, cum ar fi capul, gâtul sau umerii.

Mai mulți factori tehnologici pot duce la oboseala ochilor, cum ar fi:

- timpul ecranului
- strălucirea ecranului
- luminozitatea ecranului
- vizualizarea prea aproape sau prea departe
- postură proastă în șezut
- problemele de vedere subiacente

Luând pauze regulate departe de ecran poate reduce probabilitatea de oboseală a ochilor.

Oricine se confruntă în mod regulat cu aceste simptome ar trebui să consulte un optometrist pentru un control.



Regula 20-20-20 pentru vizionarea digitală

Când utilizați orice formă de ecran digital pentru perioade mai lungi de timp, este recomandat să folosiți regula 20-20-20. Pentru a folosi regula, după fiecare 20 de minute de timp pe ecran, luați o pauză de 20 de secunde pentru a privi ceva la cel puțin 20 m distanță. Acest lucru poate ajuta la reducerea tensiunii asupra ochilor de la privirea la un ecran pentru o perioadă continuă.

Poziție proastă

Modul în care mulți oameni folosesc dispozitivele mobile și computerele poate contribui, de asemenea, la o postură incorectă. În timp, acest lucru poate duce la probleme musculo-scheletice. Multe tehnologii promovează

o poziție de utilizator „în jos și înainte”, ceea ce înseamnă că persoana este cocoșată în față și privește în jos la ecran. Acest lucru poate pune o presiune inutilă asupra gâtului și coloanei vertebrale. Un studiu de 5 ani în jurnalul Applied Ergonomics a descoperit o asociere între mesajele de pe un telefon mobil și durerile de gât sau de spate la adulții tineri. Rezultatele au indicat că efectele au fost în mare parte pe termen scurt, deși unii oameni au continuat să aibă simptome pe termen lung.

Cu toate acestea, unele studii contestă aceste rezultate.

Un studiu din 2018 sursă de încredere din European Spine Journal a constatat că postura gâtului în timp ce trimiteți mesaje nu a făcut nicio diferență în simptomele precum durerea de gât.

Acest studiu a concluzionat că mesajele text și „gâtul textului” nu au influențat durerea de gât la adulții tineri. Cu toate acestea, studiul nu a inclus o urmărire pe termen lung. Este posibil ca și alți factori să influențeze durerea de gât, cum ar fi vârsta și nivelul de activitate. Corectarea problemelor de postură în timpul utilizării tehnologiei poate duce la o îmbunătățire generală a posturii și a forței la nivelul miezului, gâtului și spatelui.

De exemplu, dacă o persoană se află în aceeași poziție ore întregi, cum ar fi stând la un birou în timp ce lucrează, statul în picioare sau întinderea regulat poate ajuta la reducerea tensiunii asupra corpului.

În plus, luarea de pauze scurte, cum ar fi mersul în jurul biroului la fiecare oră, poate ajuta, de asemenea, să mențină mușchii liberi și să evite tensiunea și postura incorectă.

Probleme de somn

Utilizarea tehnologiei prea aproape de ora de culcare poate cauza probleme cu somnul. Acest efect are de-a face cu faptul că lumina albastră, cum ar fi lumina telefoanelor mobile, cititoarelor electronice și computerelor, stimulează creierul. Autorii unui studiu din 2014 au descoperit că această lumină albastră este suficientă pentru a perturba ritmul circadian natural al corpului. Această tulburare ar putea îngreuna adormirea sau poate duce la o persoană să se simtă mai puțin alertă a doua zi. Pentru a evita impactul potențial al luminii albastre asupra creierului, oamenii pot înceta să mai folosească dispozitive electronice care emit lumină albastră cu o oră sau două înainte de culcare. În schimb, activitățile blânde cu care să te relaxezi, cum ar fi citirea unei cărți, întinderi ușoare sau baie, sunt alternative.

Activitate fizică redusă

Majoritatea tehnologiilor digitale de zi cu zi sunt sedentare. Utilizarea mai extinsă a acestor tehnologii promovează un stil de viață mai sedentar, despre care se știe că are efecte negative asupra sănătății, cum ar fi contribuția la:

- obezitatea
- boala cardiovasculara
- diabet de tip 2
- moarte prematura

Găsirea unor modalități de a lua pauze de la tehnologiile sedentare poate ajuta la promovarea unui stil de viață mai activ.

Cercetările din 2017 indică faptul că tehnologiile active, cum ar fi notificările aplicațiilor, e-mailurile și tehnologiile portabile care promovează exercițiile fizice pot reduce comportamentul sedentar pe termen scurt. Acest lucru ar putea ajuta oamenii să stabilească modele sănătoase și să devină mai activi fizic.

4.3.2 Ați auzit de cyberbullying?

Hărțuirea cibernetică folosește tehnologia pentru a hărțui sau a hărțui pe altcineva. Bătăușii erau restricționați la metode precum intimidarea fizică, corespondența poștală sau telefonul, dar computerele, telefoanele mobile, tabletele și alte dispozitive mobile oferă forumuri pentru bătăuși, cum ar fi e-mailul, mesageria instantanee, pagini web și fotografii digitale.

Formele de hărțuire cibernetică pot varia în severitate, de la zvonuri crude sau jenante la amenințări, hărțuire sau urmărire. Poate afecta orice grupă de vârstă; cu toate acestea, adolescenții și adulții tineri sunt victime obișnuite, iar hărțuirea cibernetică este o problemă în creștere în școli.

De ce a devenit cyberbullying o astfel de problemă?

Relativul anonimat al internetului este atrăgător pentru bătăuși, deoarece sporește intimidarea și îngreunează urmărirea activității. De asemenea, unor bătăuși le este mai ușor să fie mai vicioși, deoarece nu există un contact personal. Internetul și e-mailul pot crește și vizibilitatea activității. Informațiile sau imaginile postate online sau redirecționate în e-mailuri în masă pot ajunge la un public mai larg mai repede decât metodele mai tradiționale, provocând mai multe daune victimelor. O cantitate mare de informații personale este disponibilă online, astfel încât bătăușii ar putea să-și aleagă în mod arbitrar victimele.

Hărțuirea cibernetică poate indica, de asemenea, o tendință spre un comportament mai serios. Deși bullying-ul a fost întotdeauna o realitate nefericită, cei mai mulți bătăuși cresc din ea. Hărțuirea cibernetică nu a existat suficient de mult pentru a avea cercetări solide, dar există dovezi că ar putea fi un avertisment timpuriu pentru comportamentul violent.

Cum te poți proteja pe tine sau pe copiii tăi?

- Învață-ți copiii obiceiuri bune online. Explicați riscurile tehnologiei și învățați copiii cum să fie responsabili online. Reduceți-le riscul de a deveni agresori cibernetici prin stabilirea de linii directoare și monitorizarea utilizării lor a internetului și a altor mijloace electronice (telefoane mobile, tablete etc.).
- Păstrați liniile de comunicare deschise. Discutați în mod regulat cu copiii dvs. despre activitățile lor online, astfel încât să se simtă confortabil să vă spună dacă sunt victimizați.
- Urmăriți semnele de avertizare. Dacă observați modificări în comportamentul copilului dumneavoastră, încercați să identificați cauza cât mai curând posibil. Dacă este implicată hărțuirea cibernetică, acțiunea devreme poate limita daunele.

- Limitați disponibilitatea informațiilor personale. Limitarea numărului de persoane care au acces la informații de contact sau detalii despre interese, obiceiuri sau angajare reduce expunerea la bătăuși pe care dumneavoastră sau copilul dumneavoastră nu îi cunoașteți. Acest lucru poate limita riscul de a deveni victimă și poate facilita identificarea agresorului dacă tu sau copilul tău sunteți victimizat.
- Evitați escaladarea situației. Răspunsul cu ostilitate este probabil să provoace un agresor și să escaladeze situația. În funcție de circumstanțe, luați în considerare ignorarea problemei. Adesea, bătăușii se bucură de reacția victimelor lor. Alte opțiuni includ acțiuni subtile. De exemplu, este posibil să puteți bloca mesajele de pe site-urile de rețele sociale sau să opriți e-mailurile nedorite schimbând adresa de e-mail. Dacă continuați să primiți mesaje la noua adresă de e-mail, este posibil să aveți un caz mai puternic pentru acțiune în justiție.
- Documentați activitatea. Păstrați o evidență a oricărei activități online (e-mailuri, pagini web, mesaje instantanee etc.), inclusiv datele și orele relevante. Pe lângă arhivarea unei versiuni electronice, luați în considerare tipărirea unei copii.
- Raportați hărțuirea cibernetică autorităților competente. Dacă dumneavoastră sau copilul dumneavoastră sunteți hărțuiți sau amenințați, raportați activitatea. Multe școli au instituit programe anti-bullying, astfel încât oficialii școlii ar putea avea stabilite politici pentru a face față activităților care implică cursanții. Dacă este necesar, contactați autoritățile locale de aplicare a legii.

4.3.3 Activitati practice

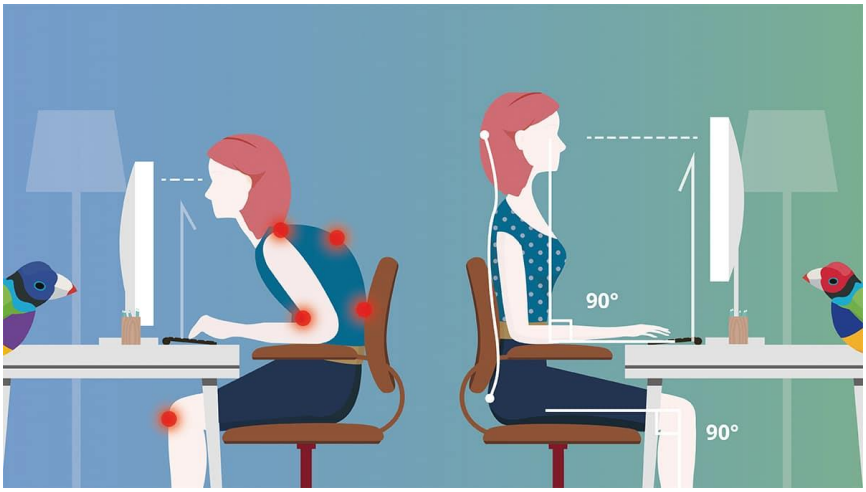
Pasul 1: Protecția ochilor

1. Pe computer, deschideți o aplicație de editare MS Office sau Notepad. Am folosit Notepad, un software inclus în sistemul de operare Windows.
2. Scrieți un text de câteva litere/cuvinte, cu dimensiunea standard de font definită, fără a fi schimbat.
3. Selectați cu mouse-ul, textul scris în Notepad și cu textul selectat, din bara de meniu de sus apăsați Format-> Font-> iar în zona numită Size selectează cea mai mare dimensiune disponibilă (în cazul meu 72). Observați, ochiul cât de ușoară poate citi textul scris, senzația de odihnă pe care o aveți când citiți un text cu un font de dimensiune mai mare.
4. Selectați din nou cu mouse-ul, textul scris în Notepad și cu textul selectat, din bara de meniu de sus apăsați Format-> Font-> iar în zona numită Size selectați cea mai mică dimensiune disponibilă pentru font (în cazul meu 8). Observați, ochiul cât de greu poate citi textul scris, senzația de a forța ochiul, pe care o simți când citești un text cu un font de dimensiune foarte mică.
5. Daca vrei, sa observi acele 2 diferente, poti face acest exercitiu de cateva ori.
6. Acum, vă rugăm să priviți acest exercițiu din următoarea perspectivă: Să presupunem că petreceți 5 ore pe zi în fața computerului. Fie că ai de lucru, fie că te uiți la un film sau te uiți la fotografii, în orice moment ochiul va încerca să se adapteze cât mai mult și cât mai bine să citească cât mai multe informații din imaginile afișate pe monitor, chiar dacă acea informație este mai ușor sau mai greu de văzut. Acest mod de a forța ochiul poate duce la probleme de vedere în timp.

7. Din acest motiv, există diferite moduri de a vă prelungi sănătatea ochilor. Google cunoaște această problemă și în extensiile din Google Chrome poate fi adăugată o extensie numită sugestiv „eyeCare – Protejează-ți vederea”. Se poate căuta în motorul de căutare google după cuvinte cheie precum „Eye Care Chrome” iar din rezultatele afișate accesați linkulhttps://chrome.google.com/webstore/detail/eyecare-protect-your-visi/eeeningnfkaonkonalpcicgemnnijjhn
8. În pagină, lângă eyeCare - Protejați-vă extensia de vedere, faceți clic pe butonul „Adăugați în Chrome”.
9. În fereastra nou deschisă, faceți clic pe butonul Adăugați extensie
10. Această extensie este un rest pentru regula 20-20-20 (la fiecare 20 de minute, luați ochii de la computer și priviți ceva la 20 de metri distanță timp de cel puțin 20 de secunde)
11. În acest fel, ochiul este setat să privească la o distanță diferită de monitor (20 de picioare distanță), contribuind astfel la sănătatea ochilor.

Pasul 2: Protejarea sănătății fizice (poziția de lucru pe computer)

1. Primul pas în acest exercițiu este să fii conștient de poziția pe care o ai în fața computerului (nu schimba această poziție, nu te întinde spatele. Stai exact în aceeași poziție în care te afli, pentru următorul punct).
2. Privește imaginea de mai jos și spune în ce poziție te afli: poziția stângă (cu coloana vertebrală într-o poziție curbată) sau poziția dreaptă (cu coloana vertebrală dreaptă)?



3. Astfel, daca te afli in pozitia din imaginea din dreapta: FELICITARI! Dar dacă vă aflați în poziția din imaginea din partea stângă, o poziție în care se află de obicei majoritatea oamenilor, atunci trebuie să înțelegeți următoarele aspecte:
4. După o perioadă mai lungă petrecută în fața echipamentelor electronice, involuntar, fără să-și dea seama, corpul tinde să se relaxeze și din poziția corectă de lucru se poate ajunge în poziția din stânga

imaginii, ceea ce duce în timp la probleme de sănătate la nivelul coloanei vertebrale, în special la oamenii care petrec multe ore pe zi și multe zile pe săptămână la computer

5. Din acest motiv trebuie să fim conștienți de poziția noastră atunci când lucrăm la computer și să ne corectăm! Acest mic efort ne poate menține coloana vertebrală sănătoasă în timp.
6. Cum e spatele acum? Ți-ai îndreptat coloana vertebrală?

4.4 Protejand mediul inconjurator

Unitatea 4.4	Protejand mediul inconjurator
Durată	5 ore
Obiective	Pentru a putea selecta medii sigure, eficiente și rentabile Pentru a înțelege impactul media digitală Pentru a ști cum să aruncați dispozitivele electronice în siguranță
Conţinut	4.4.1 Eliminarea corespunzătoare a dispozitivelor electronice 4.4.2 Activități practice
Resurse	Manual de instruire, calculatoare cu acces la internet
Metodologii de instruire	Prezentare de către trainer Exercițiu de grup Discuție / Dezbatere

Masa 25- Structura unităţii de competenţă 4.4. – Protejarea mediului în modulul 4 – Securitate.

4.4.1 Eliminarea corespunzătoare a dispozitivelor electronice

De ce este important să aruncați dispozitivele electronice în siguranță?

Pe lângă securizarea eficientă a informațiilor sensibile de pe dispozitivele electronice, este important să urmați cele mai bune practici pentru eliminarea dispozitivelor electronice. Calculatoarele, smartphone-urile și camerele vă permit să păstrați o mulțime de informații la îndemână, dar atunci când aruncați, donați sau reciclați un dispozitiv, este posibil să dezvăluiți din neatenție informații sensibile, care ar putea fi exploatate de criminalii cibernetici.

Tipurile de dispozitive electronice includ:

- Calculatoare, smartphone-uri și tablete — dispozitive electronice care pot stoca și procesa automat date; majoritatea conțin o unitate centrală de procesare și memorie și folosesc un sistem de operare care rulează programe și aplicații;
- Media digitale - aceste dispozitive electronice creează, stochează și redă conținut digital. Dispozitivele media digitale includ articole precum camere digitale și playere media;
- Hardware extern și dispozitive periferice — dispozitive hardware care oferă intrare și ieșire pentru computere, cum ar fi imprimante, monitoare și hard disk-uri externe; aceste dispozitive conțin caractere digitale stocate permanent; și
- Console de jocuri — dispozitive electronice, digitale sau computerizate care scot un semnal video sau o imagine vizuală pentru a afișa un joc video.

Care sunt câteva metode eficiente pentru eliminarea datelor de pe dispozitiv?

Există o varietate de metode pentru ștergerea definitivă a datelor de pe dispozitivele dvs. (numite și dezinfectare). Deoarece metodele de igienizare variază în funcție de dispozitiv, este important să utilizați metoda care se aplică dispozitivului respectiv.

Înainte de a igieniza un dispozitiv, luați în considerare să faceți o copie de rezervă a datelor. Salvarea datelor pe un alt dispozitiv sau pe o a doua locație (de exemplu, un hard disk extern sau cloud) vă poate ajuta să vă recuperați datele dacă ștergeți din greșeală informații pe care nu ați intenționat să le faceți sau dacă dispozitivul este furat (acest lucru vă poate ajuta și să identificați exact ce informații ar fi putut accesa un hoț). Opțiunile pentru stocarea digitală includ servicii de date în cloud, CD-uri, DVD-uri și unități flash amovibile sau hard disk-uri amovibile.

Metodele de igienizare includ:

- Ștergerea datelor. Eliminarea datelor de pe dispozitiv poate fi o metodă de igienizare. Când ștergeți fișiere de pe un dispozitiv - deși fișierele pot părea a fi fost eliminate - datele rămân pe suportul media chiar și după ce este executată o comandă de ștergere sau formatare. Nu vă bazați exclusiv pe metoda de ștergere pe care o utilizați în mod obișnuit, cum ar fi mutarea unui fișier în coșul de gunoi sau coșul de gunoi sau selectarea „Ștergeți" din meniu. Chiar dacă goliți coșul de gunoi, fișierele șterse sunt încă pe dispozitiv și pot fi recuperate. Ștergerea definitivă a datelor necesită mai mulți pași.
- Calculatoare. Utilizați un software de curățare a discurilor conceput pentru a elimina definitiv datele stocate pe hard diskul unui computer pentru a preveni posibilitatea de recuperare.
- Ștergere sigură. Acesta este un set de comenzi din firmware-ul majorității hard disk-urilor computerelor. Dacă selectați un program care rulează setul de comenzi de ștergere securizată, acesta va șterge datele prin suprascrierea tuturor zonelor de pe hard disk.
- Ștergerea discului. Acesta este un utilitar care șterge informațiile sensibile de pe hard disk și șterge în siguranță unitățile flash și cardurile digitale securizate.
- Smartphone-uri și tablete. Asigurați-vă că toate datele sunt eliminate de pe dispozitiv efectuând o „resetare completă". Acest lucru va readuce dispozitivul la setările originale din fabrică. Fiecare dispozitiv are o procedură diferită de resetare hard, dar majoritatea smartphone-urilor și tabletelor pot fi resetate prin setările lor. În plus, scoateți fizic cardul de memorie și cardul modulului de identitate a abonatului, dacă dispozitivul dvs. are unul.
- Camere digitale, playere media și console de jocuri. Efectuați o resetare standard din fabrică (adică o resetare hard) și scoateți fizic hard disk-ul sau cardul de memorie.
- Echipamente de birou (de exemplu, copiatoare, imprimante, faxuri, dispozitive multifuncționale). Scoateți orice card de memorie din echipament. Efectuați o resetare completă de fabricație pentru a restabili echipamentul la valorile implicite din fabrică.
- Suprascriere. O altă metodă de igienizare este să ștergeți informațiile sensibile și să scrieți noi date binare peste ele. Folosirea datelor aleatorii în loc de modele ușor de identificat face mai dificil pentru atacatori să descopere informațiile originale de dedesubt. Deoarece datele stocate pe un computer sunt scrise în cod binar - șiruri de 0 și 1 - o metodă de suprascriere este să umpleți cu zero un hard disk și să selectați programe care folosesc toate zerourile din ultimul strat. Utilizatorii ar trebui să suprascrie întregul hard disk și să adauge mai multe straturi de date noi (trei până la șapte treceri de date binare noi) pentru a preveni atacatorii să obțină datele originale.
- Cipher.exe este un instrument de linie de comandă încorporat în sistemele de operare Microsoft Windows care poate fi utilizat pentru a cripta sau decripta datele de pe unitățile New Technology File System. De asemenea, acest instrument șterge în siguranță datele prin suprascriere.
- Ștergerea este un nivel de igienizare media care nu permite preluarea informațiilor de către utilitarele de recuperare a datelor, discurilor sau fișierelor. Dispozitivele trebuie să fie rezistente la încercările de recuperare a apăsării tastelor de la dispozitive standard de intrare (de exemplu, o tastatură sau mouse) și de la instrumentele de colectare a datelor.
- Distrugând. Distrugerea fizică a unui dispozitiv este modalitatea supremă de a împiedica alte persoane să vă recupereze informațiile. Sunt disponibile servicii specializate care vă vor dezintegra, arde, topi sau

pulveriza unitatea computerului și alte dispozitive. Aceste metode de igienizare sunt concepute pentru a distruge complet mediile și sunt de obicei efectuate la o instalație de distrugere a metalelor externalizată sau de incinerare autorizată. Dacă alegeți să nu utilizați un serviciu, vă puteți distruge hard disk-ul batând cuie sau găurind singuri în dispozitiv. Piesele fizice rămase ale unității trebuie să fie suficient de mici (cel puțin 1/125 de inchi) încât informațiile dvs. să nu poată fi reconstruite din ele. Există și dispozitive hardware disponibile care șterg CD-urile și DVD-urile distrugându-le suprafața.

- Demagnetizatoare cu medii magnetice. Demagnetizările expun dispozitivele la câmpuri magnetice puternice care elimină datele care sunt stocate magnetic pe mediile magnetice tradiționale.
- Distrugerea în stare solidă. Distrugerea întregii memorie a cipurilor de stocare a datelor prin zdrobire, mărunțire sau dezintegrare se numește distrugere în stare solidă. Unitățile cu stare solidă ar trebui distruse cu dispozitive care sunt proiectate special pentru acest scop.
- Distrugere CD și DVD. Multe dispozitive de distrugere a hârtiei de birou și acasă pot distruge CD-uri și DVD-uri (asigurați-vă că verificați dacă tocatorul pe care îl utilizați poate distruge CD-uri și DVD-uri înainte de a încerca această metodă).

Cum puteți elimina în siguranță dispozitivele electronice învechite?

Deșeurile electronice (uneori numite deșeuri electronice) sunt un termen folosit pentru a descrie produsele electronice care se apropie de sfârșitul duratei de viață utilă și sunt aruncate, donate sau reciclate. Deși donarea și reciclarea dispozitivelor electronice conservă resursele naturale, puteți alege totuși să eliminați deșeurile electronice, contactând depozitul local de gunoi și solicitând o locație desemnată de predare a deșeurilor electronice. Rețineți că, deși există multe opțiuni pentru eliminare, este responsabilitatea dvs. să vă asigurați că locația aleasă este reputată și certificată.

4.4.2 Activitati practice

Pasul 1: Consumul de energie electrică - Costurile de exploatare a echipamentelor

1. După cum știm cu toții, echipamentul electric poate funcționa numai dacă este alimentat de electricitate. Dar câtă energie se consumă pentru un computer? Pentru răspuns, să trecem prin calculul descris mai jos.

2. Luați în considerare două unități de computer: un laptop (de exemplu cel pe care îl folosesc) și un computer (o unitate centrală), cu caracteristici tehnice aproximativ aceleași cu laptopul

3. Laptop: am citit valoarea sursei de alimentare pentru laptop si observ ca este de 130W (watt)

4. Să facem împreună următorul calcul: laptop folosit 7 zile pe săptămână (5 zile la serviciu și 2 zile în weekend pentru filme, muzică, fotografii etc.), aproximativ 8 ore/zi (h/zi) în medie

5. Să estimăm durata medie de viață a laptopului la aproximativ 5 până la 7 ani

6. Să calculăm consumul de energie pentru acest laptop, după cum urmează:

For 1 year of use	For 7 years of use
• 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)	• Power consumed for 1 year x 7 years = 379.600 kWh/year x 7 year= 2.657.200 Wh = 2.657,2 kWh

Figura 12 – Date pentru calculul consumului de energie.

7. Calcul computer (unitate centrală): Am făcut o cercetare pe internet pentru cele mai bune surse de alimentare pentru un computer: https://www.digitaltrends.com/computing/best-pc-power-supply/ și am ales câteva exemple de surse de alimentare: „Corsair RM750" 750W, „FSP Dagger" 550W sau „Thermaltake Toughpower Grand RGB" 650W

8. Dacă luăm în considerare pentru calcul sursa „FSP Dagger" valoarea puterii este de 550W (este cea mai mică putere dintre exemple). Pentru sursa de 550W aplicăm același calcul din figura 12, doar că înlocuim 130 kWh cu 550 kWh și obținem 11242 kWh.

9. Diferența (Economie) de energie între laptop și computer este de aproximativ 11.242 - 2.657,2 = 8.584,8 kWh

10. Să ne gândim la următoarele 2 aspecte: din punct de vedere personal dacă îți cumperi un laptop vei avea o economie de energie electrică după 7 ani de utilizare de 8584,8 kWh! Dacă înmulțiți această valoare cu prețul unui kWh, ce economii de bani obțineți după 7 ani de utilizare?

11. Din punct de vedere globalPentru obținerea energiei electrice se folosesc diverse surse, cum ar fi energia eoliană, energia calorică, energia hidroelectrică etc. Dacă pentru un singur computer obțineți o astfel de economie de energie, atunci calculată, să presupunem pentru 1000 de computere de aceeași putere electrică, câte resurse naturale sunt salvati? Dar pentru 1.000.000 de computere? Deci, în viitor, când veți cumpăra un computer, vă puteți gândi și la aspectul protecției mediului.

12. Și acum, la sfârșit, un mic exercițiu pentru tine. Dacă ar fi trebuit să alegem cea mai puternică sursă dintre cele exemplificate de 750W, câtă energie ar fi fost consumată în 7 ani pe lângă laptop? Poti sa faci acest calcul?

Pasul 2: Reciclarea electronicelor

Creați ipotetic un scenariu în care, noaptea, mergeți cu o lanternă. La un moment dat, se presupune că este nevoie să înlocuiți bateria din lanternă cu una nouă încărcată. Dacă acea baterie este aruncată accidental undeva în natură, bateria nu se va dizolva ca substanțele biodegradabile, va exista acolo unde a fost aruncată mult timp. În plus, substanțele acide și toxice din baterie se pot scurge și contamina zona în care a fost aruncată, pot pătrunde în apele subterane și pot contamina apa etc. Dacă ne gândim global, și nu doar la această baterie, există mii de tone de deșeuri electrice care dacă nu este reciclat, poate contamina mediul. Din acest motiv, este necesară reciclarea deșeurilor electrice, și există legislație legată de acest aspect.

Cum poți ajuta?

Dacă aveți echipamente electrice pe care urmează să le aruncați (Ex: un computer vechi și ruginit sau baterii descărcate), aruncați aceste deșeuri în centrele de colectare pentru reciclare! In acest fel puteti proteja mediul!

SAU: daca nu vrei sa arunci acele echipamente vechi si vrei sa ai un mic venit din ele (sa presupunem un calculator vechi) si intentionezi sa cumperi unul nou exista programe guvernamentale (in Romania, de exemplu, este Programul Scrap pentru electrocasnice) pentru a stimula reînnoirea echipamentelor cu altele mai economice și în același timp cele vechi sunt reciclate.

SAU: sunt comercianti, care in schimbul echipamentului vechi ofera reducere la achizitionarea unui alt utilaj nou din acelasi domeniu. Sunt oferte de tip BUY-BACK care au același efect pentru reciclarea echipamentelor electronice și sunt mai eficiente energetic.

Și în sfârșit, un mic exercițiu pentru tine: ai un computer vechi pe care ai vrea să-l schimbi (nu acum, în viitor)? Daca da, incearca sa gasesti pe internet ce comercianti iti pot oferi solutii de BUY-BACK?

Felicitări, acum ați finalizat Modulul 4.

Nu uitați să verificați Anexele pentru resurse și documente suplimentare furnizate pentru a sprijini auto-studiul!

Modulul 5: Rezolvarea problemelor

Modulul „Rezolvarea problemelor” este destinat celor interesați să identifice și să rezolve cele mai comune probleme hardware și software, precum și o modalitate sigură de selectare și achiziție a instrumentelor necesare pentru rezolvarea problemelor de zi cu zi folosind mijloace digitale.

Vă rugăm să rețineți că activitățile practice descrise în fiecare unitate pot presupune sprijinul unui formator cu experiență. Deși informațiile prezentate în manual sunt scrise într-un mod ușor de înțeles, unele acțiuni, adiacente informațiilor prezentate, pot necesita sprijinul unor oameni cu experiență.

Modulul 5	**Rezolvarea problemelor**			
Durată	**25h**			
Obiective	A fi capabil să rezolve probleme tehnice TIC comune și simple. A fi capabil să caute, să găsească și să aleagă soluția potrivită pentru o anumită problemă TIC. Fiind capabil să se dezvolte și să rămână în contact cu dezvoltarea TIC.			
Unități	5.1 Rezolvarea problemelor tehnice	5.2 Identificarea nevoilor și a răspunsurilor tehnologice	5.3 Utilizarea creativă a tehnologiilor digitale	5.4 Identificarea lacunelor de competență digitală
Organizarea instruirii	Față în față E-Learning	Față în față E-Learning	Față în față E-Learning	Față în față E-Learning
Durată	7h	7h	6h	5h

Masa 26 - Structura globală a Modulului 5 – Rezolvarea problemelor.

5.1 Rezolvarea problemelor tehnice

Unitatea 5.1	Rezolvarea problemelor tehnice
Durată	7h
Obiective	Pentru a putea rezolva problemele legate de viteza Internetului
Conţinut	5.1.1 Calculatoare și sistemele sale 5.1.2 Cele mai frecvente probleme tehnice 5.1.3 Activități practice
Resurse	Manual de instruire Computer cu conexiune la internet Modem
Metodologii de instruire	Prezentare de către trainer

Masa 27- Structura unităţii de competenţă 5.1. – Rezolvarea problemelor tehnice ale Modulului 5 – Rezolvarea problemelor.

5.1.1 Calculatoarele și sistemele sale

Modulul „Rezolvarea problemelor” este destinat celor interesați să identifice și să rezolve cele mai comune probleme hardware și software, precum și o modalitate sigură de selectare și achiziție a instrumentelor necesare pentru rezolvarea problemelor de zi cu zi folosind mijloace digitale.

Ce e un calculator?

Un computer este un dispozitiv electronic care manipulează informații sau date. Are capacitatea de a stoca, prelua și procesa date. Poate știți deja că puteți folosi un computer pentru a introduce documente, a trimite e-mailuri, a juca jocuri și a naviga pe Web. De asemenea, îl puteți folosi pentru a edita sau crea foi de calcul, prezentări și chiar videoclipuri.

Care sunt diferitele tipuri de computere?

Când majoritatea oamenilor aud cuvântul computer, se gândesc la un computer personal, cum ar fi un desktop sau un laptop. Cu toate acestea, computerele au multe forme și dimensiuni și îndeplinesc multe funcții diferite în viața noastră de zi cu zi

Multe dintre electronicele de astăzi sunt în principiu computere specializate, deși nu le gândim întotdeauna așa. Iată câteva exemple comune:

Tablete sau tablete— sunt computere portabile care sunt chiar mai portabile decât laptopurile. În loc de tastatură și mouse, tabletele folosesc un ecran sensibil la atingere pentru tastare și navigare. iPad-ul este un exemplu de tabletă.

Smartphone-uri – Multe telefoane mobile pot face o mulțime de lucruri pe care le pot face computerele, inclusiv navigarea pe internet și jocurile. Ele sunt adesea numite smartphone-uri și pentru mulți oameni, un smartphone poate înlocui de fapt componentele electronice precum un laptop vechi, un player de muzică digitală și o cameră digitală în același dispozitiv.

Hardware vs. software

Înainte de a vorbi despre diferite tipuri de computere, să vorbim despre două lucruri pe care toate computerele le au în comun: hardware și software.

- **Hardware**este orice parte a computerului dvs. care are o structură fizică, cum ar fi tastatura sau mouse-ul. De asemenea, include toate părțile interne ale computerului
- **Software**este orice set de instrucțiuni care spune hardware-ului ce trebuie să facă și cum să o facă. Exemple de software includ browsere web, jocuri și procesoare de text

Ce este un sistem de operare (OS)?

Un sistem de operare este cel mai important software care rulează pe un computer. Gestionează memoria și procesele computerului, precum și tot software-ul și hardware-ul acestuia. De asemenea, vă permite să comunicați cu computerul fără să știți să vorbiți limba computerului. Fără un sistem de operare, un computer este inutil. (Ex. sisteme de operare: Windows, Linux, macOs sunt folosite pentru desktop-uri și laptop-uri; Google Android și Apple IOS sunt folosite pentru tablete și smartphone-uri)

Ce este o aplicație?

Poate că ați auzit oameni vorbind despre utilizarea unui program, a unei aplicații sau a unei aplicații, dar ce înseamnă exact asta? Mai simplu spus, o aplicație este un tip de software care vă permite să efectuați anumite sarcini. Aplicațiile pentru computere desktop sau laptop sunt uneori numite aplicații desktop, în timp ce cele pentru dispozitive mobile sunt numite aplicații mobile.

Dacă utilizați în mod regulat computere în viața de zi cu zi, în cele din urmă veți întâlni unele probleme tehnice care necesită atenția dvs. Deși cele mai complexe probleme de calculator pot fi adesea rezolvate de un tehnician specializat, există multe alte probleme mici, dar comune, care apar în mod regulat pe un computer și utilizarea acestuia în mediul digital. Vestea bună este că multe probleme cu computerele au soluții simple, iar învățarea să recunoașteți o problemă și să o remediați singur vă va economisi mult timp și bani.

5.1.2 Cele mai frecvente probleme tehnice

1. Computerul nu pornește

Un computer care se oprește brusc sau are dificultăți la pornire ar putea avea o sursă de alimentare defectă. Verificați dacă computerul este conectat corect la priza de alimentare și, dacă acest lucru nu funcționează, testați priza de alimentare cu un alt dispozitiv care funcționează pentru a confirma dacă există sau nu energie adecvată.

2. Ecranul este gol

Dacă computerul este pornit, dar ecranul este gol, este posibil să existe o problemă cu conexiunea dintre computer și ecran. Mai întâi, verificați dacă monitorul este conectat la o priză de alimentare și dacă conexiunea dintre monitor și hard diskul computerului este sigură. Dacă problema este pe un laptop, atunci poate fi necesar să apelați la un profesionist pentru a o remedia, deoarece unele dintre firele interne pot fi uzate.

3. Sistem de operare sau software care funcționează anormal

Dacă sistemul de operare sau alt software nu răspunde sau funcționează, atunci încercați să reporniți computerul și executați o scanare antivirus. Pentru a evita acest lucru, instalați un software antivirus de încredere.

4. Windows nu va porni

Dacă întâmpinați probleme la pornirea Windows, atunci poate fi necesar să-l reinstalați cu discul de recuperare Windows.

5. Ecranul este înghețat

Când computerul se îngheață, este posibil să nu aveți altă opțiune decât să reporniți și să riscați să pierdeți orice lucrare nesalvată. Înghețarile pot fi un semn de memorie RAM insuficientă, conflicte de registry, fișiere corupte sau lipsă sau spyware. Apăsați și mențineți apăsat butonul de pornire până când computerul se oprește, apoi reporniți-l și treceți la treabă cu curățarea sistemului, astfel încât să nu înghețe din nou.

6. Computerul este lent

Dacă computerul este mai lent decât în mod normal, puteți rezolva adesea problema pur și simplu curățând hard diskul de fișiere nedorite. De asemenea, puteți instala un firewall, instrumente antivirus și anti-spyware și puteți programa scanări regulate ale registrului. Hard disk-urile externe sunt soluții excelente de stocare pentru procesoarele suprasolicitate și vă vor ajuta computerul să funcționeze mai rapid.

7. Zgomote ciudate

Mult zgomot provenit de la computer este, în general, un semn al unei defecțiuni hardware sau al unui ventilator zgomotos. Hard disk-urile fac adesea zgomot chiar înainte de a se defecta, așa că poate doriți să faceți o copie de rezervă a informațiilor pentru orice eventualitate, iar ventilatoarele sunt foarte ușor de înlocuit.

8. Viteza de net mica

Pentru a îmbunătăți performanța browserului dvs. de Internet, trebuie să ștergeți frecvent cookie-urile și fișierele temporare de Internet. În bara de căutare Windows, tastați „%temp%” și apăsați Enter pentru a deschide folderul cu fișiere temporare.

9. Supraîncălzire PC

Dacă carcasei computerului nu dispune de un sistem de răcire suficient, atunci componentele computerului pot începe să genereze căldură în exces în timpul funcționării. Pentru a evita arderea computerului, opriți-l și lăsați-l să se odihnească dacă se încălzește. În plus, puteți verifica ventilatorul pentru a vă asigura că funcționează corect.

10. S-au scăpat conexiunile la internet

Întreruperea conexiunilor la internet poate fi foarte frustrantă. Adesea, problema este simplă și poate fi cauzată de un cablu sau o linie telefonică defectuoasă, care este ușor de remediat. Problemele mai grave includ viruși, o placă de rețea sau un modem prost sau o problemă cu driverul.

11. Smartphone-ul tău funcționează încet

Aceasta este cea mai frecventă problemă a smartphone-ului, mai ales pe măsură ce telefonul tău îmbătrânește. Motivul din spatele vitezei reduse este instalarea de aplicații inutile care folosesc RAM-ul dispozitivului și salvează numeroase fișiere în telefon.

Ștergeți toate aplicațiile și fișierele inutile de pe mobil, curățați datele din cache. Puteți face acest lucru și prin aplicația de diagnosticare. Dacă totuși, vă confruntați cu această problemă, restaurați-o la datele din fabrică.

12. Durată slabă a bateriei

Din păcate, această problemă de telefon se întâmplă tuturor. Problemele comune sunt descărcarea bateriei, încărcarea lentă sau eșecul încărcării. Suntem lipiți de telefonul nostru, așa că problema de descărcare a bateriei este problema comună. Această problemă majoră este atunci când telefonul se descarcă fără a fi utilizat.

Aflați că, dacă anumite aplicații consumă prea multă baterie, puteți verifica acest lucru în Setări->Baterie și, dacă identificați vreo eroare, eliminați acele aplicații. Activați modul de economisire a bateriei, opriți locațiile, reduceți luminozitatea.

13. Spatiu de depozitare

Cea mai mare parte a stocării smartphone-ului este plină de fotografii și videoclipuri. Ar trebui să aveți grijă de stocare atunci când cumpărați un nou smartphone pentru că, după câteva zile, începeți să vă panicați pentru spațiul de stocare redus. Foarte puține smartphone-uri au o funcție de memorie extensibilă în zilele noastre.

Ștergeți mai întâi memoria cache. Utilizați aplicații precum cache cleaner, care vă permite să curățați memoria cache pentru o anumită aplicație. Dezinstalați aplicații sau mutați aplicațiile de pe telefon. Transferați imaginile pe nori pentru a elibera spațiu pe dispozitiv.

14. Blocarea telefonului sau a aplicației

Acest lucru se întâmplă atunci când există o eroare în aplicațiile instalate sau când telefonul tău rămâne fără spațiu. Aceasta este una dintre problemele frustrante ale telefonului mobil.

Ștergeți datele aplicației din „Manager de aplicații". Evitați utilizarea mai multor aplicații în același timp. Depanați-vă telefonul repornind dispozitivul, scoateți bateria sau restabiliți-l la setările din fabrică.

15. Supraîncălzirea smartphone-ului

Utilizarea în exces a smartphone-ului aduce probleme de supraîncălzire. Aplicațiile solicitante, mai probabil cele de jocuri fac ca temperatura telefonului să fie ridicată, ceea ce poate afecta performanța bateriei. Poate ați descărcat aplicații rău intenționate care rulează în fundal.

Încercați să nu vă folosiți telefonul în timpul încărcării. Nu utilizați aplicații care consumă un procesor ridicat și acordați o pauză telefonului. Dacă încă, telefonul tău se încălzește, acesta este defectul producătorului.

16. Problemă de conectare cu Bluetooth, wifi, rețea celulară

Aceasta este problema temporară a telefonului mobil care poate fi rezolvată cu ușurință. Țineți telefonul în modul avion timp de 30 până la 60 de secunde și încercați să-l reconectați. Mai ai o problemă? Reparați sau modificați din nou setările Bluetooth și WiFi.

17. Aplicațiile nu se descarcă

Cauza principală a acestei probleme este memoria cache coruptă. Accesați aplicația Google Play Store și ștergeți memoria cache a aplicației. Mai bine ștergeți istoricul magazinului Google Play. Asigurați-vă că utilizați cea mai recentă versiune a magazinului Google Play. Dacă există în continuare o problemă, ștergeți datele și memoria cache pe serviciile Google Play.

18. Problemă de sincronizare

Problema de sincronizare se rezolvă automat după ceva timp. Dacă nu, eliminați contul Google și adăugați-l din nou. Asigurați-vă că conexiunea dvs. la internet nu este limitată și funcționează corect. Verificați actualizarea sistemului și actualizați-o dacă este necesar.

19. Cardul MicroSD nu funcționează pe smartphone

Poate fi cauzat atunci când cardul SD are erori de citire/scriere greșite. Telefonul mobil nu recunoaște cardul SD după formatare. Verificați capacitatea cardului de memorie și formatați-l în exFAT dacă este de până la 32 GB. Reporniți telefonul în modul de recuperare și selectați ștergeți memoria cache în Android. Acest lucru va șterge cardul SD și îl va formata în FAT32, care este cel mai potrivit pentru stocarea într-un telefon.

20. Ecran crăpat sau scufundare în apă

Această problemă a telefonului mobil se întâmplă din greșeală și nu putem face nimic în acest sens. Pentru a evita astfel de incidente, folosește protectorul bun pentru telefon. Da, pot fi scumpe, dar este o investiție demnă pentru a evita aceste accidente.

Un computer este un dispozitiv electronic care manipulează informații sau date. Are capacitatea de a stoca, prelua și procesa date. Poate știți deja că puteți folosi un computer pentru a introduce documente, a trimite e-mailuri, a juca jocuri și a naviga pe Web. De asemenea, îl puteți folosi pentru a edita sau crea foi de calcul, prezentări și chiar videoclipuri.

5.1.2 Activități practice

Pasul 1:Reporniți modemul și dispozitivele fără fir

Odată ce v-ați conectat modemul și ați configurat rețeaua de domiciliu, atât conexiunile dvs. de internet cu fir, cât și fără fir ar trebui să fie de încredere, în fiecare zi. Vitezele mici și deconectările pot rezulta din semnale slabe, echipamente sau cabluri vechi, interferențe, capacități/limitări ale dispozitivului și posibil probleme legate de terți. Dacă credeți că există o problemă cu WiFi-ul dvs., încercați soluțiile simple prezentate mai jos pentru a rezolva cele mai frecvente probleme.

O simplă repornire a modemului poate rezolva multe probleme de WiFi sau de conexiune

1. Deconectați cablul de alimentare din spatele modemului WiFi sau de la priza de perete.
2. Așteptați 30 de secunde.
3. Reconectați cablul de alimentare la modem.

În câteva minute, rețeaua dvs. WiFi ar trebui să reapară în lista rețelelor disponibile pe dispozitivele dvs. fără fir. Încercați să conectați un dispozitiv la WiFi pentru a vedea dacă funcționează.

Repornirea dispozitivelor wireless poate fi, de asemenea, soluția la multe probleme comune, inclusiv întârzierile sau pierderea accesului la internet. Consultați manualul dispozitivului pentru a afla cum să efectuați o repornire standard.

Pasul 2: Plasarea modemului și acoperirea

Locația modemului dvs. în casa dvs. joacă un rol important în acoperirea dvs. WiFi și este un factor cheie pentru o conexiune WiFi stabilă. Pentru o acoperire WiFi mai bună, modemul dvs. ar trebui să fie amplasat într-o locație centrală, acest lucru funcționează mai ales dacă aveți o casă deschisă. Alternativ, plasarea modemului în centrul locului unde este folosit cel mai des internetul este, de asemenea, o alegere bună. Asigurați-vă că plasați modemul

✓ In aer liber

✓ Ridicat de la sol

Evitați să plasați modemul

✕ În subsoluri

✕ În dulapuri

✕ În spatele altor obiecte

Pentru a evita interferențele, încercați să țineți modemul departe de

✕ Aparate de uz casnic

✕ Obiecte metalice

✕ Echipament electric

Pasul 3: Verificați conexiunile

Conexiunile slăbite, cablurile deteriorate și divizoarele de linie pot degrada semnalele Internet înainte ca acestea să ajungă chiar la modemul dvs. și vă pot împiedica să atingeți viteze mai mari de internet. Pentru a rezolva acest lucru, ar trebui să vă asigurați că cablurile sunt conectate corect.

1. Deconectați cablul de alimentare din spatele modemului.
2. Deșurubați cablul coaxial din spatele modemului.
3. Verificați cablul coaxial pentru îndoiri sau îndoituri care indică deteriorare.
4. Urmați cablul coaxial până la mufa de cablu de pe perete.
5. Determinați dacă cablul coaxial intră direct în mufă sau dacă trece prin alte dispozitive, cum ar fi un splitter.
6. Dacă este prezent un splitter, îndepărtați temporar splitter-ul, astfel încât linia coaxială să poată conecta mufa de cablu direct la modem.
7. Reconectați cablurile coaxiale și de alimentare la spatele modemului.
8. Așteptați ca modemul să revină online.

Dacă utilizați un cablu Ethernet pentru a vă conecta computerul la router sau modemul la un router terță parte, verificați și acele cabluri și înlocuiți-le dacă par deteriorate.

Pasul 4: Restabiliți setările modemului

În unele circumstanțe rare, ar putea ajuta să restabiliți modemul la setările din fabrică ca ultimă soluție, care va reseta toate setările personalizate pe care le-ați configurat, inclusiv numele și parola rețelei Wi-Fi la valorile implicite, care se găsesc pe autocolantul de pe modemul dvs.

Pentru a vă restabili modemul:

1. Găsiți butonul mic de resetare al modemului dvs.
2. Apăsați și mențineți apăsat butonul cu o agrafă sau un ac timp de 15 secunde.
3. Urmăriți luminile modemului clipind, apoi, după câteva momente, rămâneți aprinse.

În câteva minute, rețeaua dvs. Wi-Fi ar trebui să reapară în lista de rețele disponibile pe dispozitivele dvs. fără fir. Încercați să conectați un dispozitiv la Wi-Fi pentru a vedea dacă funcționează.

5.2 Identificarea nevoilor și a răspunsurilor tehnologice

Unitatea 5.2	Identificarea nevoilor și a răspunsurilor tehnologice
Durată	7h
Obiective	A fi capabil să rezolve probleme tehnice TIC comune și simple.
Conținut	5.2.1 Identificarea nevoilor și a răspunsurilor tehnologice 5.2.2 Activități practice
Resurse	Manual de instruire Calculatoare cu acces la internet
Metodologii de instruire	Prezentare de către trainer

Masa 28- Structura unității de competență 5.2. – Identificarea nevoilor și a răspunsurilor tehnologice ale Modulului 5 – Rezolvarea problemelor.

5.2.1 Identificarea nevoilor și a răspunsurilor tehnologice

Primul pas atunci când vine vorba de rezolvarea oricărei probleme de calcul este să aflați care componentă nu funcționează corect. Uneori se datorează faptului că ceva simplu, cum ar fi sunetul nu funcționează, sau nu putem vedea corect că ecranul sau tastatura/mouse-ul nu mai funcționează. Alteori computerul nici nu pornește, repornește sau se oprește brusc și nu știm ce se întâmplă. Pentru a identifica problema, trebuie să fim atenți la indiciile pe care ni le oferă computerul.

Există multe lucruri diferite care ar putea cauza o problemă cu computerul dvs. Indiferent de ce cauzează problema, depanarea va fi întotdeauna un proces de încercare și eroare, în unele cazuri, poate fi necesar să utilizați mai multe abordări diferite înainte de a găsi o soluție; alte probleme pot fi ușor de rezolvat. Vă recomandăm să începeți prin a utiliza următoarele sfaturi.

- **Notează-ți pașii**: După ce începeți depanarea, poate doriți să notați fiecare pas pe care îl faceți. Astfel, vei putea să-ți amintești exact ce ai făcut și poți evita să repeți aceleași greșeli. Dacă ajungi să ceri ajutor altor persoane, va fi mult mai ușor dacă ei știu exact ce ai încercat deja.
- **Luați notițe despre mesajele de eroare**: Dacă computerul vă dă un mesaj de eroare, asigurați-vă că notați cât mai multe informații posibil. Este posibil să puteți utiliza aceste informații mai târziu pentru a afla dacă alte persoane au aceeași eroare.
- **Verificați întotdeauna cablurile**: Dacă întâmpinați probleme cu o anumită piesă hardware a computerului, cum ar fi monitorul sau tastatura, un prim pas ușor este să verificați toate cablurile aferente pentru a vă asigura că sunt conectate corect.

- **Reporniți computerul**: Când toate celelalte nu reușesc, repornirea computerului este un lucru bun de încercat. Acest lucru poate rezolva o mulțime de probleme de bază pe care le puteți întâlni cu computerul dvs.

- **Utilizarea procesului de eliminare**: Dacă aveți o problemă cu computerul dvs., este posibil să puteți afla ce este greșit utilizând procesul de eliminare. Aceasta înseamnă că veți face o listă cu lucrurile care ar putea cauza problema și apoi le veți testa unul câte unul pentru a le elimina. Odată ce ați identificat sursa problemei computerului dvs., va fi mai ușor să găsiți o soluție.

Caută pe internet

Puteți găsi o soluție prin mii de tutoriale video pe YouTube sau din surse online care oferă instrucțiuni pas cu pas despre depanarea computerului.

Ce este un tutorial video?

Este un ghid video despre cum să rezolvi o anumită problemă.

Care este scopul tutorialului video?

Tutorialele video oferă o experiență multidimensională care poate combina diagrame, diapozitive, fotografii, grafică, narațiune, capturi de ecran, subtitrări pe ecran, muzică și videoclipuri live. Acest lucru permite elevilor cu diferite abilități de învățare să rețină informațiile într-o metodă mai potrivită pentru ei.

De exemplu, dacă doriți să instalați o imprimantă, puteți introduce pe un motor de căutare „tutorial de instalare a imprimantei”. Unul dintre rezultate este un videoclip numit: Configurați sau instalați o imprimantă pe Windows 10|Cum se facehttps://www.youtube.com/watch?v=E83yneh4xCA, faceți clic pe el și urmați pas cu pas informațiile despre instalarea imprimantei.

Surse online: Site-uri web care vă pot oferi cunoștințele adecvate în depanarea computerelor și asistență tehnică.

Exemplu: Bleeping Computer: http://www.bleepingcomputer.com

Site-ul este o sursă excelentă de informații, sfaturi și tutoriale despre software și hardware pentru computer, depanare și securitate, pentru a numi câteva. Are o bază de date de articole care poate fi căutată, care este actualizată lunar de către stabilul său de colaboratori obișnuiți.

Exemple de nevoi hardware:

- **camera web**: O cameră web este o cameră video care furnizează sau transmite în flux o imagine sau un videoclip în timp real către sau printr-o rețea de computere, cum ar fi Internetul. Camerele web sunt de obicei camere mici care stau pe un birou, se atașează la monitorul unui utilizator sau sunt încorporate în hardware.
- **Imprimanta**: o mașină pentru tipărirea textului sau a imaginilor, în special una legată de un computer.
- **Scanner**: un dispozitiv care scanează documente și le convertește în date digitale.
- **Microfon**: Un microfon (microfon pe scurt) este un dispozitiv electronic care convertește undele audio în semnale electronice, care este apoi preluat de computer ca intrare. În desktop-uri, este la fel ca orice alt dispozitiv periferic și este de obicei conectat separat.
- **Difuzoare audio**: Difuzoarele sunt traductoare care convertesc undele electromagnetice în unde sonore. Difuzoarele primesc intrare audio de la un dispozitiv, cum ar fi un computer sau un receptor audio. ... Sunetul produs de difuzoare este definit de frecvență și amplitudine. Frecvența determină cât de ridicat sau scăzut este înălțimea sunetului.
- **Cameră pentru smartphone**: Smartphone-urile care sunt telefoane cu cameră pot rula aplicații mobile pentru a adăuga capabilități, cum ar fi geoetichetarea și cusătura de imagini. ... Începând cu mijlocul anilor 2010, unele telefoane cu cameră avansată dispun de stabilizare optică a imaginii (OIS), senzori mai mari, lentile luminoase, video 4K și chiar zoom optic.
- **Porturi și conexiuni**: În hardware-ul computerului, un port servește ca interfață între computer și alte computere sau dispozitive periferice. În termeni informatici, un port se referă în general la partea unui dispozitiv de calcul disponibilă pentru conectarea la periferice, cum ar fi dispozitivele de intrare și ieșire.
- **Tehnologia wireless**: Tehnologia wireless oferă capacitatea de a comunica între două sau mai multe entități la distanțe fără a utiliza fire sau cabluri de orice fel. Unii dintre acești termeni vă pot fi familiari: transmisii radio și televiziune, comunicații radar, comunicații celulare, sisteme de poziție globală (GPS), Wi-Fi, Bluetooth și identificarea frecvenței radio sunt toate exemple de „wireless", cu utilizări extrem de diferite în unele cazuri.

Exemple de nevoi software:

- **Extensii de fișiere**: Extensiile de fișiere sunt o modalitate de a eticheta numele fișierelor, astfel încât dvs. și computerul dvs. să puteți urmări ceea ce conțin ele. ... Ultima parte a numelui fișierului este folosită pentru a indica tipul de fișier, astfel încât computerul să poată deschide programul corect atunci când doriți să utilizați fișierul.
  Windows folosește extensii de fișiere pentru a determina modul în care deschide diferite tipuri de fișiere. Când un utilizator face dublu clic pe un fișier pentru a-l deschide, Windows îl va deschide cu aplicația asociată cu extensia acelui fișier. Configurația sistemului Windows menține o listă de aplicații și extensiile de fișiere asociate acestora. Acestea se numesc „programe implicite". Dacă o anumită extensie de fișier este înregistrată cu un program, Windows va porni acel program ori de câte ori utilizatorul alege să deschidă un fișier cu acea extensie. Cu toate acestea, o singură aplicație poate fi înregistrată ca program implicit pentru fiecare extensie de fișier. Pentru a utiliza un alt program decât cel implicit pentru a deschide un fișier, faceți clic dreapta pe fișier și alegeți „Deschide cu".

- **Actualizați software-ul**: Actualizările de software sunt importante deoarece includ adesea patch-uri critice pentru găurile de securitate. ... De asemenea, pot îmbunătăți stabilitatea software-ului dvs. și pot elimina funcțiile învechite. Toate aceste actualizări au ca scop îmbunătățirea experienței utilizatorului
- **Instalare antivirus:** Software-ul antivirus vă ajută să vă protejați computerul împotriva programelor malware și a criminalilor cibernetici. Software-ul antivirus analizează datele — pagini web, fișiere, software, aplicații — care călătoresc prin rețea către dispozitivele dvs. ... Caută să blocheze sau să elimine programele malware cât mai repede posibil.
- **Setări de afișare**: Computerul are o serie de setări de afișare care vă permit să vă personalizați experiența de vizionare în funcție de activitatea dvs. Setările dvs. de afișare sunt ajustabile în funcție de ceea ce utilizați computerul și de tipul de monitor pe care îl aveți

5.2.2 Activități practice

Pasul 1: Reporniți telefonul

1. Pe majoritatea telefoanelor, apăsați butonul de pornire al telefonului timp de aproximativ 30 de secunde sau până când telefonul repornește
2. Pe ecran, poate fi necesar să atingeți Restart.

Pasul 2: Verificați actualizările Android

Important: setările pot varia în funcție de telefon.

1. Deschideți aplicația Setări a telefonului.
2. În partea de jos, atingeți Sistem > Avansat > Actualizare de sistem. Dacă este necesar, atingeți mai întâi Despre telefon sau Despre tabletă.
3. Va apărea starea actualizării dvs. Urmați pașii de pe ecran.

Pasul 3: Verificați spațiul de stocare și liber

Telefonul poate începe să aibă probleme atunci când mai puțin de 10% din spațiul de stocare este gratuit. Dacă rămâneți fără spațiu de stocare,mai jos puteți găsi informații despre cum să eliberați spațiu.

Ștergeți fotografii și videoclipuri

1. Pe telefonul sau tableta Android, deschideți aplicația Google Foto.
2. Conectați-vă la Contul dvs. Google.
3. Atingeți lung o fotografie sau un videoclip pe care doriți să îl mutați în coșul de gunoi. Puteți selecta mai multe articole.

4. În partea de sus, atinge Coș de gunoi.

Pe majoritatea telefoanelor, puteți verifica cât de mult spațiu de stocare aveți disponibil în aplicația Setări. Setările pot varia în funcție de telefon.

Goliți-vă gunoiul

Dacă vedeți o solicitare de „Ștergere definitivă” când încercați să mutați un articol în coșul de gunoi, coșul de gunoi este plin. Coșul de gunoi poate conține 1,5 GB.

Important: dacă goliți coșul de gunoi, ștergeți definitiv toate elementele din coșul de gunoi.

1. Pe telefonul sau tableta Android, deschideți aplicația Google Foto.
2. Conectați-vă la Contul dvs. Google.
3. În partea de jos, atingeți Bibliotecă > Gunoi > Mai mult > Goliți Coșul de gunoi > Șterge.

Eliminați filmele descărcate, muzică și alte conținuturi media

Pentru a șterge conținut de pe Google Play:

1. Deschideți aplicația Google Play cu conținut, cum ar fi Muzică Play sau Filme Play și TV.
2. Atingeți Meniu > Setări > Gestionați descărcările.
3. Atinge Descărcat > Elimina.

Pentru a șterge conținut din alte surse, ștergeți din aplicația pe care ați folosit-o pentru a-l descărca.

Pasul 4: Închideți aplicațiile care nu răspund

Android gestionează memoria pe care o folosesc aplicațiile. De obicei, nu trebuie să închideți aplicațiile, dar dacă o aplicație nu răspunde, încercați să închideți aplicația.

Pasul 5: Actualizați aplicația

1. Pe telefon, deschideți aplicația Magazin Google Play.
2. Atingeți Meniu > Aplicațiile și jocurile mele.
3. Aplicațiile cu actualizări disponibile sunt etichetate „Actualizare”.
   - Dacă este disponibilă o actualizare, atingeți Actualizare.
   - Dacă sunt disponibile mai multe actualizări, atingeți Actualizați toate.

Pasul 6: Dezinstalați aplicațiile pe care nu le utilizați

Atenție: orice date salvate în această aplicație vor fi șterse.

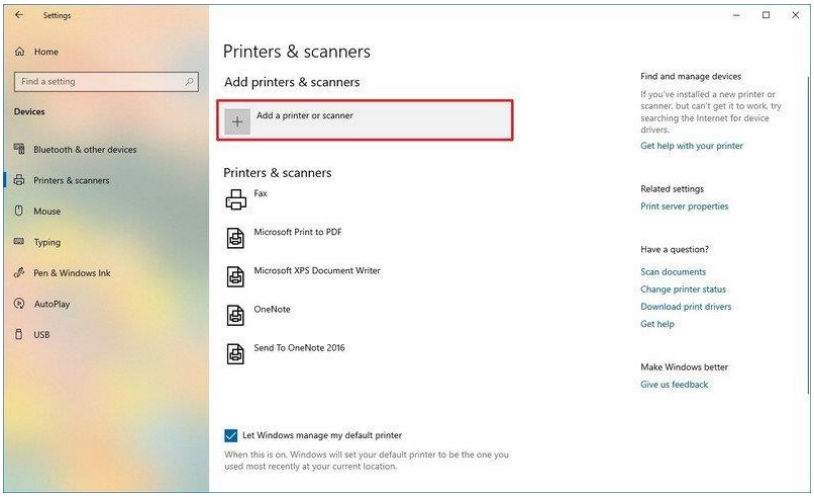
1. Atingeți și mențineți apăsată aplicația pe care doriți să o dezinstalați.
2. Pentru a vedea opțiunile, începeți să trageți aplicația.
3. Trageți aplicația la Dezinstalare în partea de sus a ecranului. Dacă nu vedeți „Dezinstalare”, nu puteți dezinstala aplicația.
4. Ridicați degetul.

Sfat: dacă doriți să utilizați din nou aplicația, puteți încerca să o reinstalați.

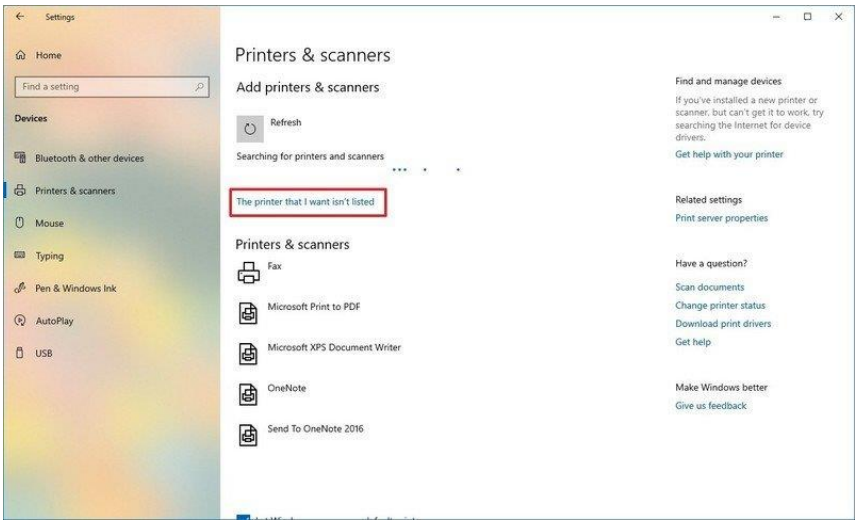
Instalarea manuală a unei imprimante locale

Când sistemul nu detectează automat imprimanta dvs., puteți adăuga dispozitivul manual, în funcție de tipul de conexiune și de vechimea imprimantei.
Important:Înainte de a continua, asigurați-vă că computerul este conectat la internet pentru a permite Windows Update să descarce drivere suplimentare.

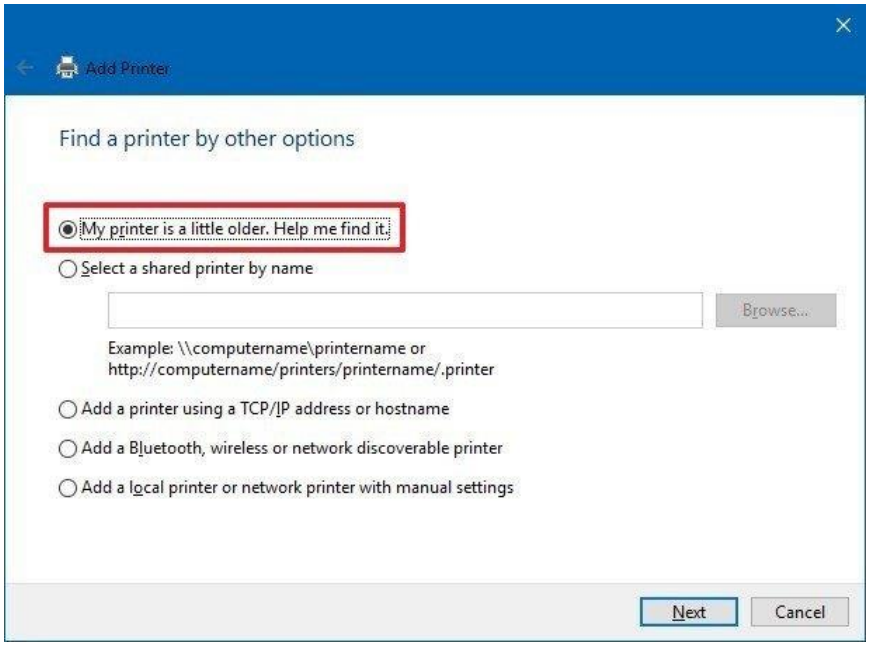
1. Deschide setările.
2. Faceți clic pe Dispozitive.
3. Faceți clic pe Imprimante și scanere.
4. Faceți clic pe butonul Adăugați o imprimantă sau un scanner.



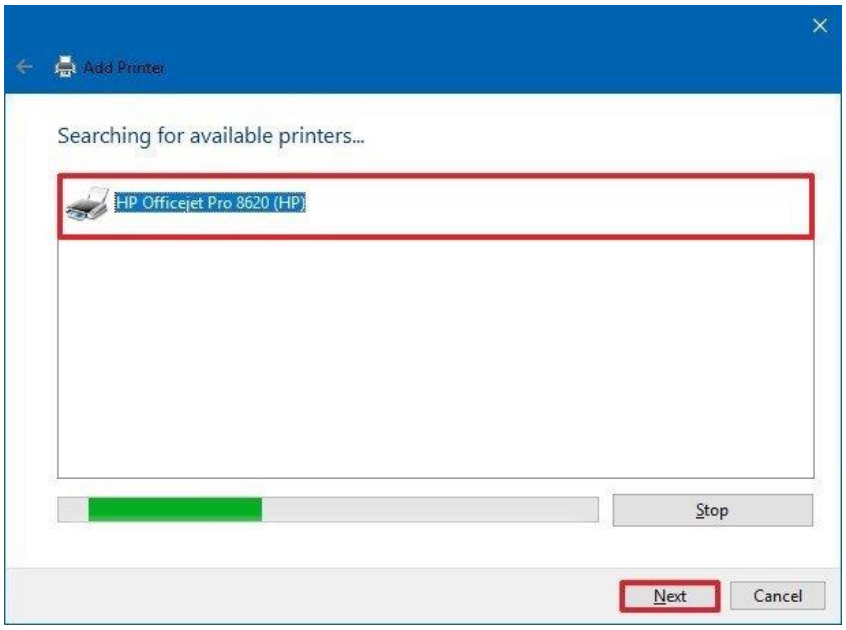
5. Așteptați câteva clipe.
6. Faceți clic pe opțiunea Imprimanta pe care o doresc nu este listată.



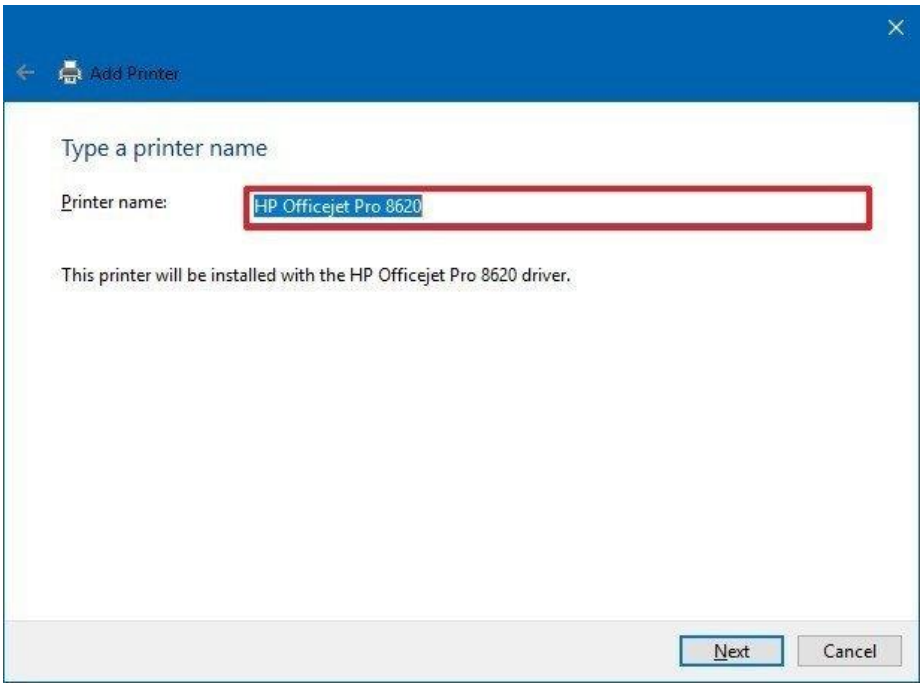
7. Selectați Imprimanta mea este puțin mai veche. Ajută-mă să găsesc opțiunea.



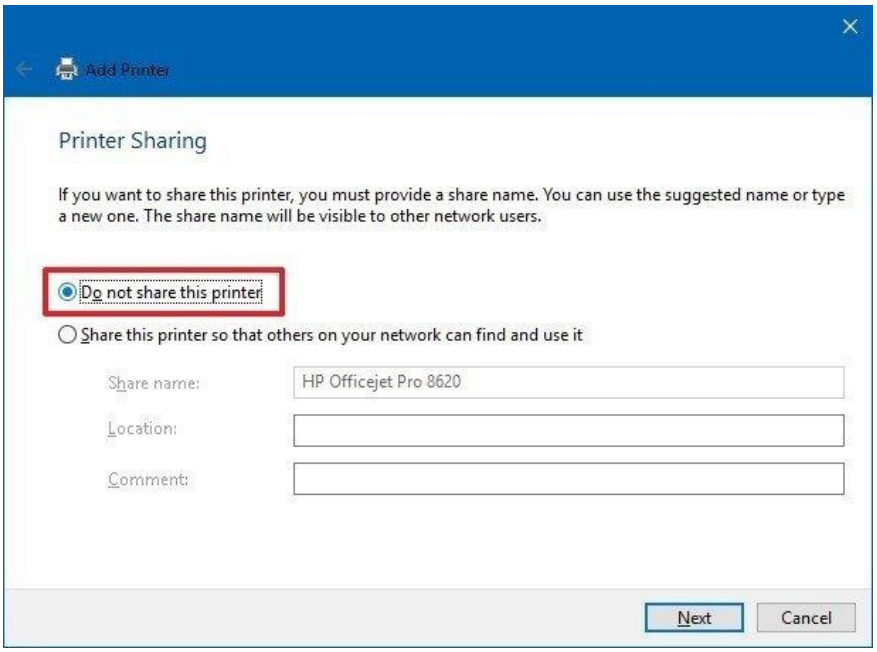
8. Selectați imprimanta dvs. din listă.
9. Faceți clic pe butonul Următorul.



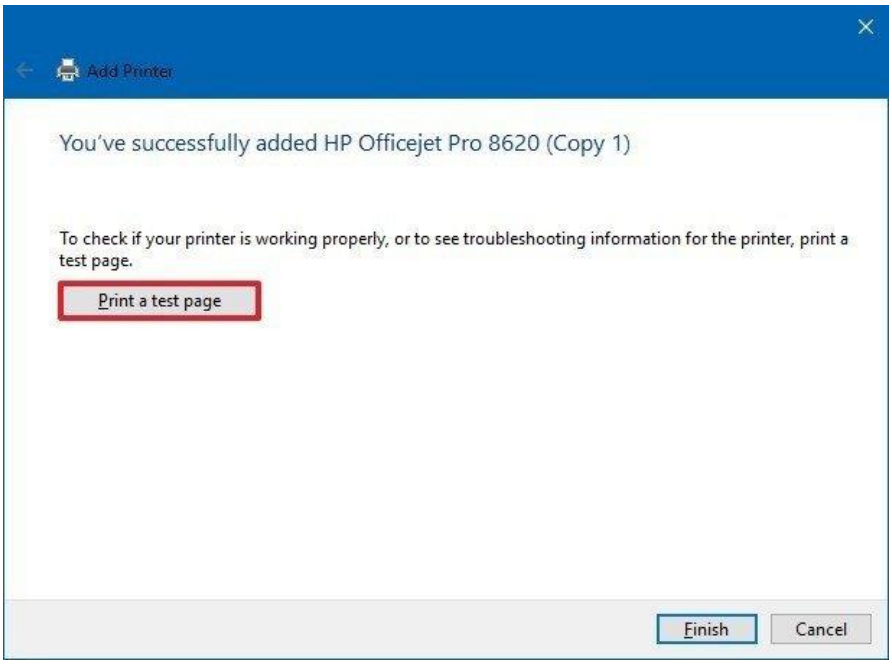
10. Introduceți un nume pentru imprimantă.
11. Faceți clic pe butonul Următorul.



12. Selectați opțiunea Nu partajați această imprimantă.
13. Faceți clic pe butonul Următorul.



14. Faceți clic pe opțiunea Print a test page pentru a confirma că dispozitivul funcționează.



15. Faceți clic pe butonul Terminare.

După ce ați finalizat pașii, ar trebui să puteți începe să imprimați pe dispozitiv.

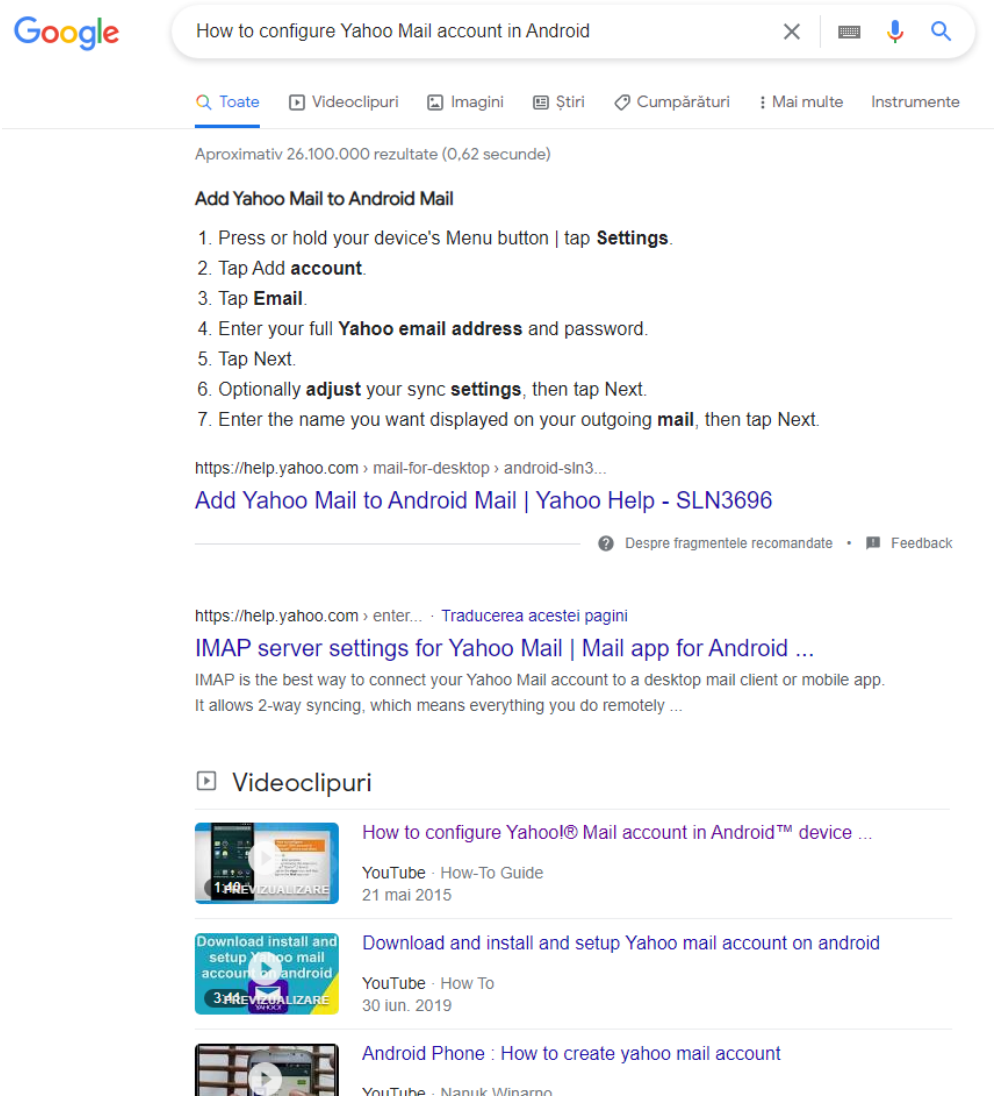
Cum să configurați contul Yahoo!® Mail în clientul de e-mail al dispozitivului Android™

Doriți să vă verificați e-mailurile contului Yahoo!® Mail pe dispozitivul Android™? Dacă doriți să configurați contul Yahoo!® Mail în clientul de e-mail al dispozitivului dvs. smartphone, puteți utiliza un tutorial video pentru a vă ajuta să rezolvați această situație.

1. Deschideți o pagină de browser și introduceți numele unui motor de căutare Ex. Google.

2. Pe bara motorului de căutare Google tastați „Cum se configurează contul Yahoo Mail în Android”.

3. Multe rezultate vor apărea pe ecran. Alegeți unul dintre rezultatele video ale criteriilor de căutare făcând dublu clic pe el. Ex. primul video :(https://www.youtube.com/watch?v=C0KxJ-T7rRw)



4. Urmăriți acest videoclip și urmați pașii pentru a face acest lucru.

Cereți audienței să dea un exemplu de nevoi și repetați căutarea tutorialelor în funcție de răspunsurile lor.

5.3 Folosind creativ tehnologiile digitale

Unitatea 5.3	Folosind creativ tehnologiile digitale
Durată	6h
Obiective	Înțelegeți și explorați tehnologiile digitale creative
Conţinut	5.3.1 Creativitate digitală 5.3.2 Activități practice
Resurse	Manual de instruire Calculatoare cu acces la internet
Metodologii de instruire	Prezentare de către trainer Exercițiu de grup Discuție / Dezbatere Lucrul în perechi/grupuri mici

Masa 29- Structura unității de competență 5.3. – Utilizarea creativă a tehnologiilor digitale din Modulul 5 – Rezolvarea problemelor.

5.3.1 Creativitate digitală

Creativitatea devine rapid una dintre cele mai apreciate trăsături ale secolului 21 și, conform unui raport din 2016 al Forumului Economic Mondial, este una dintre primele trei abilități pe care angajatorii le vor căuta până în 2020. Un sondaj realizat de IBM a mai constatat că că 60% dintre directori executivi cred că creativitatea este cea mai importantă calitate a conducerii în prezent.

Creativitatea digitală este un domeniu nou, dinamic, interdisciplinar și în creștere rapidă. Deși există o claritate din ce în ce mai mare cu privire la ceea ce este creativitatea, sensul digitalului se extinde în fiecare zi. În mod deloc surprinzător, creativitatea digitală poate însemna multe lucruri diferite în afaceri, al treilea sector, în educație și în învățarea informală.

Noul hardware/software le permite, fără îndoială, tinerilor să se implice cu lumea, adesea jucăuș și experimental, în moduri pe care nu le-ar fi putut face nici măcar acum zece ani. Cu siguranță, creativitatea digitală este uimitor de rapidă și, după toate probabilitățile, este mai mult decât suma digitală + creativitate.

Exemple de creativitate digitală:

- **Procesarea textului**. În informatică, termenul de procesare a textului se referă la teoria și practica automatizării creării sau manipulării textului electronic. ... Termenul de prelucrare se referă la prelucrarea automatizată (sau mecanizată), spre deosebire de aceeași manipulare făcută manual.
- **Editare media**. Editarea este procesul de selectare și pregătire a materialului scris, fotografic, vizual, sonor sau cinematografic utilizat de o persoană sau de o entitate pentru a transmite un mesaj sau o informație.
- **Proiectarea prezentărilor**. Ce este designul de prezentare? Designerii de prezentări creează o serie de idei, povești, cuvinte și imagini într-un set de diapozitive care sunt aranjate pentru a spune o poveste și a convinge publicul.
- **E-mail**. E-mailul este un sistem de trimitere electronică a mesajelor scrise de la un computer la altul. E-mailul este o abreviere a cuvântului „electronic mail”.
- **Social media**. Social media este o tehnologie bazată pe computer care facilitează schimbul de idei, gânduri și informații prin construirea de rețele și comunități virtuale. Prin design, rețelele sociale sunt bazate pe internet și oferă utilizatorilor o comunicare electronică rapidă a conținutului.
- **Vizualizarea datelor**. Vizualizarea dateloreste reprezentarea grafică a informațiilor și datelor. Prin utilizarea elementelor vizuale precum diagrame, grafice și hărți, instrumentele de vizualizare a datelor oferă o modalitate accesibilă de a vedea și înțelege tendințele, valorile aberante și modelele din date.

Instrumente de creativitate digitală

- **Calendare:** Un calendar digital vă permite să mergeți atât de departe cât aveți nevoie, să vedeți evenimentele recurente pe care le veți avea și să programați ceva pentru 2031 ca și cum ar fi săptămâna viitoare. Îl ai mereu cu tine. Probabil. Oricât de minunat este un planificator de hârtie, este încă un lucru de purtat cu tine.

- **Aplicație de editare foto**: O aplicație de editare a imaginilor pentru fotografii digitale. Este folosit pentru decuparea și retușarea fotografiilor, precum și pentru a le organiza în albume și prezentări de diapozitive. Editorii de fotografii nu au, de obicei, nenumăratele filtre și caracteristici ale unui editor de imagini complet, cum ar fi Photoshop de la Adobe sau Corel's Paint Shop Pro.

- **Aplicație de editare a textului**: Un editor de text este un tip de program de calculator care editează text simplu. Editorii de text sunt furnizate cu sisteme de operare și pachete de dezvoltare software și pot fi utilizate pentru a schimba fișiere precum fișierele de configurare, fișierele de documentație și codul sursă al limbajului de programare.

- **Aplicație de social media**: Aplicațiile de rețele sociale sunt aplicații care pot fi fie descărcate și stocate pe telefon sau tabletă, fie transmise prin intermediul browserului de internet. Aplicațiile de rețele sociale implică, în general, mesagerie, partajare de fotografii și conținut interactiv. Facebook, Instagram, Twitter.

5.3.2 Activități practice

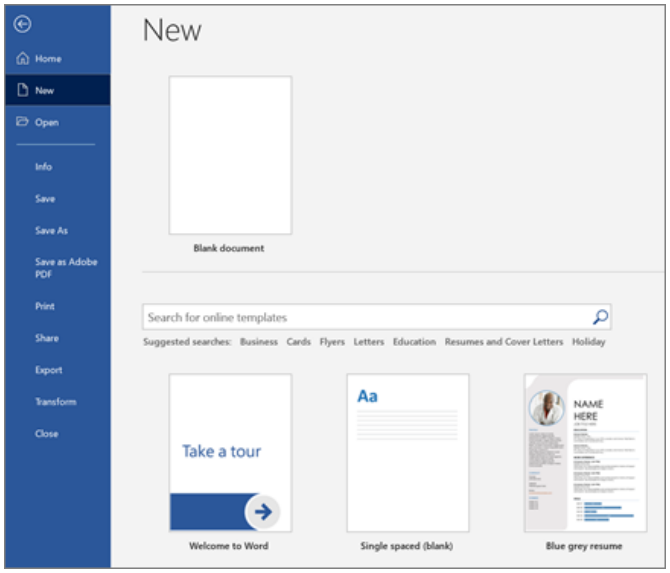
Pasul 1: Creați un document

1. Deschideți o aplicație de text, de ex. Doamna Word.

2. În fila Fișier, faceți clic pe Nou.

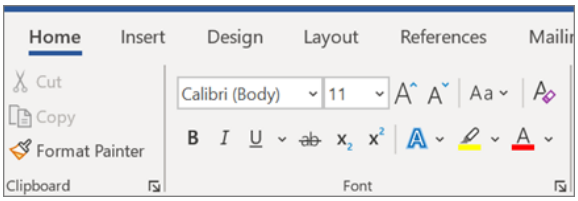
3. În caseta Căutare șabloane online, introduceți tipul de document pe care doriți să îl creați și apăsați ENTER.

Sfat: Pentru a începe de la zero, selectați Document necompletat sau pentru a exersa utilizarea caracteristicilor Word, încercați un ghid de învățare precum Bun venit la Word, Inserați primul cuprins și multe altele.



4. Adăugați și formatați text

1. Plasați cursorul și introduceți ceva text.
2. Pentru a formata, selectați textul și apoi selectați o opțiune: aldine, cursive, marcatori, numerotare și multe altele.



5. Adăugați imagini, forme, SmartArt, diagramă și multe altele

1. Selectați fila Inserare.
2. Selectați ceea ce doriți să adăugați:
    - Tabele - selectați Tabele, plasați cursorul peste dimensiunea dorită și selectați-o.
    - Imagini - selectați Imagini, căutați imaginea dorită și selectați Inserare.
    - Imagini online - selectați Imagini online, căutați și alegeți fotografia dorită și selectați Inserare.
    - Forme - selectați Forme, apoi selectați o formă din meniul drop-down.
    - Pictograme - selectați Pictograme, alegeți-l pe cel dorit și selectați Inserare.
    - Modele 3D - selectați Modele 3D, alegeți dintr-un fișier sau sursă online, accesați imaginea dorită și selectați Inserare.
    - SmartArt - selectați SmartArt, alegeți un grafic SmartArt și selectați OK.
    - Diagramă - selectați Diagramă, selectați diagrama dorită și selectați OK.
    - Captură de ecran - selectați Captură de ecran și selectați una din meniul drop-down.

6. Imprimați un document în Word

1. Faceți clic pe Fișier > Imprimare.
2. Pentru a previzualiza fiecare pagină, faceți clic pe săgețile înainte și înapoi din partea de jos a paginii. Dacă textul este prea mic pentru a fi citit, utilizați glisorul de zoom din partea de jos a paginii pentru a-l mări.
3. Alegeți numărul de copii și orice alte opțiuni dorite și faceți clic pe butonul Imprimare.

Pasul 2: Creați o postare pe rețelele sociale

Urmați pașii următori pentru a crea o postare pe Facebook, atât în aplicația mobilă, cât și pe site-ul Facebook. Postările pot conține text, fotografii, videoclipuri și date despre locație. Puteți posta pe propria pagină, pe pagina unui prieten sau pe pagina unui grup din care faceți parte.

1. Deschide Facebook. Pictograma aplicației Facebook arată ca un „f” alb pe un fundal albastru închis. Facebook se va deschide în fluxul dvs. de știri dacă sunteți deja autentificat.

Dacă nu sunteți deja autentificat, introduceți adresa de e-mail (sau numărul de telefon) și parola, apoi atingeți Conectare.

2. Accesați pagina în care doriți să postați. În funcție de locul în care doriți să vă creați postarea, aceasta va varia:

- Pagina dvs. - Puteți crea o postare pentru pagina dvs. din partea de sus a fluxului de știri.

- Pagina unui prieten - Atingeți bara de căutare din partea de sus a ecranului, introduceți numele unui prieten, atingeți-i numele, apoi atingeți imaginea de profil a acestuia.
- Un grup - Atingeți☰, atingeți Grupuri, atingeți fila Grupuri și atingeți grupul dvs.

3. Atingeți căsuța poștală.Această casetă se află în partea de sus a fluxului de știri. Dacă postați pe pagina unui prieten, acesta se află sub secțiunea de fotografii care se află în partea de sus a paginii acestuia. Dacă postați într-un grup, veți găsi caseta chiar sub fotografia de copertă.

- În general, va exista o expresie precum „Scrie ceva” sau „Ce ai în minte?” in cutie.

4. Încărcați o fotografie sau un videoclip.Atingeți Foto/Video lângă mijlocul ecranului de postare, apoi selectați o fotografie sau un videoclip de încărcat și atingeți Terminat. Procedând astfel, fotografia sau videoclipul se adaugă la postarea ta.

- Puteți atinge mai multe fotografii sau videoclipuri pentru a le încărca pe toate simultan.
- Omite acest pas dacă vrei să încarci o postare numai text.

5. Adăugați text la postarea dvs.Atingeți câmpul de text, apoi introduceți textul pentru postarea dvs.

- De asemenea, puteți atinge un cerc colorat de-a lungul mijlocului ecranului pentru a seta un fundal pentru postarea dvs. Puteți adăuga culoare doar postărilor cu 130 de caractere sau mai puțin.

6. Atinge Adaugă la postarea ta. Este în mijlocul ecranului. Acest lucru va aduce următoarele opțiuni de postare:

- Foto/Video - Adăugați mai multe fotografii sau videoclipuri.
- Înregistrare - Vă permite să adăugați o adresă sau o locație la postarea dvs.
- Sentiment/Activitate/Sticker - Vă permite să adăugați o emoție, activitate sau emoji.
- Etichetează persoane - Vă permite să adăugați o persoană la această postare. Procedând astfel, postarea va fi pusă și pe pagina lor.

7. Selectați o opțiune de postare pentru a adăuga mai multe la postare.Acest lucru este complet opțional. Dacă nu doriți să adăugați mai multe la postare, treceți la pasul următor.

8. Atingeți Postare. Este în colțul din dreapta sus al ecranului. Procedând astfel, veți crea postarea și o veți adăuga la pagina pe care vă aflați.

5.4 Identificarea lacunelor de competență digitală

Unitatea 5.4	Identificarea lacunelor de competență digitală
Durată	5h
Obiective	A fi capabil să folosească tehnologiile pentru a interacționa cu ceilalți
Conținut	5.4.1 Decalajul de competențe digitale în Europa 5.4.2 Activități practice
Resurse	Manual de instruire Computer cu acces la internet
Metodologii de instruire	Prezentare de către trainer Lucrul în perechi/grupuri mici

Masa 30- Structura unității de competență 5.4. – Identificarea lacunelor de competențe digitale ale Modulului 5 – Rezolvarea problemelor

5.4.1 Decalajul de competențe digitale în Europa

Tehnologiile digitale sunt utilizate în multe sectoare precum agricultură, sănătate, transport, educație, comerț cu amănuntul, automată, energie, transport maritim, logistică, predare și industria tehnologiei informației și comunicațiilor. Cererea de specialiști în tehnologia informației și comunicațiilor crește rapid. În viitor, 9 din 10 locuri de muncă vor necesita competențe digitale. În același timp, 169 de milioane de europeni între 16 și 74 de ani – 44% – nu au competențe digitale de bază

Ca orice, dacă vrei să crești în acest domeniu, trebuie să înveți în continuare.

Elevii vor putea afla ce îmbunătățiri vor trebui să facă pentru a dobândi sau a îmbunătăți abilitățile și competențele necesare pentru a performa cât mai bine în rolul lor (viitor). În cele din urmă, acest lucru va avea și un impact pozitiv asupra vieții tale de zi cu zi.

1. **Investește în educație.** Site-uri precum Udemy și Skillshare au niște cursuri geniale pe o serie întreagă de subiecte digitale. DinSEOși Google Analytics la Social Media și Content Marketing, veți fi sigur că veți găsi ceva în zona despre care doriți să aflați mai multe. Asigurați-vă întotdeauna că verificați recenziile înainte de a cumpăra un curs și uitați-vă în cât timp va dura să fie finalizat. Unele cursuri pot fi finalizate într-o zi, în timp ce altele vor necesita mai mult timp.
2. **Apăsați abonați-vă.** Când întâlniți un articol cu adevărat util, apăsați abonați-vă pe site pentru a primi buletine informative viitoare. Merită atunci când conținutul iese în evidență pentru tine, deoarece, sunt șanse, articolele viitoare vor fi la fel de utile.

Asigurați-vă că faceți acest lucru selectiv, deoarece ultimul lucru pe care îl doriți este să fiți bombardat. Prin filtrarea conținutului superior, veți ști când un e-mail ajunge în căsuța dvs. de e-mail, merită citit.

3. **Alăturați-vă la grupuri**. Comunitățile, forumurile și grupurile online pot fi o resursă excelentă pentru a fi la curent în acest domeniu. Învață de la alții și împărtășește-ți experiența în conversațiile în curs. Asigurați-vă că procedați cu prudență, deoarece unele grupuri pot conține o mulțime de spam și informații irelevante.

   Căutați pe Facebook și LinkedIn grupuri din nișa dvs., indiferent dacă este vorba de marketing digital în general sau ceva mai specific, cum ar fi comerțul electronic sau rețelele sociale. Ține minte, cu cât ești mai specific, cu atât conversațiile și postările vor fi mai relevante.

4. **Începeți-vă cu Google Alerts**. Acest instrument ingenios este o modalitate excelentă de a rămâne la curent cu tendințele și sfaturile. Pur și simplu informați Google cuvintele cheie despre care doriți să fiți notificat atunci când apar în rezultatele căutării și veți fi avertizat printr-un e-mail.

   De exemplu, când apare „Tendințe SEO 2019”, vi se va trimite un e-mail cu un link către site-ul corespunzător. Acesta este un mod excelent de a fi la curent cu aproape orice. În plus, puteți limita numărul de e-mailuri de pe Google și puteți avea totul împachetat într-un rezumat săptămânal pentru a evita un bombardament zilnic.

5. **Mergeți pe YouTube.** În zilele noastre, există un videoclip despre aproape orice pe YouTube. Da, trebuie să verificați uneori pentru a găsi pietrele prețioase, dar poate merita. Se poate întâmpla ca un concept cu care te lupți să poată fi rezolvat cu ușurință în câteva minute atunci când aterizezi pe un videoclip informativ.

6. **Folosește hashtag-uri.** Aceasta este o modalitate excelentă de a căuta tendințe recente, știri și actualizări în orice domeniu. Luați doar câteva minute când călătoriți cu trenul sau în timpul prânzului pentru a merge pe Twitter sau LinkedIn și pentru a căuta câteva hashtag-uri. Veți putea naviga rapid la conținutul de top sub acel hashtag și veți putea citi cel mai recent conținut. Dacă întâlniți pe cineva care împărtășește actualizări regulate în nișa dvs., probabil că merită urmărit.

5.4.2 Activități practice

Pasul 1: Abonați-vă la un canal YouTube

1. Accesațihttps://www.youtube.comîntr-un browser web. Aceasta deschide site-ul YouTube.

2. Conectați-vă la contul dvs. Trebuie să fiți conectat la un cont Google pentru a vă abona la canalele YouTube. Dacă nu sunteți conectat, faceți clic pe butonul albastru „CONECTARE” din colțul din dreapta sus și apoi conectați-vă cu contul dvs. Google.

- Dacă sunteți deja conectat și doriți să schimbați conturile, faceți clic pe fotografia de profil din colțul din dreapta sus, selectați Schimbați cont și apoi alegeți alt cont din listă. Dacă nu vedeți contul pe care doriți să-l utilizați, faceți clic pe Adăugare cont pentru a adăuga sau a crea alt cont.

3. Căutați un canal. Puteți verifica ce este Trending în panoul din stânga, puteți căuta un anumit canal sau puteți găsi ceva nou căutând cuvinte cheie.

- Dacă știți numele canalului la care doriți să vă abonați (sau doriți să căutați după cuvânt cheie), introduceți-l în bara de căutare din partea de sus a YouTube și apăsați Enter sau Return. Pentru a vedea doar canalele, dați clic pe Filtru în colțul din stânga sus al rezultatelor căutării și selectați Canale sub „Tip”.
- De asemenea, vă puteți abona la un canal din oricare dintre videoclipurile canalului. Introduceți numele unui videoclip în bara de căutare și apăsați Enter sau Return. Apoi, dați clic pe un videoclip pentru a începe să-l vizionați—numele canalului va apărea sub titlul videoclipului.

4. Faceți clic pe ABONARE pentru a vă abona la un canal. Este un buton roșu-alb – dacă vă aflați pe pagina de pornire a canalului, acesta va fi lângă colțul din dreapta sus al paginii, sub imaginea de copertă. Dacă aveți un videoclip deschis, acesta se află sub videoclipul din dreapta numelui canalului.

- Acum că sunteți abonat, textul de pe butonul „SUBSCRIBE” va deveni gri și se va schimba în SUBSCRIBED. Făcând clic pe acel buton în orice moment, te va dezabona de la canal.

5. Vizualizați abonamentele dvs. Faceți clic pe cele trei linii orizontale din colțul din stânga sus al YouTube pentru a deschide meniul și selectați Abonamente pentru a vedea toate canalele la care sunteți abonat.

- Abonamentele dvs. apar sub „ABONAMENTE” în panoul din stânga.
- Faceți clic pe unul dintre canalele dvs. abonate pentru a vedea conținutul său cel mai recent.

6. Ajustați preferințele de notificare. Veți fi notificat în mod prestabilit cu privire la unele actualizări ale canalului. Pentru a primi mai multe sau mai puține actualizări de la un canal, faceți clic pe canal, apoi faceți clic pe pictograma clopoțel de lângă butonul „SUBSCRIBED”. Apoi, faceți clic pe Toate, Niciunul sau Personalizat. Personalizate bazează notificări despre activitatea dvs.

- Pentru a specifica modul în care sunteți notificat cu privire la actualizări, faceți clic pe fotografia de profil din colțul din dreapta sus, selectați Setări, apoi faceți clic pe Notificări în panoul din stânga. Utilizați glisoarele pentru a controla notificările despre care sunteți notificat.

Pasul 2: Alăturați-vă unui grup de interese pe rețelele sociale

1. Deschide Facebook. Pictograma aplicației mobile Facebook este un „f" alb pe un fundal albastru închis. Facebook se va deschide în fluxul dvs. de știri dacă sunteți deja autentificat.

- Dacă nu sunteți deja autentificat, introduceți adresa de e-mail (sau numărul de telefon) și parola, apoi atingeți Conectare.

2. Atingeți bara de căutare. Este în partea de sus a ecranului. Aceasta va afișa tastatura dispozitivului dvs.

3. Introduceți un nume de grup sau un cuvânt cheie. Introduceți numele unui grup (sau un cuvânt sau o expresie care vă interesează), apoi atingeți Căutare. Aceasta va căuta pe Facebook conturi, pagini, locuri și grupuri care se potrivesc căutării tale.

4. Atingeți Grupuri. Aceasta este o filă în partea de sus a ecranului, chiar sub bara de căutare. Aceasta va afișa toate grupurile legate de căutarea dvs.

- Poate fi necesar să glisați rândul de file aici spre stânga pentru a afișa opțiunea Grupuri.

5. Atingeți Alăturați-vă lângă un grup. Butonul ***Alăturați-vă*** este în partea dreaptă a numelui unui grup. Atingând-o, va apărea o ștampilă „Solicitată" în partea dreaptă a grupului. Odată ce sunteți acceptat în grup de către un administrator, veți putea posta în grup.

- Dacă grupul este public în loc să fie închis, veți putea vedea (dar nu interacționa cu) postările și membrii grupului.

Felicitări, acum ați finalizat Modulul 5 și ați terminat cursul.

Nu uitați să verificați Anexele pentru resurse și documente suplimentare furnizate pentru a sprijini auto-studiul! Bine făcut!

No One Behind

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

EVALUAREA ANTRENAMENTULUI

1. Evaluarea invatarii

În cadrul metodologiei proiectului No One Behind, consorțiul a dezvoltat sistemul de evaluare care este introdus corespunzător în documentul Metodologie inovatoare pentru educarea și formarea adulților din zona rurală pentru a-și îmbunătăți competențele digitale și TIC.[16]. Conform acestui sistem, pentru fiecare unitate de competență sunt definiți indicatorii calitativi de evaluare a domeniului de competență al cursanților adulți (Tabel):

M1 - Informații și alfabetizare a datelor	
Navigarea, căutarea și filtrarea datelor, informațiilor și conținutului digital	- Să fie capabil să identifice diferite browsere web. - Să fie capabil să recunoască diferite motoare de căutare. - Să poată căuta informații și conținut online. - Să fiți capabil să navigați între mediile digitale. - Să fie capabil să înțeleagă riscurile de confidențialitate și confidențialitate ale căutării pe internet. - Să fie capabil să cunoască rolul internetului în obținerea de informații în contextul lumii de astăzi.
Evaluarea datelor, informațiilor și conținutului digital	- Să fiți capabil să recunoașteți pericolele știrilor false și dezinformării în era digitală. - Să fie capabil să identifice veridicitatea datelor și acuratețea informațiilor digitale. - Să fie capabil să detecteze credibilitatea și fiabilitatea surselor comune de date, informații și conținutul lor digital. - Să fie capabil să caute date și informații fiabile și credibile.
Gestionarea datelor, informațiilor și conținutului digital	- Să fie capabil să identifice diferite tipuri de programe, instrumente și medii pentru a stoca și gestiona date, informații și conținut digital. - Să poată utiliza instrumente și platforme digitale pentru a stoca și gestiona datele. - Să fie capabil să organizeze conținutul și datele într-o platformă digitală într-un mod structurat. - Să poată accesa medii digitale care definesc setări de confidențialitate adecvate.
M2 - Comunicare și Colaborare	
Interacționând prin tehnologii digitale	- Să fie capabil să identifice diferite instrumente digitale, să le caracterizeze și să le folosească în conformitate cu contextul. - Să fie capabil să interacționeze și să comunice cu diferite audiențe folosind instrumente și dispozitive digitale adecvate. - Să fie capabil să recunoască și să caracterizeze diferite platforme și dispozitive digitale de comunicare. - Să fiți capabil să căutați informații online în condiții de siguranță și etic.
Partajarea prin tehnologii digitale	- Să poată partaja informații cu alții folosind instrumente și/sau platforme adecvate. - Să fie capabil să recunoască și să caracterizeze diferite platforme și dispozitive digitale pentru partajarea informațiilor. - Fiți capabil să împărtășiți informații cu alții în condiții de siguranță și etic. - Să fiți capabil să căutați informații online în condiții de siguranță și etic.

[16] Accesibil Aici.

Implicarea în cetățenie prin tehnologii digitale	- Să fiți capabil să comunicați online în mod etic și deschis la minte. - Să poată participa online în societate ca cetățean. - Să poată utiliza servicii online legale. - Să fie capabil să ofere feedback și opinii cu respect față de ceilalți. - Să fie capabil să recunoască informațiile și serviciile online interactive. - Să poată configura setările pentru a păstra informațiile private.
Colaborarea prin tehnologii digitale	- Să fiți capabil să utilizați diferite instrumente și platforme pentru a comunica online cu ceilalți. - Să poată partaja informații online folosind instrumente și platforme adecvate. - Să poată identifica cele mai utilizate platforme online din țara sau regiunea lor. - Să fii capabil să distingă între platformele de mesagerie instant sau chat, voce-over-IP, platforme de social media, forumuri și e-mail.
Neticheta	- Să fii capabil să demonstreze interacțiune politicoasă online cu ceilalți. - Să fie capabil să identifice ce fel de comportament ar trebui utilizat în diferite medii online (cum ar fi e-mailul, rețelele sociale sau chatul). - Să fie capabil să aplice „bunele maniere” într-un mediu online, comunicând cu ceilalți. - Să fiți capabil să înțelegeți importanța regulilor online atunci când utilizați resursele digitale.
Gestionarea identității digitale	- Să fie capabil să descrie conceptul de identitate digitală. - Să fiți capabil să înțelegeți cum să protejați identitatea digitală. - Să fiți capabil să descrie modalități simple de a proteja reputația online. - Să fie capabil să gestioneze amprenta digitală. - Să fiți capabil să știți cum să respectați identitățile digitale ale altora și să aveți grijă ce să postați despre alți oameni.
M3 - Creare de conținut digital	
Dezvoltarea continutului digital	- Să poată crea și edita conținut digital în diferite formate. - Să fiți capabil să creați conținut și cunoștințe noi, originale. - Să fie capabil să reprezinte bine ceea ce se urmărește să comunice. - Să fie capabil să identifice valoarea conținutului digital ca ajutor vizual. - Să fie capabil să adapteze expresia prin crearea celor mai potrivite mijloace digitale.
Integrarea și reelaborarea conținutului digital	- Să poată modifica informațiile și conținutul într-un document sau platformă existentă. - Să poată integra informații și conținut noi într-un document sau platformă existentă. - Să fie capabil să evalueze cele mai adecvate modalități de a integra anumite elemente noi de conținut și informații.
Drepturi de autor și licențe	- Să fie capabil să aplice drepturile de autor și licențele într-un mod precis. - Să fie capabil să identifice ce licențe sunt necesare în anumite circumstanțe. - Să știe cum să se protejeze împotriva încălcării drepturilor de autor.
Programare	- Să fie capabil să enumere instrucțiuni simple pentru un sistem de calcul pentru a rezolva o problemă simplă sau a efectua o sarcină simplă. - Să fie capabil să rezolve probleme tehnice simple. - Să fie capabil să aplice instrucțiuni pentru a îndeplini sarcini sau pentru a rezolva probleme.
M4 - Siguranță	
Dispozitive de protecție	- Să fie capabil să înțeleagă importanța protecției dispozitivelor și să evite riscurile. - Să fie capabil să identifice diferența dintre diferitele tipuri de malware. - Să fie capabil să înțeleagă importanța măsurilor legate de fiabilitate și confidențialitate.

Protejarea datelor personale și a confidențialității	- Să poată păstra datele personale protejate. - Să poată înțelege riscul furtului de identitate. - Să poată aplica „Politica de confidențialitate" atunci când utilizați servicii digitale. - Să fie capabil să înțeleagă regulile de bază ale securității.
Protejarea sănătății și a bunăstării	- Să fiți capabil să evitați riscurile pentru sănătate și amenințările la adresa bunăstării fizice și psihologice în timp ce utilizați tehnologiile digitale. - Să fie capabil să controleze posibilele pericole și amenințări în mediile digitale. - Să fie capabil să identifice riscurile utilizării abuzive a serviciilor online și digitale.
Protejand mediul inconjurator	- Să fie capabil să recunoască impacturile simple asupra mediului ale tehnologiilor digitale și ale utilizării acestora. - Să poată utiliza serviciile digitale fără a fi dependent de acestea. - Să fie capabil să protejeze mediul înconjurător de impactul aruncării dispozitivelor digitale.
M5 - Rezolvarea problemelor	
Rezolvarea problemelor tehnice	- Să fiți capabil să navigați online în contexte de zi cu zi. - Să fie capabil să identifice când un dispozitiv digital este suficient de adecvat pentru a lucra. - Să fie capabil să identifice când a apărut o problemă pe un dispozitiv sau serviciu digital.
Identificarea nevoilor și a răspunsurilor tehnologice	- Să fie capabil să recunoască problemele tehnice care provin de la un dispozitiv digital sau din mediu. - Să fie capabil să recunoască metodele de rezolvare. - Să fiți capabil să înțelegeți cum să utilizați facilitățile de ajutor, ghidurile manuale.
Folosind creativ tehnologiile digitale	- Să fie capabil să utilizeze tehnologia digitală adecvată pentru un anumit scop (a aduna informații, a crea conținut). - Să fie capabil să utilizeze componente ale sistemelor digitale și informații digitale în condiții reale.
Identificarea lacunelor de competență digitală	- Să fie capabil să se evalueze pe sine sau pe alții dacă noile medii digitale sunt mijloace adecvate de îmbunătățire a nivelului de competență digitală. - Să fie capabil să caute oportunități de auto-dezvoltare și să fii la curent cu evoluția digitală.

Masa 31 – Identificarea criteriilor de evidență a fiecărei unități de competență, pentru evaluarea domeniului de competență de către cursanții adulți.

Aceste criterii de dovezi ar trebui utilizate pentru a evalua domeniul de competență de către cursanți și pot fi evaluate în două moduri:

- De către educatori sau formatori de adulți prin observarea performanței cursanților pe parcursul desfășurării activităților propuse și la finalul instruirii prin completarea unei fișe de evaluare.
- De către cursanți adulți care își evaluează domeniul de competență prin completarea unei fișe de evaluare de autoevaluare, la începutul și la sfârșitul fiecărui modul.

În ambele cazuri, se pot folosi fișele de evaluare prevăzute în **Anexele II-V.**

2. Evaluarea instruirii

La finalul cursului de formare, este prevăzută evaluarea acestuia de către cursanții care beneficiază de acesta. Evaluarea instruirii va permite înțelegerea:

- adecvarea și relevanța formării pentru grupurile țintă definite
- calitatea curriculumului de formare din punct de vedere al conţinutului şi al duratei
- valoarea suporturilor si materialelor puse la dispozitie
- suport oferit pe parcursul instruirii

Acest lucru se va face printr-un chestionar (Anexa VI) care va fi disponibil online. De asemenea, recomandăm un moment de debriefing, la sfârșitul fiecărui modul și la sfârșitul cursului, în care cursanții pot găsi spațiu pentru a vorbi despre experiența lor de învățare, ce le-a plăcut cel mai mult și cel mai puțin, care au fost principalele dificultăți, cum au planifică să continue să exerseze ceea ce au învățat la curs și așa mai departe.

No One Behind

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

ANEXE

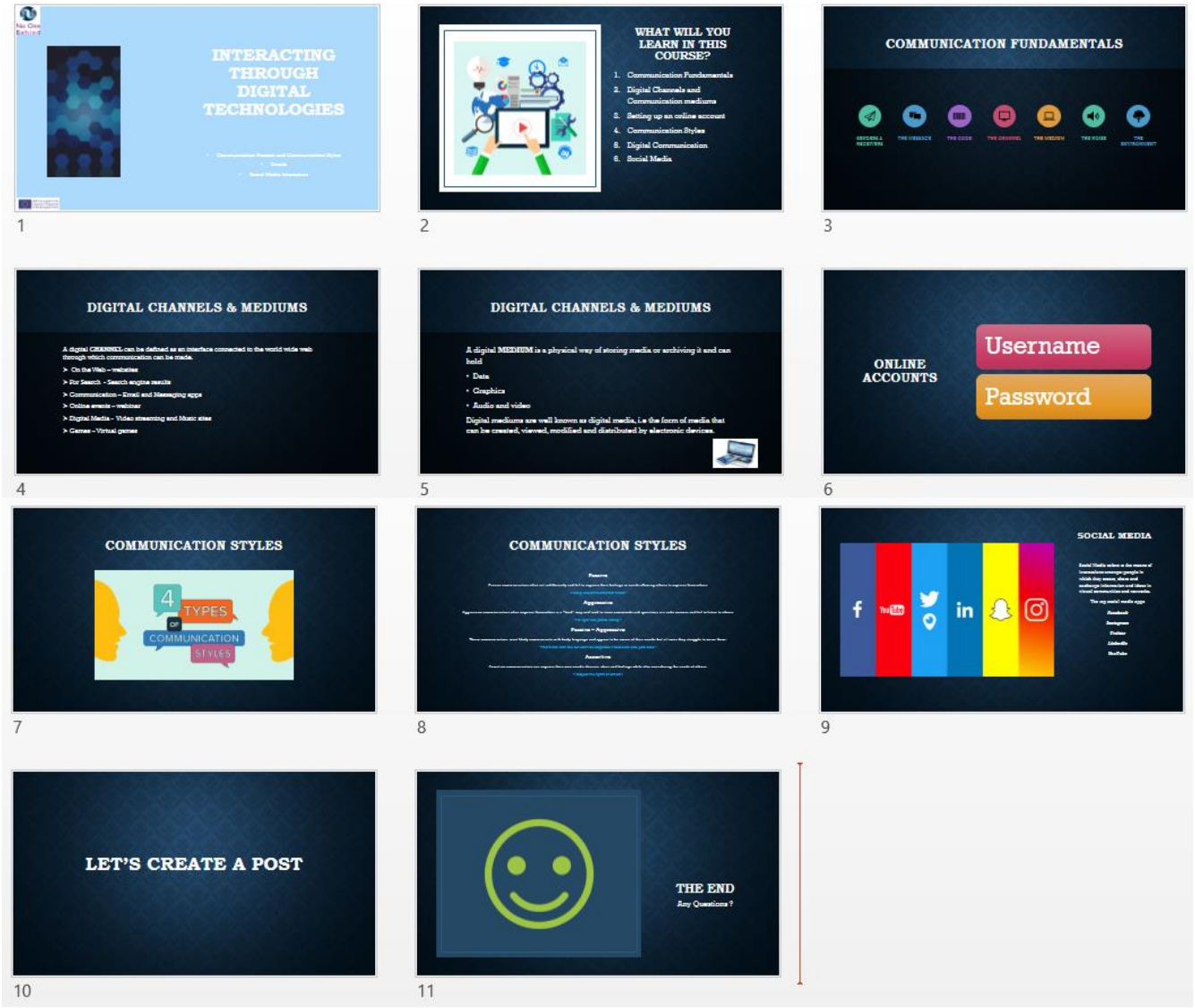
Anexa I – Resurse suplimentare

Modul	Unitate	Resurse
Modulul 1	1.1	**Instruire online IT** – https://edu.gcfglobal.org/en/subjects/tech/ **Tutorial „Utilizarea motoarelor de căutare”** – https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/ **Cum să cauți eficient pe internet (1)** – https://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_How_Search_Internet_Effectively.pdf **Cum să cauți eficient pe internet (2)** – https://mediasmarts.ca/sites/default/files/tip-sheet/tipsheet_we_are_broadcasters.pdf
	1.2	**Protejarea datelor** - https://ec.europa.eu/info/sites/default/files/charter-application_en.pdf **Cum se răspândesc știrile false** - https://www.youtube.com/watch?v=cSKGa_7XJkg
Modulul 2	2.1	**Tutorial de bază pentru e-mail**: https://www.youtube.com/watch?v=cnxsl8h5gj4 **Utilizarea instrumentelor digitale pentru a transforma sălile de clasă**: https://www.youtube.com/watch?v=B99FXVamqMM **Ce spune stilul tău de comunicare digitală despre tine**: https://www.webroot.com/us/en/resources/tips-articles/what-your-digital-communication-style-says-about-you
	2.2	**Cele mai bune lecții pentru a partaja notele lecției digital:**http://blog.whooosreading.org/digital-notes/ **Distribuiți digital și comentați:** https://applieddigitalskills.withgoogle.com/c/middle-and-high-school/en/create-a-presentation-all-about-a-topic/create-a-presentation-all-about-a-topic/distribuie-și-comentează-digital.html
	2.3	**Cetățenie digitală:** https://education.microsoft.com/en-us/course/192d4b4a/overview https://www.youtube.com/watch?v=ju9aOc2MLyo https://www.youtube.com/watch?v=HIll6YjE2ds https://ikeepsafe.org/content/uploads/2020/02/Class-2_Student_FINAL-1.pdf **Ce sunt informațiile personale:** https://www.commonsensemedia.org/educators/lesson/keep-it-private-k-2 **Cetățenia digitală și predarea acesteia:** https://files.eric.ed.gov/fulltext/EJ1286737.pdf
	2.4	**30 dintre cele mai bune instrumente de colaborare digitală pentru studenți** - https://www.teachthought.com/technology/12-tech-tools-for-student-to-student-digital-collaboration/ **Importanța muncii în echipă și a colaborării într-o lume digitală** - https://blog.bit.ai/importance-of-teamwork-and-collaboration/ **Instrument de colaborare digitală**: https://www.youtube.com/watch?v=TSz2CxnuGkQ https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework https://zapier.com/blog/dropbox-vs-google-drive/ https://support.google.com/a/users/answer/9302892?hl=ro https://kissflow.com/project/best-project-management-tools/

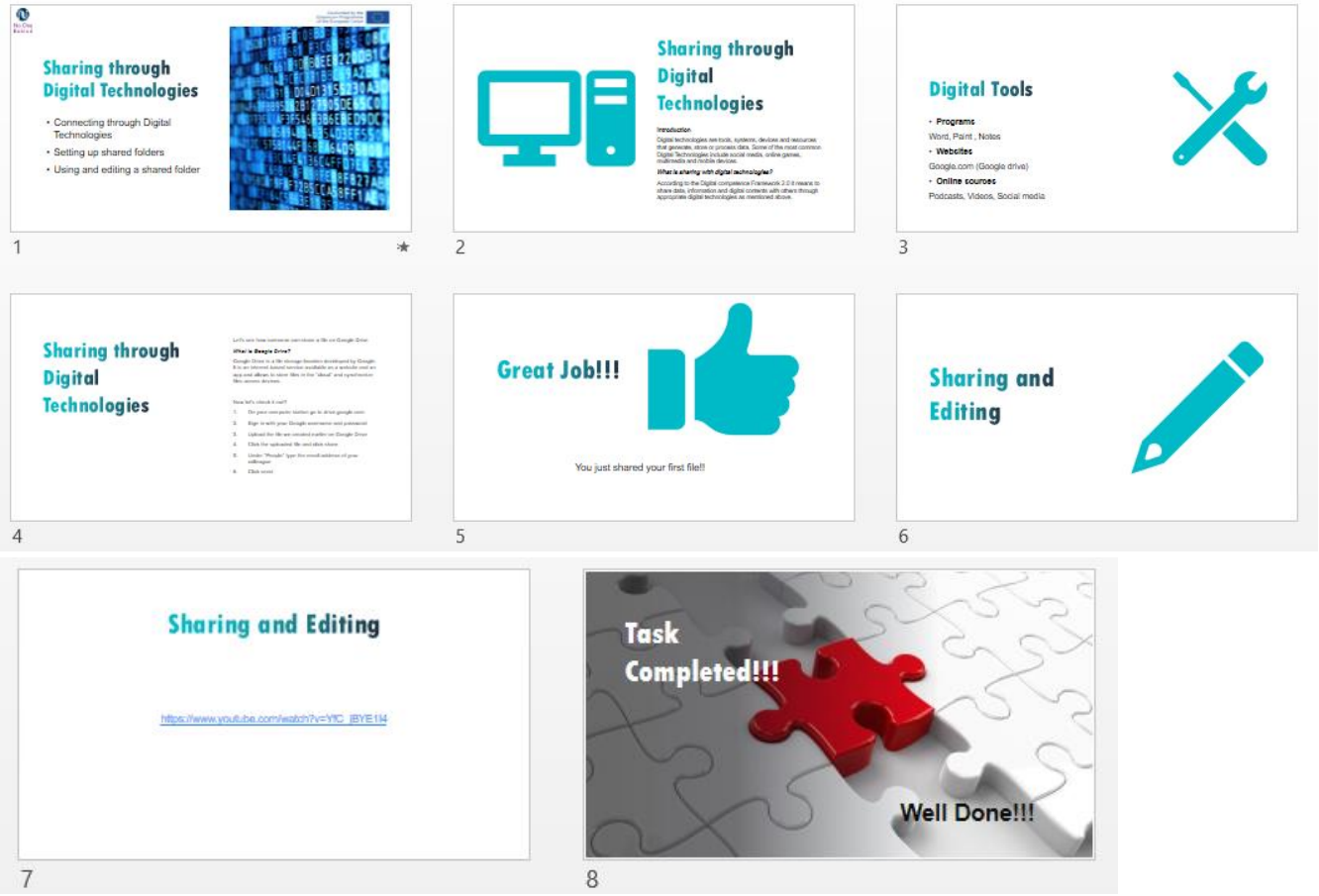
	2.5	**Netiquette sens, definiție și explicație -** https://www.youtube.com/watch?v=7-HopTAFUm0 **Exemple de netichetă proastă -** https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette **Exemple de netichetă bună -** https://www.cybersmile.org/advice-help/category/examples-of-good-netiquette https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette https://slangit.com/meaning/keyboard_warrior
	2.6	**Parole: Cum să vă protejați activele digitale -** https://www.funeralwise.com/learn/digitallegacy/how-to-manage-passwords/ **Identitatea digitală: ce este + de ce este valoroasă -** https://learn.g2.com/digital-identity **Ce este identitatea digitală și cum funcționează -** https://www.techfunnel.com/information-technology/what-is-digital-identity/ https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/ https://www.techrepublic.com/article/how-to-protect-yourself-and-your-organization-against-digital-identity-fraud/ https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message
Modulul 5		https://medium.com/beyond/6-ways-to-stay-on-top-of-emerging-technology-trends-ca6a7b27bc20 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://digital-strategy.ec.europa.eu/en/library/digital-skills-gap-europe http://www.dcds-project.eu/wp-content/uploads/2019/02/D6_DCD-Methodology-_v1_revised.pdf http://www.dcds-project.eu/wp-content/uploads/2018/12/D5_Contents_assessment_tool.pdf https://www.digitalhrtech.com/skills-gap-analysis 341727166_Digital_Creative_Skills_What_sun_they_What_does_progression_look_like_How_sont_they_developed_What_promising_practices_are_there https://www.opencolleges.edu.au/informed/features/8-ways-boost-creativity-technology 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/

Resurse suplimentare – prezentări Power Point

Modulul 2, Unitatea 2.1 – Interacțiunea prin tehnologii digitale



Modulul 2, Unitatea 2.2 - Partajarea prin tehnologii digitale



Modulul 2, Unitatea 2.3 – Implicarea în cetățenie prin tehnologii digitale

Anexa II – Fișă de evaluare Modulul 1. Informații și alfabetizare a datelor

Informații și alfabetizare a datelor

1.1. Navigarea, căutarea și filtrarea informațiilor

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fie capabil să identifice diferite browsere web.	☐	☐	☐
Să fie capabil să recunoască diferite motoare de căutare.	☐	☐	☐
Fiți capabil să căutați informații și conținut online.	☐	☐	☐
Să fiți capabil să navigați între mediile digitale.	☐	☐	☐
Să fiți capabil să înțelegeți riscurile confidențialității și confidențialității căutării pe internet.	☐	☐	☐
Să fie capabil să cunoască rolul internetului în obținerea de informații în contextul lumii de astăzi.	☐	☐	☐

1.2. Evaluarea datelor, informațiilor și conținutului digital

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fiți capabil să recunoașteți pericolele știrilor false și dezinformării în era digitală.	☐	☐	☐
Să fie capabil să identifice veridicitatea datelor și acuratețea informațiilor digitale.	☐	☐	☐
Să fie capabil să detecteze credibilitatea și fiabilitatea surselor comune de date, informații și conținutul lor digital.	☐	☐	☐
Să fiți capabil să căutați date și informații fiabile și credibile.	☐	☐	☐

1.3. Gestionarea datelor, informațiilor și conținutului digital

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fie capabil să identifice diferite tipuri de programe, instrumente și medii pentru a stoca și gestiona date, informații și conținut digital.	☐	☐	☐
Să fiți capabil să utilizați instrumente și platforme digitale pentru a stoca și gestiona datele.	☐	☐	☐
Să fii capabil să organizezi conținutul și datele într-o platformă digitală într-un mod structurat.	☐	☐	☐
Să poată accesa medii digitale care definesc setările de confidențialitate adecvate.	☐	☐	☐

Anexa III – Fișă de evaluare Modulul 2. Comunicare și colaborare

Comunicare și colaborare

2.1. Interacționând prin tehnologii

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fie capabil să identifice diferite instrumente digitale, să le caracterizeze și să le folosească în conformitate cu contextul.	☐	☐	☐
Să fie capabil să interacționeze și să comunice cu diferite audiențe folosind instrumente și dispozitive digitale adecvate.	☐	☐	☐
Să fie capabil să recunoască și să caracterizeze diferite platforme și dispozitive digitale de comunicare.	☐	☐	☐
Fiți capabil să căutați informații online în condiții de siguranță și etic.	☐	☐	☐

2.2. Partajarea prin tehnologii digitale

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să poată partaja informații cu alții folosind instrumente și/sau platforme adecvate.	☐	☐	☐
Să fie capabil să recunoască și să caracterizeze diferite platforme și dispozitive digitale pentru partajarea informațiilor.	☐	☐	☐
Fiți capabil să împărtășiți informații cu alții în condiții de siguranță și etic.	☐	☐	☐
Fiți capabil să căutați informații online în condiții de siguranță și etic.	☐	☐	☐

2.3. Implicarea în cetățenie prin tehnologii digitale

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fiți capabil să comunicați online în mod etic și deschis la minte.	☐	☐	☐
Să fii capabil să participi online în societate ca cetățean.	☐	☐	☐
Să poată utiliza serviciile legale online.	☐	☐	☐
Să fie capabil să ofere feedback și opinii cu respect pentru ceilalți.	☐	☐	☐
Să fie capabil să recunoască informațiile și serviciile online interactive.	☐	☐	☐
Puteți configura setările pentru a păstra informațiile private.	☐	☐	☐

2.4. Colaborarea prin tehnologii digitale

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fiți capabil să utilizați diferite instrumente și platforme pentru a comunica online cu ceilalți.	☐	☐	☐
Să poată partaja informații online folosind instrumente și platforme adecvate.	☐	☐	☐
Să poată identifica cele mai utilizate platforme online din țara sau regiunea lor.	☐	☐	☐

	Fiți capabil să distingeți între platformele de mesagerie instantanee sau chat, voce peste IP, platforme de social media, forumuri și e-mail.	☐	☐	☐
	2.5. Neticheta			
	Unitatea de competență	**Nici unul**	**De bază**	**Deasupra de bază**
	Să fii capabil să demonstrezi interacțiune politicoasă online cu ceilalți.	☐	☐	☐
	Să fiți capabil să identificați ce fel de comportament ar trebui utilizat în diferite medii online (cum ar fi e-mailul, rețelele sociale sau chatul).	☐	☐	☐
	Să fiți capabil să aplicați „bunele maniere” într-un mediu online, comunicând cu ceilalți.	☐	☐	☐
	Să fiți capabil să înțelegeți importanța regulilor online atunci când utilizați resurse digitale.	☐	☐	☐
	2.6. Gestionarea identității digitale			
	Unitatea de competență	**Nici unul**	**De bază**	**Deasupra de bază**
	Să fie capabil să descrie conceptul de identitate digitală.	☐	☐	☐
	Să fiți capabil să înțelegeți cum să protejați identitatea digitală.	☐	☐	☐
	Să fiți capabil să descrie modalități simple de a proteja reputația online.	☐	☐	☐
	Să fii capabil să gestionezi amprenta digitală.	☐	☐	☐
	Să fiți capabil să știți cum să respectați identitățile digitale ale altora și să aveți grijă ce să postați despre alți oameni.	☐	☐	☐

Anexa IV – Fișă de evaluare Modulul 3. Crearea conținutului

Creare de conținut digital

3.1. Dezvoltarea continutului

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să poată crea și edita conținut digital în diferite formate.	☐	☐	☐
Să fiți capabil să creați conținut și cunoștințe noi, originale.	☐	☐	☐
Să fii capabil să reprezinte bine ceea ce se dorește să comunice.	☐	☐	☐
Să fie capabil să identifice valoarea conținutului digital ca ajutor vizual.	☐	☐	☐
Să fie capabil să adapteze expresia prin crearea celor mai potrivite mijloace digitale.	☐	☐	☐

3.2. Integrarea și reelaborarea

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să poată modifica informațiile și conținutul într-un document sau platformă existentă.	☐	☐	☐
Să poată integra informații și conținut noi într-un document sau platformă existentă.	☐	☐	☐
Să fie capabil să evalueze cele mai adecvate modalități de a integra elemente noi specifice de conținut și informații.	☐	☐	☐

3.3. Drepturi de autor și licențe

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fie capabil să aplice drepturile de autor și licențele într-un mod precis.	☐	☐	☐
Să fie capabil să identifice ce licențe sunt necesare în anumite circumstanțe.	☐	☐	☐
Să poată știi cum să se protejeze împotriva încălcării drepturilor de autor.	☐	☐	☐

3.4. Programare

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fiți capabil să enumerați instrucțiuni simple pentru un sistem de calcul pentru a rezolva o problemă simplă sau pentru a efectua o sarcină simplă.	☐	☐	☐
Să fie capabil să rezolve probleme tehnice simple.	☐	☐	☐
Să fie capabil să aplice instrucțiuni pentru a îndeplini sarcini sau pentru a rezolva probleme.	☐	☐	☐

Anexa IV – Fișă de evaluare Modulul 4. Siguranță

Siguranță

4.1. Dispozitive de protecție

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fiți capabil să înțelegeți importanța protecției dispozitivelor și să evitați riscurile.	☐	☐	☐
Să fiți capabil să identificați diferența dintre diferitele tipuri de malware.	☐	☐	☐
Să fie capabil să înțeleagă importanța măsurilor legate de fiabilitate și confidențialitate.	☐	☐	☐

4.2. Protejarea datelor personale

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să poată păstra datele personale protejate.	☐	☐	☐
Să fiți capabil să înțelegeți riscul furtului de identitate.	☐	☐	☐
Să puteți aplica „Politica de confidențialitate” atunci când utilizați servicii digitale.	☐	☐	☐
Să fie capabil să înțeleagă regulile de bază ale securității.	☐	☐	☐

4.3. Protejarea sănătății

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fiți capabil să evitați riscurile pentru sănătate și amenințările la adresa bunăstării fizice și psihologice în timp ce utilizați tehnologiile digitale.	☐	☐	☐
Să fiți capabil să controlați posibilele pericole și amenințări din mediile digitale.	☐	☐	☐
Să fie capabil să identifice riscurile utilizării abuzive a serviciilor online și digitale.	☐	☐	☐

4.4 Protejarea mediului

Unitatea de competență	Nici unul	De bază	Deasupra de bază
Să fie capabil să recunoască impacturile simple asupra mediului ale tehnologiilor digitale și ale utilizării acestora.	☐	☐	☐
Să poată utiliza serviciile digitale fără a fi dependent de acestea.	☐	☐	☐
Să fie capabil să protejeze mediul înconjurător de impactul aruncării dispozitivelor digitale.	☐	☐	☐

Anexa V – Fişa de evaluare Modulul 5. Rezolvarea problemelor

Rezolvarea problemelor

5.1. Rezolvarea problemelor tehnice			
Unitatea de competență	**Nici unul**	**De bază**	**Deasupra de bază**
Să fiți capabil să navigați online în contexte de zi cu zi.	☐	☐	☐
Să fiți capabil să identificați când un dispozitiv digital este suficient de adecvat pentru a lucra.	☐	☐	☐
Să poată identifica când a apărut o problemă pe un dispozitiv sau serviciu digital.	☐	☐	☐
5.2. Identificarea nevoilor și a răspunsurilor tehnologice			
Unitatea de competență	**Nici unul**	**De bază**	**Deasupra de bază**
Să fie capabil să recunoască problemele tehnice care provin de la un dispozitiv digital sau din mediu.	☐	☐	☐
Să fie capabil să recunoască metodele de rezolvare.	☐	☐	☐
Să fiți capabil să înțelegeți cum să utilizați facilitățile de ajutor, ghidurile manuale.	☐	☐	☐
5.3. Inovarea și utilizarea creativă a tehnologiei			
Unitatea de competență	**Nici unul**	**De bază**	**Deasupra de bază**
Să fie capabil să utilizeze tehnologia digitală adecvată pentru un anumit scop (a aduna informații, a crea conținut).	☐	☐	☐
Să fie capabil să utilizeze componente ale sistemelor digitale și informații digitale în condiții reale.	☐	☐	☐
5.4. Identificarea lacunelor de competență digitală			
Unitatea de competență	**Nici unul**	**De bază**	**Deasupra de bază**
Să fie capabil să se evalueze pe sine sau pe alții dacă noile medii digitale sunt mijloace adecvate de îmbunătățire a nivelului de competență digitală.	☐	☐	☐
Să fii capabil să cauți oportunități de auto-dezvoltare și să fii la curent cu evoluția digitală.	☐	☐	☐

Anexa VI – Evaluarea instruirii

Această fișă de evaluare are ca obiectiv principal colectarea de date și feedback-ul dumneavoastră despre calitatea programului de formare pentru un cetățean „competent digital". Acest chestionar trebuie completat individual și la sfârșitul instruirii. Chestionarul este confidențial, iar opinia dumneavoastră este crucială pentru îmbunătățirea programului de formare.
Chestionarul este structurat în trei părți: partea A – Statistică are două întrebări care le permit partenerilor să facă o analiză statistică a atelierelor implementate; partea B - Evaluarea cantitativă este compusă din 13 afirmații, la care se răspunde folosind următoarea scală de la 1 la 5: 1 – total dezacord, 2 – în mare parte dezacord, 3 – nici de acord sau dezacord, 4 – în mare parte de acord și 5 – total de acord[17]; partea B – Evaluare calitativă este compusă din două întrebări deschise: una prima în care trebuie să oferiți comentarii/sugestii suplimentare despre afirmațiile pe care le-ați punctat cu 1, 2 sau 3; un al doilea în care puteți adăuga orice comentariu suplimentar la programul de formare și atelier.

Partea A – Date personale

Tara de resedinta

România ☐ Portugalia ☐ Grecia ☐ Italia ☐ Danemarca ☐

Profesie

Partea B – Evaluare Cantitativă

	1	2	3	4	5	N/A
Curriculumul de formare este relevant pentru viața mea personală și/sau profesională.						
Antrenamentul corespundea așteptărilor mele inițiale.						
Obiectivele instruirii au fost atinse.						
Unitățile și conținuturile abordate au fost interesante și relevante.						
Durata instruirii este în funcție de obiectivele, conținuturile și activitățile/sarcinile acestuia.						
Training-ul a permis dobândirea de competențe digitale.						
Conținuturile, practicile și/sau instrumentele introduse în cadrul instruirii au fost potrivite pentru a fi implementate în activitățile mele zilnice.						
Materialele suport utilizate în timpul instruirii au fost adecvate (din punct de vedere al designului, limbajului, utilității, informațiilor furnizate).						
Activitățile, sarcinile și exercițiile propuse în timpul instruirii sunt adecvate dobândirii și dezvoltării/consolidării competențelor digitale.						
Formatorii au oferit suportul necesar participanților pe parcursul instruirii.						
Formatorii au fost clari și eficienți în timpul antrenamentului.						

[17] Dacă una dintre afirmații nu se aplică experienței dumneavoastră, vă rugăm să răspundeți „NA" (nu se aplică).

Formatorii au promovat participarea și implicarea participanților la training.

Partea C – Evaluare calitativă

1. Vă rugăm să furnizați recomandări/sugestii suplimentare cu privire la afirmația pe care ați obținut nota cu 1, 2 sau 3:

2. Aveți vreun comentariu suplimentar legat de programa de formare? Vă rugăm să o distribuiți aici.

Data: ___ / ____ / _____

Vă mulțumim pentru contribuție!

No One Behind

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

REFERINȚE

No One Behind

Comisia Europeană: 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). Conceptele de bază ale Tehnologiei Informației și Comunicațiilor Manual. Societatea deschisă pentru schimbul de idei (ODRAZI), Zagreb. Sursă:http://www.itdesk.info/handbook_basic_ict_concepts.pdf

Enciclopedia Britannica: https://www.britannica.com/technology/browser

Centrul australian de securitate cibernetică: https://www.cyber.gov.au/acsc/view-all-content/guidance/proactive-measures-protect-your-information

Biblioteca Universității din Georgetown: https://www.library.georgetown.edu/tutorials/research-guides/evaluating-internet-content

Revista Smithsonian: https://www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/?no-ist

Universitatea de Stat din Washington Vancouver: https://webliteracy.pressbooks.com/chapter/building-a-habit-by-checking-your-emotions/#footnote-51-1

Bilanțul întreprinderii mici: https://www.thebalancesmb.com/copyright-definition-2948254

Universitatea, Spring Arbor. Fundamentele comunicării: 8 concepte de bază și definiții. Universitatea Spring Arbor. [Online] iunie 2021. https://online.arbor.edu/news/fundamentals-communication-eight-basic-concepts-and-definitions.

7 Exemple de canale digitale. **Spacey, John.** 2017, Simplic .

Cele 10 noi paradigme ale comunicării în era digitală. **Orihuela, Jose Luis.** 2017, Jlori.

4 tipuri de stiluri de comunicare. Universitatea Alvernia. Pennsylvania : sn, 2018, Universitatea Alvernia, p. 2.

LEADGENERA.LEADGENERA. Marketing de conținut. [Online] iunie 2021. https://leadgenera.com/knowledge-hub/marketing/the-10-best-social-media-and-content-apps-for-2020/.

Comisia Europeană. Cadrul de competențe digitale 2.0. EU SCIENCE HUB. [Online] 9 ianuarie 2019. https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework.

Îngrijire, Departamentul de Sănătate și Social. Angajează-te. Pașaport digital. [Online] https://engage.dhsc.gov.uk/digitalpassport/tools/.

Google. Google. Google Drive. [Online] Google. https://support.google.com/drive/answer/2424384?hl=ro&co=GENIE.Platform%3DDesktop.

Comisia Europeană. Europa. Transformarea cetățeniei digitale. [Online] Comisia Europeană. https://epale.ec.europa.eu/en/blog/digital-citizenship-transformation.

Bun simț. Tot ce aveți nevoie pentru a preda cetățenia digitală. [site web] sl : Common Sense, 2021.

Guvernul australian. Comisar eSafety . Ghidul cetățenilor digitali. [Online] https://www.esafety.gov.au/media/2563.

Liveworkstudio.trăiesc|muncă. Relații digitale. [Online] https://www.liveworkstudio.com/themes/organisational-change/digital-relationships/.

Eferin, Kate Gromova și Yaroslav. Blogurile Băncii Mondiale. Etica în lumea digitală: unde suntem acum și ce urmează. [Online] 9 aprilie 2021. https://blogs.worldbank.org/opendata/ethics-digital-world-where-we-are-now-and-whats-next.

Zwerdling, Daniel. NPR. Traseul tău digital și cum poate fi folosit împotriva ta. [Online] 2013. https://www.npr.org/sections/alltechconsidered/2013/09/30/226835934/your-digital-trail-and-how-it-can-be-used-against-you.

Universitatea din Alabama din Birmingham. Blogul Institutului UAB pentru Drepturile Omului. Cetățenia digitală: binele, răul și rolul internetului. [Online] ianuarie 2019. https://sites.uab.edu/humanrights/2019/01/18/digital-citizenship-the-good-the-bad-the-role-of-the-internet/.

Biblioteca BYU:

- 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

Acest proiect a fost finanțat cu sprijinul Comisiei Europene. Această publicație reflectă doar punctul de vedere al autorului, iar Comisia nu poate fi făcută responsabilă pentru orice utilizare care poate fi făcută a informațiilor conținute în ea.

Proiectul nr. º 2020-1-RO01-KA204-079988