No One Behind

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

Il presente progetto è finanziato con il sostegno della Commissione Europea. L'autore è il solo responsabile di questa pubblicazione e la Commissione declina ogni responsabilità sull'uso che potrà essere fatto delle informazioni in essa contenute. (Progetto n. º 2020-1-RO01-KA204-079988)

No One Behind

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

Manuale di formazione del cittadino "digitalmente competente"

Programma Erasmus Plus – Partenariato Strategico per l'Educazione degli Adulti KA2

Composto da:

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* | agosto 2021

Partenariati

North-East Regional Development Agency - NERDA, Romania
Lucian Alexa e Olivian Secara
Sito web: https://www.adrnordest.ro/en/homepage/

Eurocrea Merchant, SRL, Italia
Beatrice Del Nero
Sito web: http://www.eurocreamerchant.it/

INOVA+ - Innovation Services S.A., Portogallo
Andreia Monteiro e Sara Correia
Sito web: https://inova.business/

ECO LAND, Romania
Ciprian Barsan
Sito web: https://www.facebook.com/AdlEcoLand/

IDEC, Grecia
Rafaela Paspati and Lila Anthopoulou
Sito web: https://idec.gr/

European E-learning Institute – EUEI, Danimarca
Canice Hamill e Catherine Neill
Sito web: https://www.euei.dk/

ATERMON, Paesi Bassi
Anna Stamouli
Sito web: https://www.atermon.nl/

INDICE

INDICE DELLE FIGURE

INDICE DELLE TABELLE

ABBREVIAZIONI

EQF	Quadro Europeo delle Qualifiche[1]
ECVET	Sistema Europeo di Crediti per l'Istruzione e la Formazione Professionale[2]

[1] European Qualification Framework

[2] European credit system for vocational education and training

No One Behind

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

SOMMARIO ESECUTIVO

Il ***manuale di formazione del cittadino digitalmente competente*** è stato sviluppato nell'ambito del progetto ***No One Behind*** per guidare educatori e discenti attraverso un facile percorso al fine di promuovere le competenze digitali negli adulti provenienti da aree rurali.

Questa guida fornisce un programma formativo e dei materiali per supportare gli educatori di adulti (e altri stakeholder) nello sviluppo di competenze digitali negli adulti provenienti da aree rurali, permettendo loro di diventare "cittadini digitalmente competenti".

Il programma formativo è stato creato sulla base del profilo del **cittadino digitalmente competente**, progettato dal Consorzio in conformità con i principi del Sistema Europeo di Crediti per l'Istruzione e la Formazione Professionale (ECVET)[3] e del Quadro Europeo delle Qualifiche (EQF)[4].

In termini di struttura e contenuti, il programma e i materiali sono correlati con il DigComp – *European Digital Competence Framework for citizens*. Il manuale contiene 5 moduli formativi che ricoprono 21 competenze digitali:

- Informazioni e *data literacy*
- Comunicazione e collaborazione
- Creazione di contenuti digitali
- Sicurezza
- *Problem solving*

Per ogni modulo, il manuale fornisce:

- Una panoramica degli obiettivi, dei contenuti e della struttura da seguire da parte di studenti e educatori;
- Programmi specifici, attività e risorse relative alle unità di competenza individuate in ogni modulo promuovendo lo sviluppo e il consolidamento delle competenze digitali negli adulti.

In questo documento sono presenti anche una serie di griglie al fine di supportare la valutazione relativa al grado di sviluppo delle competenze digitali negli adulti provenienti da aree rurali, da effettuare prima e dopo la formazione.

[3] *European Qualification Framework*: maggiori informazioni disponibili qui.
[4] *European credit system for vocational education and training*: maggiori informazioni disponibili qui.

No One Behind

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

INTRODUZIONE

1. Introduzione al manuale di formazione di *No One Behind*

Questo manuale di formazione è il risultato di un lavoro congiunto da parte di diverse organizzazioni con lo scopo di creare una guida, passo dopo passo, al fine di promuovere competenze digitali all'interno di gruppi di persone che vivono in zone rurali e favorire l'inclusione sociale rafforzando le competenze digitali. Le unità e i contenuti sono organizzati in modo che il manuale possa essere usato da autodidatta ma anche come uno strumento per gli educatori che desiderino fornire un'istruzione sulle competenze digitali per le persone che ne hanno davvero poche.

A chi si rivolge questo manuale?

Educatori di adulti: operatori sociali, insegnanti, tutor, professori e altri professionisti che lavorano con gli adulti;

Adulti provenienti da zone rurali che vogliono migliorare la loro vita quotidiana, cambiare lavoro o trovare nuove opportunità sviluppando competenze digitali utili.

Lo scopo di questo manuale è di guidare educatori e studenti attraverso un innovativo e facile percorso al fine di promuovere le competenze digitali, seguendo le linee guida del quadro *DigComp*.

Il manuale è organizzato in quattro sezioni principali, come segue:

- **Sommario esecutivo**: una sintesi dei contenuti che può essere utilizzata per introdurre l'argomento ai gruppi destinatari e ai social media.
- **Introduzione**: una breve introduzione al manuale di formazione con inclusa una panoramica generale del profilo del cittadino "digitalmente competente" presentato nella *Metodologia*[5].
- **Profilo del cittadino digitalmente competente**: comprende 5 capitoli che corrispondono ai 5 moduli di formazione. Ogni capitolo fornisce informazioni circa la struttura del modulo e le corrispondenti unità di competenza. Fornisce anche linee guida e materiali al fine di supportare il perfezionamento della formazione e l'acquisizione/potenziamento delle competenze digitali degli studenti.
- **Valutazione della formazione**: questa sezione fornisce indicazioni legate alla valutazione delle competenze digitali e all'apprendimento dei discenti, garantendone gli adeguati supporti. Fornisce anche un supporto per la valutazione della formazione da parte degli studenti.

In questo documento vengono anche fornite diverse appendici per supportare il perfezionamento della formazione, tra cui:

- Appendice I – Risorse supplementari: con collegamenti relativi ai moduli e alle unità di competenza inclusi in questo manuale di formazione, accessibili da educatori e studenti per saperne di più.
- Appendice II – Scheda di valutazione Modulo 1: una griglia di valutazione da usare per misurare il livello di sviluppo delle competenze digitali degli studenti su *informazioni e data literacy*.

[5] L'intera presentazione del profilo è disponibile nel documento *Metodologia innovativa per educare e formare gli adulti delle zone rurali per migliorare le loro competenze digitali e ICT.* Consultabile qui.

- Appendice III – Scheda di valutazione Modulo 2: griglia di valutazione, da usare per misurare il livello di sviluppo delle competenze digitali degli studenti, riguardante *Comunicazione e Collaborazione*.
- Appendice IV – Scheda di valutazione Modulo 3: griglia di valutazione, da usare per misurare il livello di sviluppo delle competenze digitali degli studenti, relativa alla *creazione dei contenuti*.
- Appendice IV – Scheda di valutazione Modulo 4: griglia di valutazione, da usare per misurare il livello di sviluppo delle competenze digitali degli studenti, relativa alla *Sicurezza*.
- Appendice V – Scheda di valutazione Modulo 5: griglia di valutazione, da usare per misurare il livello di sviluppo delle competenze digitali degli studenti, riguardante il *Problem Solving*.
- Appendice VI – Valutazione del programma formativo: griglia di valutazione relativa alla qualità e alla validità del corso da parte dei discenti.

2. Profilo del cittadino "digitalmente competente"

Dietro al corso di formazione introdotto dal presente manuale troviamo il profilo del cittadino "digitalmente competente" descritto nel seguente schema (figura 1):

Cittadino digitalmente competente

PANORAMICA

Livello EQF[6]

3

Crediti EQF: 5

Descrizione: il cittadino "digitalmente competente" sarà in grado di:

- Capire l'utilità delle competenze digitali.
- Usare i principali sistemi digitali nella vita quotidiana.
- Capire i rischi e le possibili minacce collegate al mondo di Internet.
- Capire come interagire con gli altri e usare le tecnologie per accedere ai servizi.

STRUTTURA GENERALE

N.	Modulo	Durata	Crediti
1	Informazioni e *data literacy*	25h	1
2	Comunicazione e collaborazione	25h	1
3	Creazione di contenuti digitali	25h	1
4	Sicurezza	25h	1
5	*Problem Solving*	25h	1

Figura 1: Panoramica generale e struttura del profilo del Cittadino Digitalmente Competente, come definito dal Consorzio in accordo con l'ECVET[7].

Ogni modulo è suddiviso in unità di competenza, fondamentali al fine di guidare educatori e discenti nell'acquisizione, lo sviluppo e il consolidamento delle competenze digitali (figura 2).

[6] *European Qualification Framework*: maggiori informazioni disponibili qui.

[7] *European credit system for vocational education and training*: maggiori informazioni disponibili qui.

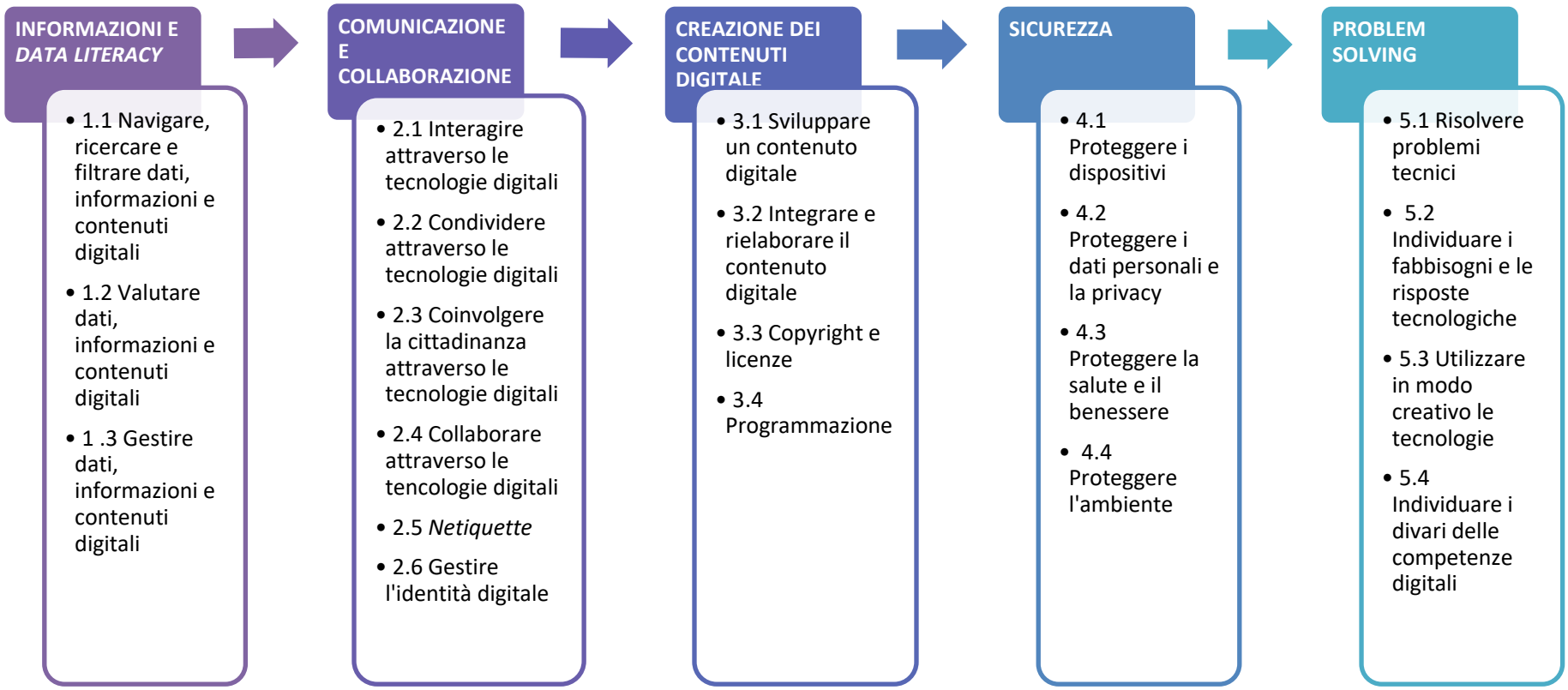


Figura 2: Individuazione delle unità di competenza corrispondenti ai moduli del profilo del cittadino digitalmente competente.

Le presenti unità di competenza sono descritte nel documento *Metodologia innovativa per educare e formare gli adulti delle zone rurali per migliorare le loro competenze digitali e ICT*[8].

[8] Consultabile qui.

No One Behind

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

CURRICULUM DEL CITTADINO DIGITALMENTE COMPETENTE

Questa sezione è dedicata al curriculum del **Cittadino digitalmente competente** in cui avrai accesso a:

- Una panoramica generale della struttura del curriculum;
- Una breve presentazione dei 5 moduli contenenti il curriculum;
- Programmi specifici, attività e risorse relative alle unità di competenza individuate in ogni modulo, promuovendo lo sviluppo e il consolidamento delle competenze digitali negli adulti.

La tabella 1 presenta la struttura generale del curriculum del **Cittadino digitalmente competente** come strutturato nel campo del progetto *No One Behind*:

Corso di formazione	**Cittadino digitalmente competente**
Durata	125h
Modalità	Combinazione di lezioni frontali, sessioni online e studio autonomo.
Organizzazione della formazione	Apprendimento misto con lezioni frontali accompagnate da sessioni online.
Principali obiettivi	Il presente manuale ha lo scopo di diventare un punto di riferimento per gli educatori durante il lavoro con gli adulti con poche competenze digitali. Per raggiungere questo obiettivo, il manuale comprende contenuti teorici e attività pratiche al fine di favorire l'apprendimento. Il presente manuale ha come obiettivo quello di supportare principianti e adulti a migliorare le loro competenze digitali, fornendo attività passo dopo passo.
Piano di formazione	Questo corso è suddiviso in 5 moduli: • Modulo 1 - Informazioni e *data literacy* (25h) • Modulo 2 - Comunicazione e collaborazione (25h) • Modulo 3 - Creazione di contenuti digitali (25h) • Modulo 4 - Sicurezza (25h) • Modulo 5 - *Problem solving* (25h)
Valutazione dell'apprendimento	Schede di valutazione per ogni modulo e unità (fornite alla fine del manuale)
Valutazione della formazione	Schede di valutazione (fornite alla fine del manuale)

Tabella 1: Curriculum del corso di formazione del cittadino digitalmente competente.

Come si può vedere, il corso è organizzato in 5 moduli, ognuno con uno scopo preciso, e diviso in unità di competenza mostrate nella tabella 2:

Modulo 1 **Informazioni e *data literacy***	
Questo modulo introduce gli strumenti e le competenze necessarie ad effettuare ricerche online, fornendo diverse strategie e tecniche utili al fine di trovare informazioni affidabili. Entro la fine di questo modulo, i discenti dovrebbero aver imparato a gestire le informazioni e a salvarle su dispositivi tecnologici essendo consapevoli delle regole vigenti sul copyright e sulla protezione dei dati.	1.1. Navigare, ricercare e filtrare dati
	1.2. Valutare dati, informazioni e contenuti digitali
	1.3. Gestire dati, informazioni e contenuti digitali
Modulo 2 **Comunicazione e collaborazione**	
In questo modulo, i discenti svilupperanno competenze e abilità per relazionarsi con gli altri usando tecnologie digitali. Saranno in grado di interagire e condividere informazioni, conoscendo la netiquette e l'identità personale online.	2.1. Interagire attraverso le tecnologie digitali
	2.2. Condividere informazioni attraverso le tecnologie digitali
	2.3. Coinvolgere la cittadinanza attraverso le tecnologie digitali
	2.4. Collaborare attraverso le tecnologie digitali
	2.5. *Netiquette*
	2.6. Gestire l'identità digitale
Modulo 3 **Creazione di contenuti digitali**	
L'obiettivo di questo modulo è quello di promuovere competenze riguardanti il contenuto digitale e la programmazione, in modo che i discenti si sentano sicuri nella promozione del proprio business online.	3.1. Sviluppare contenuti digitali
	3.2. Integrare e rielaborare i contenuti digitali
	3.3. Copyright e licenze
	3.4. Programmazione
Modulo 4 **Sicurezza**	
Una volta completato questo modulo, i discenti dovranno essere consapevoli delle azioni che possono intraprendere per proteggere i dispositivi, la loro salute e l'ambiente mentre usano la tecnologia. Questo modulo ha anche lo scopo di aumentare la consapevolezza per quanto riguarda la privacy e i dati personali.	4.1. Proteggere i dispositivi
	4.2. Proteggere i dati personali e la privacy
	4.3. Proteggere la salute e il benessere
	4.4. Proteggere dell'ambiente
Modulo 5 ***Problem solving***	
Questo modulo evidenzia i problemi tecnici e le strategie per gestire i problemi più comuni quando si usa un computer. Inoltre, i discenti avranno la possibilità di pensare a metodologie creative durante l'utilizzo di strumenti digitali.	5.1. Risolvere problemi tecnici
	5.2. Individuare i fabbisogni e le risposte tecnologiche
	5.3. Utilizzare in modo creativo le tecnologie digitali
	5.4. Individuare i divari delle competenze digitali

Tabella 2: Breve descrizione e individuazione delle unità di competenza di ogni modulo del manuale di formazione.

Seguendo la presente struttura, in questa sezione puoi trovare cinque capitoli, corrispondenti ai moduli del curriculum. All'inizio di ogni capitolo, avrai una tabella con una panoramica circa la durata, gli obiettivi e le unità trattate nel modulo. Segue una presentazione delle unità di competenza in termini di durata, obiettivi, contenuti, risorse e metodologie di formazione e le modalità di erogazione del modulo. Per ogni unità troverai sia informazioni teoriche sia attività pratiche, in modo che l'esperienza di apprendimento risulti facile e, possibilmente, favorisca un approccio "pratico". Inoltre, nel manuale vengono suggerite diverse attività che utilizzano metodologie di apprendimento differenti, come:

Metodo	Descrizione
Presentazione dell'educatore	Partecipazione dei discenti a lezioni basate su presentazioni *PowerPoint*, visione di video, dimostrazioni, ricerche, libri, giornali o altre risorse e supporti mostrati dagli educatori attraverso sessioni di formazione o piattaforma *e-learning*. Possono essere usati maggiori supporti (casi studio, compiti e quiz) in modo da permettere il consolidamento delle competenze e un incremento delle conoscenze.
Esercizio di gruppo Discussione / Dibattito	Può essere svolto in gruppi grandi o piccoli e l'idea è quella di promuovere la discussione o il dibattito tra i discenti per quanto riguarda temi specifici proposti dall'educatore. La discussione o il dibattito dovrebbero essere monitorati al fine di permettere la partecipazione di tutti i discenti e una maggior concentrazione sui temi più rilevanti. Alla fine della discussione o del dibattito è importante delineare e condividere alcune conclusioni.
Lavoro a coppie / Piccoli gruppi	L'educatore dovrà fornire ad ogni gruppo informazioni esatte circa i temi, i risultati derivanti dal lavoro di gruppo previsti (anche il metodo di presentazione dei risultati – al gruppo dovrebbe essere chiaro chi presenterà questi risultati all'inizio del lavoro) e la durata del lavoro di gruppo. Prima di iniziare l'esercizio, l'educatore e tutti i discenti guardano l'orario e l'educatore dice agli studenti quando dovranno riunirsi in un solo gruppo per evitare incomprensioni. Durante il lavoro in gruppo l'educatore coadiuva tutti i gruppi e controlla l'orario.
Presentazioni dei partecipanti	Gli educatori possono mettere alla prova gli studenti chiedendo loro di preparare una presentazione su un determinato argomento moderando la sessione di formazione. Gli studenti possono scegliere il formato della presentazione (PowerPoint, attività, video…) e coinvolgere gli altri studenti in momenti diversi della presentazione.
Simulazioni / giochi di ruolo	Il gioco di ruolo è un metodo di apprendimento in cui i discenti impersonano ruoli di personaggi e insieme creano storie. Questa tecnica rappresenta uno strumento eccellente per coinvolgere i discenti permettendo loro di interagire con i colleghi cercando di completare i compiti loro assegnati in uno specifico ruolo. Questo lavoro può essere svolto in gruppi e/o i discenti possono mantenere lo stesso ruolo durante tutto il periodo di lezione. Gli studenti si sentiranno più coinvolti nel momento in cui proveranno ad intervenire sui materiali dalla prospettiva del loro personaggio.
Apprendimento basato su progetto (PBL)	Il PBL è un metodo di insegnamento basato su progetti o attività integrate. Partendo da un problema concreato, ai discenti è richiesto di sviluppare progetti che rispondano a problemi della vita reale, permettendo loro di essere coinvolti attivamente nell'attività di apprendimento, imparare facendo e acquisire/rinforzare le loro abilità.
Apprendimento cooperativo	Questa metodologia è basata sulla discussione: un piccolo gruppo di discenti discute su un tema fornito dall'educatore. I ruoli da assegnare ai discenti sono perlopiù tre: 1) il segretario prende appunti sul dibattito in modo che tutti i partecipanti possano essere coinvolti nella conversazione; 2) l'assistente segue chi sta parlando e quando lo fa e delinea l'evoluzione della conversazione; 3) il moderatore si accerta che la conversazione non rimanga ferma sullo stesso argomento per troppo o troppo poco tempo e che ognuno prenda la parola. I formatori intervengono solo quando è necessario.
Insegnamento capovolto	Si tratta di un approccio pedagogico in cui si invertono gli elementi tradizionali di una lezione impartiti dall'insegnante: il materiale didattico base viene studiato a casa dai discenti e messo in pratica durante le sessioni.
Stazioni di apprendimento	Con l'aiuto delle stazioni di apprendimento, il contenuto è processato individualmente ed è adeguato alle esigenze. L'educatore prepara una stazione di apprendimento per ogni componente di utilizzo per i quali nuovi incarichi e materiale da lavoro sono disponibili. I discenti possono scegliere le stazioni più interessanti e importanti in termini di contenuto e di utilizzo personale. L'educatore è sempre disponibile per rispondere alle domande. I discenti prendono appunti e, in seguito, avranno accesso a materiali ed esempi di tutte le stazioni. Possono scegliere il proprio percorso di apprendimento stazione per stazione.

Tabella 3: Individuazione e breve descrizione dei metodi presi in considerazione nel presente manuale.

Modulo 1: Informazioni e *data literacy*

Il primo modulo ti mostra le procedure di ricerca online, con un focus sul modo in cui valutare, archiviare, reperire le informazioni e usarle in maniera responsabile.

Si prega di notare come le unità descritte possano prevedere il supporto di un docente esperto. Nonostante le informazioni presenti nel manuale siano scritte in maniera da comprenderle facilmente, alcune azioni, inerenti alle informazioni presentate, potrebbero richiedere la supervisione e il supporto di esperti.

Modulo 1	**Informazioni e *data literacy***		
Durata	25h		
Obiettivi	Ricercare informazioni affidabili online usando diversi browser e motori di ricerca Effettuare ricerche online in modo sicuro e protetto Identificare possibili *fake news* e informazioni ingannevoli sui siti web Organizzare, archiviare e reperire informazioni.		
Unità	1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali	1.2 Valutare dati, informazioni e contenuti digitali	1.3 Gestire dati, informazioni e contenuti digitali
Organizzazione della formazione	Lezioni frontali *E-learning*	Lezioni frontali *E-learning*	Lezioni frontali *E-learning*
Durata	9h	8h	8h

Tabella 4: Struttura generale Modulo 1: Informazioni e data literacy.

1.1. Navigare, ricercare e filtrare dati

Unità 1.1	Navigare, ricercare e filtrare dati, informazioni e contenuti digitali
Durata	9 ore
Obiettivi	• Usare diversi browser e motori di ricerca per ricerche online; • Effettuare ricerche online su uno specifico argomento, selezionare fonti affidabili di informazione; • Identificare siti web sospetti e disinformazioni; • Salvare e reperire dati quali documenti, immagini, siti web; • Gestire l'ambiente digitale considerando impostazioni privacy e riservatezza.
Contenuti	1.1.1 Concetti principali: IT, ICT e Internet 1.1.2 Introduzione alla ricerca online 1.1.3 Protezione durante l'utilizzo dell'ICT 1.1.4 Attività pratiche
Risorse	Manuale di formazione Computer con accesso alla rete Lavagna a fogli mobili Pennarelli Casi studio 1 e 2
Metodo di formazione	• Presentazione da parte dell'educatore • Discussione/dibattito di gruppo • Lavoro a coppie/piccoli gruppi • Presentazione da parte dei partecipanti

Tabella 5: Struttura dell'unità di competenza 1.1. Navigare, ricercare e filtrare dati del Modulo 1 (Informazioni e data literacy).

1.1.1. Concetti principali: IT, ICT e Internet

Per presentarti questo modulo, vorremmo introdurre due concetti base che sentirai spesso quando si parla di tecnologie informatiche:

IT (*Information Technology*): comprende le tecnologie che usiamo per raccogliere, processare, proteggere e archiviare le informazioni. Fa riferimento a hardware, software (programmi informatici) e reti informatiche.

ICT (*Information and Communication Technology*): questo concetto comprende il trasferimento e l'utilizzo di ogni genere di informazione. L'ICT sta alla base dell'economia.

> **Nota bene:**
> L'ICT include tutti i mezzi tecnici usati per gestire informazioni e facilitare la comunicazione, compresi computer, hardware di rete, line di comunicazione e tutti i software necessari. In altre parole, l'ICT è composto da: informatica, telefonia, mezzi di comunicazione elettronici e tutti i tipi di processo e trasferimento di segnali audio e video, e tutte le funzioni di controllo e gestione basate su tecnologie di rete.

Internet

Internet ("reti interconnesse") è un sistema globale composto da computer interconnessi e reti informatiche, che comunicano per mezzo di protocolli TCP/IP. Nonostante agli inizi sia nato dal semplice bisogno di scambiare dati, oggi ha un impatto su tutti i settori della società, ad esempio:

- **Economia**: Internet banking (pagamento bollette, trasferimento fondi, accesso al conto, accesso al debito…), commercio elettronico (azioni, merci, servizi intellettuali…), eccetera…
- **Socializzazione**: social network, forum…
- **Informazione**: portali news, blog…
- **Salute**: diagnosi di malattie, visite mediche (per persone che vivono su isole o in zone remote, alcuni accertamenti che richiedono uno specialista, tutto da remoto), presa di appuntamenti per visite mediche, scambio di dati sulla salute tra ospedali e Istituti, chirurgia e monitoraggio di interventi a distanza.
- **Istruzione**: università online attraverso *webinar* (*web* + *seminar*), siti web con tutorial, consulenze di esperti, esercitazioni online…

Internet ha davvero diversi campi di applicazione e un importante impatto sociale. Forse, la caratteristica più importante è lo scambio di informazioni, perché questo favorisce la collaborazione tra persone. La collaborazione tra persone affini porta a idee e azioni concrete e, azioni coordinate di persone portano al cambiamento sociale. **Ora che hai imparato qualcosa in più sulla tecnologia e sul potenziale di Internet nel cambiare il mondo, prenditi un momento per pensare al modo in cui questo possa avere un impatto su di te e sulla tua vita personale.**

Ora ti starai chiedendo: “ok, l’idea di connettersi con gli altri è davvero facile e sembra stupenda, ma… come uso questi strumenti?”. Questo è il primo argomento del presente manuale: fare ricerca online e imparare a navigare, ricercare e filtrare i dati.

1.1.2. Introduzione alla ricerca online

L’abilità di cercare informazioni online è una delle competenze più importanti che tu possa avere circa l’alfabetizzazione digitale. Ti permette di trovare velocemente quello che stai cercando senza dover setacciare pagine e pagine di risultati irrilevanti. Lo strumento più importante di questo processo è il motore di ricerca, che è un sito specializzato che ricerca informazioni su Internet. Sicuramente avrai sentito parlare dei più popolari, inclusi Google, Yahoo!, e Bing che, nonostante siano tutti utili, possono mostrare risultati diversi.
Google è, tra tutti, il più famoso motore di ricerca. È così popolare che è stato creato un verbo di uso comune, come quando qualcuno dice: “Sto googlando l’indirizzo, proprio ora”.

Come iniziare a cercare

Per far partire una ricerca dovrai cliccare su un **browser**. Un browser è un software che permette agli utenti digitali di trovare e visualizzare informazione su Internet. I browser disponibili per gli utenti sono diversi: Internet Explorer, Mozilla’s Firefox e Chrome sono solo alcuni di questi e, normalmente, li trovi nella barra delle applicazioni del tuo desktop.

Figura 3: Icone di alcuni browser.

Poi vai sulla pagina iniziale del motore di ricerca, per esempio **google.com**, e digita i tuoi termini di ricerca nella casella di testo. Per vedere i tuoi risultati puoi premere il tasto invio oppure cliccare su un’icona, come il pulsante di ricerca Google o la lente di ingrandimento.

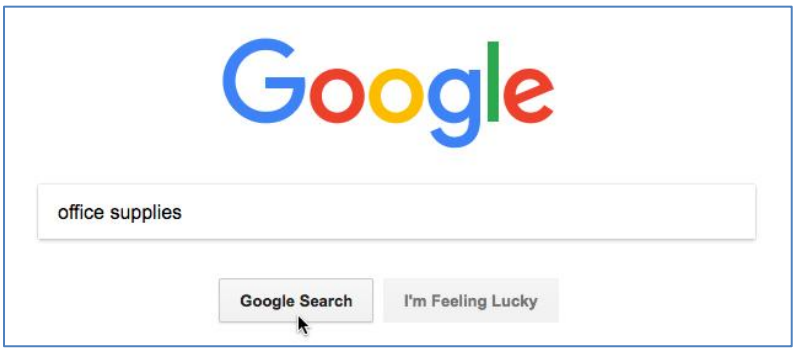


Figura 4 – Home page di Google.

In base al tuo browser, potresti essere in grado di fare una ricerca direttamente dall'interfaccia dello stesso. Ad esempio, in Chrome, puoi inserire i tuoi termini di ricerca direttamente nella barra di indirizzo. In Internet Explorer (figura in basso), per iniziare a ricercare, puoi usare sia la barra di indirizzo sia la barra di ricerca integrata.

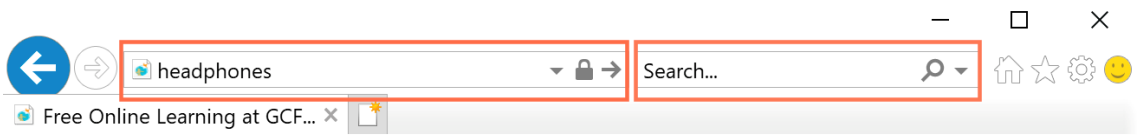


Figura 5: Home page di Chrome.

Strategie di ricerca

Con poche strategie base di ricerca, puoi sempre trovare quasi tutto quello che vuoi. Queste tecniche funzionano ovunque, non importa se stai usando Google o altri motori di ricerca.

- **Semplicità:** fai delle piccole ricerche concentrandoti su parole chiave, e tieni il numero di queste parole chiave al minimo. Facendo così sarà più facile ottenere risultati rilevanti.
- **Valuta i suggerimenti:** quando digiti il termine i motori di ricerca ti suggeriranno i risultati più probabili che lo comprendono, quindi, non aver paura a selezionarne uno, perché molto spesso possono suggerirti tantissime nuove idee.
- **Usa un linguaggio naturale:** non devi utilizzare parole o frasi complicate per ottenere risultati. I motori di ricerca possono riconoscere il linguaggio naturale che usi nella tua vita quotidiana, quindi, sentiti libero di provare con qualsiasi cosa che ti viene in mente.

In base alla tua ricerca, la forma dei risultati può variare in base a ciò che il motore di ricerca crede essere più utile. Questo significa che i tuoi risultati potrebbero includere mappe, estratti di articoli di Wikipedia, liste e altro. I motori di ricerca possono trovare molti altri tipi di contenuti oltre alle pagine web. Con solo uno o due click puoi anche ricercare immagini, video, notizie e tanto altro.
Prima di iniziare la tua esperienza online vorremmo richiamare la tua attenzione su qualcosa di estremamente importante: **protezione online e impostazioni sulla privacy.**

1.1.3. Protezione durante l'uso dell'ICT

La protezione delle informazioni è definita come la salvaguardia della riservatezza, integrità e disponibilità delle informazioni.

Le misure di sicurezza delle informazioni sono le regole riguardanti la protezione dei dati a livello fisico, tecnico e organizzativo. L'autenticazione dell'utilizzatore prevede l'identificazione dello stesso, in modo che gli individui possano avere accesso ad un determinato contenuto (dati). Ad esempio, per controllare la tua posta elettronica sul browser (accesso ad un account) è necessario inserire username e password. Se le informazioni richieste vengono inserite correttamente l'accesso sarà autorizzato. Per motivi di sicurezza, le password dovrebbero rimanere riservate. Una password è una chiave (come quella per entrare in casa o in macchina) che permette l'accesso. Come non condivideresti mai il tuo appartamento o la tua macchina con chiunque, così dovresti fare con le password. Al giorno d'oggi molte persone hanno serrature difficili da copiare, con lo scopo di bloccare l'accesso a persone non autorizzare. Le password dovrebbero essere create con la stessa attenzione. Più complessa sarà la password, più difficile sarà ottenerla (craccarla), pertanto sarà meno probabile che qualcuno otterrà un accesso non autorizzato ai tuoi dati.

Per la scelta di una password si consiglia di usare punteggiatura, numeri e un mix tra lettere maiuscole e minuscole. È raccomandata una lunghezza minima di 8 caratteri (password più corte potrebbero essere scoperte). Di tanto in tanto è necessario cambiare password, così la possibilità di scoprirla diminuirà.

Alcuni degli errori più comuni durante la scelta di una password sono:

- Usare parole del dizionario
- Password basate su informazioni personali come nome, data di nascita, luogo di lavoro…
- Caratteri che seguono l'ordine della tastiera: 123, qwert…

Sicurezza del sito web: per vedere se un sito è affidabile puoi controllare le informazioni di sicurezza del sito:

- Se vedi l'icona del lucchetto di fianco all'indirizzo del sito significa che il traffico da e verso il sito è crittografato.

È anche verificato, ciò vuol dire che l'azienda del sito ha un certificato di proprietà. Selezionando l'icona del lucchetto puoi vedere maggiori informazioni sul sito, come chi lo possiede e chi lo ha verificato.
Se non vedi l'icona del lucchetto la tua connessione non è privata e il traffico potrebbe essere intercettato.

Figura 6: Identificazione dell'icona del lucchetto.

Informazioni personali: alcune cose da ricordare!

Devi stare attento alle informazioni personali che rendi pubbliche online. Condividere indirizzo, numero di telefono, compleanno e altre informazioni personali significa essere ad alto rischio di furto di identità, stalking e molestie. Sono comprese anche le informazioni che pubblichi sui social media.
I criminali informatici possono mettere insieme piccoli pezzi della tua identità grazie a informazioni personali di dominio pubblico; quindi, pensa a ciò che rendi disponibile online.

Qui di seguito ci sono, inoltre, alcune cose da considerare quando usi Internet:

- Utilizza indirizzi mail diversi per fare shopping, per gruppi di discussione e newsletter. Potrai così cambiare questo indirizzo senza interrompere le tue attività, nel caso di bisogno.
- Condividi il tuo indirizzo principale solo con le persone che conosci.
- Se usi i social media, regola le tue impostazioni sulla privacy per controllare la quantità e il tipo di informazioni che condividi.
- Quando crei un account prenditi il tempo di familiarizzare con le politiche sulla privacy dei social media.
- Effettua acquisti online solo con aziende che abbiano chiare politiche sulla privacy e opzioni di pagamento sicure.
- Pensa prima di compilare moduli online e stai attento con chi e in che modo condividi le tue informazioni. Chiediti: “Devo davvero fornire le mie informazioni a questo sito?”.

1.1.4. Attività pratiche

Dopo ogni descrizione teorica dei contenuti, ti suggeriamo alcune dinamiche di gruppo per migliorare l’apprendimento. Queste attività sono descritte passo dopo passo.

Durante l’insegnamento, gli educatori e i discenti dovrebbero sentirsi a proprio agio all’interno del gruppo in modo da condividere esperienze, domande... Più persone si sentiranno a proprio agio con i colleghi, migliore sarà l’esperienza di apprendimento. Inoltre, suggeriamo che ogni attività abbia inizio rompendo il ghiaccio, magari qualcosa di divertente che permetta alle persone di presentarsi al gruppo senza sentirsi a disagio.

Durante la fase di presentazione, l’educatore potrebbe invitare le persone a condividere ciò che vorrebbero imparare, quale animale vorrebbero essere, il piatto preferito, il colore dello spazzolino da denti e qualsiasi altra cosa di non troppo personale.

Step 1: Rompere il ghiaccio “Non sono l’unico”

Sparsi per l’aula si crea un cerchio chiuso. L’educatore spiega che verrà lanciata una pallina, a turno, ad ogni membro del cerchio. Chiunque abbia la pallina dovrà dire il proprio nome e una cosa che solo loro sanno o sanno fare all’interno del gruppo- Potrebbero anche parlare di squisiti interessi o gusti. Se una stessa persona all’interno del Gruppo condivide la stessa abilità la persona che ha parlato deve trovare una diversa peculiarità.

La pallina non deve seguire un ordine, quindi le persone potrebbero lanciare la pallina al gruppo, assicurandosi però che ognuno abbia la possibilità di parlare.

Puoi adattare questo step anche con un format online chiedendo alle persone di nominare un collega e parlare, invece di lanciare una pallina.

Step 2: *Brainstorming*

Per presentare il tema della ricerca online, ma anche per avere un'idea generale del livello di conoscenza generale delle persone, inizia questa unità con un brainstorming.

Fai in modo di avere una lavagna pronta per scrivere i contributi di ognuno. Se l'attività è svolta online, puoi usare una piattaforma (es. https://padlet.com) per registrare o addirittura condividere un documento word con il gruppo in cui puoi scrivere le loro parole.

Informa i partecipanti che non ci sono risposte giuste o sbagliate perché l'idea è quella di condividere con il gruppo ciò che già sappiamo o che potremmo non sapere. Possibili domande:

- Cos'è una ricerca online?
- In che modo questa conoscenza potrebbe aiutarci nella vita quotidiana?
- In che modo le informazioni finiscono su Internet?
- A quali rischi si può andare incontro effettuando ricerche online?

Step 3: Ricerca online – attività pratica!

Mostra ai partecipanti diversi tipi di browser: Google Chrome, Safari, Mozilla Firefox, Edge, Internet Explorer, spiegando loro che sono programmi per accede il *World Wide Web* e navigare attraverso diverse pagine. Mostra ai partecipanti dove trovare i browser su un computer. (10 minuti)

Per introdurre la questione sul modo in cui usare un motore di ricerca, puoi anche usare il seguente tutorial: https://edu.gcfglobal.org/en/Internetbasics/using-search-engines/1/

Gli insegnati mostrano come cercare "fertilizzante organico" (questo è un esempio, ma è consigliato scegliere un tema rilevante per il tuo gruppo). Mostra al gruppo come consultare diverse pagine e il modo in cui usare diversi "criteri di ricerca". (10 minuti)

A questo punto invita ogni partecipante a cercare informazioni online circa i pericoli delle fake news e scrivi i tre fatti più rilevanti che hanno trovato. (20 minuti)

Discussione di gruppo: ogni partecipante presenta i risultati della propria ricerca. (20 minuti)

Step 4: Analizzare, archiviare e presentare informazioni

Crea una lista di diversi argomenti da far cercare online ai partecipanti. Es. salute mentale durante la pandemia, le migliori ricette al mondo, sport estremi, l'importanza delle api, malattie degli alberi, rivoluzione industriale, robot e tecnologia, stile di vita salutare….

Chiedi al gruppo di dividersi in coppie e scegli un argomento su cui lavorare. L'obiettivo dell'attività è: 1) raccogliere informazioni affidabili sul tema scelto, 2) selezionare e salvare informazioni sul desktop (in una cartella creata dallo studente), 3) creare una breve presentazione (10 minuti) assicurandosi che abbiano usato fonti affidabili. I discenti dovrebbero riportare i siti web e la sitografia usati visto che questo sarà valutato alla fine.

Per gli studenti che non saranno in grado di usare un software per lavorare sulla presentazione, l'educatore dovrà fornire fogli e pennarelli. Anche se non usano il computer per presentare le informazioni, dovranno essere in grado di ricercare immagini, grafici o video per illustrare la propria ricerca e archiviare il tutto nella propria cartella sul desktop. (4 ore)

Una volta finita l'esercitazione, ogni gruppo dovrà presentare il lavoro ai colleghi. (90 minuti)

Step 5: Impostazioni sulla privacy online

Fornisci agli studenti i casi studio n. 1 e n. 2. Inoltre, potresti suggerire loro di guardare un tutorial veloce inerente a privacy e sicurezza su Chrome: https://www.youtube.com/watch?v=zMXI6waGFp4

- Dividi gli studenti in due gruppi in modo da lavorare su ogni caso. Devono leggere e rispondere alle domande, supportate da informazioni online sulla sicurezza informativa. (30 minuti)
- Ogni gruppo produrrà una scheda informativa[9], indicando i 10 step utili ad evitare violazioni della privacy mentre si utilizza Internet.
- Dibattito di gruppo (40 minuti)

[9] Gli studenti possono farlo sul computer o su un foglio, in base alle competenze digitali pregresse.

Caso Studio n. 1 - Jane

Leggi la seguente situazione, discuti all'interno del gruppo riguardo cosa è successo e rispondi alle domande sottostanti per guidare il dibattito. Poi, scrivi le conclusioni principali in modo da presentare le tue idee al gruppo.

"Jane si collega a Internet, per quella che sembrerebbe essere un'innocua e banale ricerca sul web; acquista alcuni vestiti per sé e per i suoi due figli di due e cinque anni sul sito web di un esclusivo grande magazzino. Continua con una ricerca approfondita su un sito web dedicato a piani per la perdita di peso. Nonostante molti considererebbero questa esperienza di navigazione come una sfilza di operazioni banali, uno scaltro direct marketer, abile nel monitorare velatamente queste attività, riterrebbe preziose le informazioni ottenute. Inaspettatamente, per troppi utenti del web delineare pericolosamente il profilo dettagliato di Jane, a sua insaputa o senza il suo consenso, è possibile con una singola attività di ricerca online come quella recentemente menzionata. Sebbene questa situazione richieda alcune inferenze, un profilo marketing delle operazioni di Jane potrebbe svilupparsi come segue: Jane è madre di due bambini piccoli, acquista alcuni beni esclusivi, ed è seriamente preoccupata per il suo peso e la sua salute. Basandosi sui suoi dati, un commerciante o venditore potrebbe voler inviare a Jane pubblicità, e-mail, banner o pop-up pubblicitari che offrano costose attrezzature sportive domeniche. L'attrezzatura le permetterebbe di stare a casa con i bambini, aiutandola a raggiungere i suoi obiettivi di fitness, a prezzi accessibili in base al suo modello di spesa. Una pubblicità sull'attrezzatura ginnica non infastidirebbe Jane, anzi, in realtà, potrebbe essere interessata ad attrezzature sportive domestiche piuttosto che ad una pubblicità casualmente sponsorizzata sul suo schermo durante la sua navigazione online. Tuttavia, Jane potrebbe essere molto infastidita dai mezzi nascosti usati dai venditori per raccogliere, unire, usare e/o vendere le sue informazioni personali senza il suo permesso o senza una richiesta del loro intento di utilizzare informazioni in questo senso.

Groemminger, B. K. (2003). *Personal privacy on the Internet: should it be a cyberspace entitlement*[10].

1) **Quali impostazioni della privacy o azioni potrebbe scegliere Jane per evitare che le sue informazioni vengano diffuse attraverso le società commerciali?** (qui di seguito le possibili risposte)
- Dovrebbe stare attenta ai *cookie*, dando il consenso solo a quelli necessari.
- Potrebbe cancellare la cronologia una volta finito o navigare in incognito (questo è particolarmente importante se si utilizza un computer pubblico).
- Deve disconnettersi dalla propria e-mail o da altri account a cui ha fatto accesso.

2) **Quali misure di sicurezza considereresti durante il tuo shopping online?** (qui di seguito le possibili risposte)
- Controlla la sicurezza del sito (verifica che la connessione sia sicura).
- Crea una carta virtuale con uno specifico importo di denaro.
- Usa piattaforme affidabili per i pagamenti, come Paypal.
- Assicurati di avere un antivirus e che il tuo computer sia sicuro
- Evita di usare una connessione pubblica durante il tuo shopping.

[10] Disponibile qui.

Caso Studio n. 2 - Mary

Leggi la seguente situazione, discuti all'interno del gruppo riguardo cosa è successo e rispondi alle domande sottostanti per guidare il dibattito. Poi, scrivi le conclusioni principali in modo da presentare le tue idee al gruppo.

Mary, ventiduenne, è molto competente in materia di social network, tanto da definirsi "un'influencer". Crede che un regolare esercizio fisico e una buona alimentazione siano i pilastri di una vita sana e scrive molti post e suggerimenti a riguardo, su Instagram. Ha appena raggiunto i 10000 follower e ne va molto fiera. Recentemente, alcuni le hanno scritto lamentandosi di essere stati vittima di attacchi informatici a causa di messaggi inviati a nome suo. All'inizio non è in grado di spiegarsi il motivo, ma dopo si è resa conto di essere stata hackerata. Due giorni prima aveva ricevuto un messaggio che la informava di aver vinto una competizione online. All'inizio trovava il messaggio un po' sospetto, in quanto non riusciva a riconoscere il mittente, ma dopo ha cliccato sul link e riempito il modulo con i suoi dati personali. Dopo aver visto che non vi era nessun premio si è accorta della truffa. Essendone a conoscenza ha poi postato un avviso sui social media informando tutti di non aprire messaggi provenienti da lei.

1) **Cos'altro avrebbe potuto fare Mary una volta accortasi dell'accaduto?** (qui di seguito le possibili risposte)
   - Resettare le password (e-mail, telefono, social media, *banking account*…) e renderle sicure (minimo 8 caratteri con lettere maiuscole, numeri…).
   - Assicurarsi che l'antivirus fosse aggiornato / avviare una scansione antivirus.
   - Eseguire un backup dei dati.
   - Portare il dispositivo ad un informatico.
2) **Cosa avrebbe potuto fare Mary per evitare questa situazione?** (qui di seguito le possibili risposte)
   - Avrebbe potuto controllare due volte il mittente e non aprire il messaggio/link se sospetti.
   - Avrebbe potuto controllare l'indirizzo del sito web e vedere se fosse indicato come pericoloso.
   - Non avrebbe dovuto fornire informazioni personali non essendo sicura di cosa si trattasse.

1.2. Valutare dati, informazioni e contenuti digitali

L'unità 2 tratta della valutazione delle informazioni e della verifica dell'attendibilità e delle fonti.

Unità 1.2	Valutare dati, informazioni e contenuti digitali
Durata	8 ore
Obiettivi	Analizzare e valutare l'attendibilità delle informazioni online. Intervenire al fine di valutare diverse forme di informazioni. Capire le responsabilità di ognuno durante la condivisione online di disinformazione. Essere consapevoli del modo in cui i valori personali e i giudizi influenzino la comprensione delle informazioni.
Contenuti	1.2.1 Come verificare fonti e informazioni online 1.2.2 Valutare le tue fonti 1.2.3 Valutare siti web 1.2.4 Siti web *fact-checking* 1.2.5 Attività pratiche
Risorse	Manuale di formazione, computer con accesso a Internet, tessere vero/falso
Metodo di formazione	Presentazione da parte dell'educatore Discussione/dibattito di gruppo Lavoro a coppie/piccoli gruppi Presentazione da parte partecipanti Selezione dei contenuti

Tabella 6: Struttura dell'unità di competenza 1.2 Valutare dati, informazioni e contenuti digitali del Modulo 1 (Informazioni e data literacy)

1.2.1. Come verificare fonti e informazioni online?

Raggiunta questa parte del manuale, avrai già un'idea chiara di quali informazioni puoi trovare online: praticamente tutto! Quest'affermazione introduce la prossima unità, dove imparerai il modo in cui valutare i dati, così da poter essere in grado di cercare fonti affidabili e, inoltre, contribuire alla condivisione di dati reali online.

Al contrario delle informazioni di giornali o tv, le informazioni disponibili su Internet non sono controllate in termini di qualità e precisione. Inoltre, è molto importante per il singolo utente dell'Internet valutare la fonte o l'informazione. Ricorda che quasi tutti possono pubblicare sul web quello che vogliono. Spesso è difficile determinare l'autore di fonti web, quindi **stabilire la correttezza delle tue fonti è una tua responsabilità**. Nonostante le principali risorse per fare ciò siano il tuo giudizio e il tuo pensiero, ci sono alcune azioni che possono aiutarti ad aumentare la probabilità di informazioni affidabili.

Poniti queste domande prima di usare materiale proveniente da Internet:

1. Chi è l'autore? L'autore è qualificato a scrivere sul tema? Nel caso in cui si tratti di un'organizzazione, è attendile? Ne ho sentito parlare?
2. Qual è lo scopo del sito? A quale pubblico è destinato?
3. Le informazioni e gli obiettivi linguistici sono imparziali e privi di espressioni emotive?
4. Le informazioni reali sono elencate in maniera tale da essere verificate?
5. Le informazioni sono supportate da prove?
6. Quanto datata è quest'informazione? A quando risale l'ultimo aggiornamento del sito web?

In ultimo, ma non per importanza… Attenzione alle tue emozioni!

Sii consapevole di come una minuzia abbia il potere cambiare il tuo stato emotivo. Questa non è solo una tecnica molto antica con lo scopo di attirare la tua attenzione, ma è anche stata usata come *clickbait* per la diffusione delle fake news. La nostra normale tendenza è di ignorare i bisogni di controllo quando reagiamo violentemente a un contenuto, e i ricercatori hanno scoperto che il contenuto che causa forti emozioni è il più diffuso sui social network (Matthew Shaer, 2014). Quindi, **leggi ciò che conta**!

1.2.2. Valutare le tue fonti

Nella tua ricerca di informazioni potresti affrontare la sfida di valutare le risorse cha hai individuato e selezionare quelle che reputi più appropriate per i tuoi bisogni. Esamina ogni fonte d'informazione che individui e valuta le fonti utilizzando i criteri seguenti, conosciuti anche come metodo **TAARP:**

T – *Timeliness* (attualità) Le tue risorse devono essere piuttosto recenti per il tuo argomento. Se il tuo documento è su un argomento quale la ricerca oncologica, vorrai le informazioni più recenti, ma su un tema come la Seconda Guerra mondiale le informazioni saranno state scritte con un intervallo di tempo maggiore.
A – *Authority* (competenza) L'informazione arriva da un autore o un'organizzazione che ha le competenze di parlare del tema? Le informazioni sono state visionate da esperti? (Puoi utilizzare *Ulrichsweb* per determinare se un giornale è controllato da esperti). Menzionano le loro qualifiche? Accertati che ci sia una documentazione sufficiente che possa aiutarti a determinare l'affidabilità della pubblicazione compresi note a piè di pagina, bibliografie, riferimenti o citazioni.
A – *Audience* (pubblico) Chi sono i lettori target e qual è lo scopo della pubblicazione? C'è differenza tra un giornale scritto per un pubblico generico e un giornale scritto per professore ed esperti di un settore.
R – *Relevance* (pertinenza) Questo articolo è pertinente al tema? Quali collegamenti si possono fare tra le informazioni presentate e la tua tesi? Leggere l'abstract o il riassunto dell'articolo, prima di effettuare il download, è il modo corretto di controllarne la pertinenza.
P – *Perspective* (prospettiva) Fonti faziose potrebbero essere utili a creare e sviluppare una discussione, ma accertati di trovare fonti che ti aiutino a capire anche l'altro lato della questione. Fonti estremamente distorte possono spesso presentare male le informazioni e questo potrebbe essere inutile da usare nel tuo documento.

1.2.3. Valutare i siti web

I siti web generano una sfida intelligente nella valutazione della credibilità e dell'utilità perché nessuno sito web è creato allo stesso modo. Il metodo TAARP descritto pocanzi può essere usato, ma ci sono altri fattori che puoi considerare guardando un sito:

L'aspetto del sito web: i siti affidabili hanno un aspetto più professionale rispetto a siti personali.

L'URL dei tuoi risultati: .com, .edu, .gov, .net, e .org significano qualcosa e possono aiutarti a valutare il sito.

Le **risorse informative** sono quelle che presentano informazioni reali. Queste sono spesso sponsorizzate da istituzioni educative e agenzie governative. (Queste risorse spesso includono **.edu** o **.gov**)

Risorse *advocacy* sono quelle sponsorizzate da un'organizzazione che cerca di vendere idee o influenzare opinioni personali. (Queste risorse possono includere **.org** all'interno dell'URL)

Risorse di business e marketing sono quelle sponsorizzate da un'entità commerciale che cerca di vendere prodotti. Queste pagine sono spesso molto di parte, ma possono fornire informazioni importanti. (Spesso troverai all'interno di queste risorse **.com** nell'URL)

Risorse di news sono quelle che forniscono informazioni estremamente attuali su temi caldi. La maggior parte delle volte queste risorse non sono credibili come le riviste accadeche, è la credibilità dei giornali cambia da testata a testata. (L'URL includerà spesso **.com**)

Pagine web/risorse personali sono siti come social mead: blog, pagine Twitter, Facebook... queste risorse possono aiutarti a determinare cosa dicono le persone su un argomento e quali discussioni sono in atto. Sii cauto se cerchi di incorporare queste fonti in una documentazione accademica. Molto raramentehanno un peso nella comunica scolastica.

Ci sono pubblicità sul sito? Le pubblicità possono essere indice di informazioni meno affidabili.

Controlla i link nella pagina: link incorretti o parziali possono significare che nessuno si occupa del sito e che le informazioni potrebbero non essere aggiornate o non attendibili.

Controlla l'ultimo aggiornamento della pagina: le date di aggiornamento sono indizi utili riguardanti l'attendibilità e la precisione.

1.2.4. Siti web *fact-checking*

Fortunatamente, puoi anche usare siti web fact-checking, in cui puoi controllare meglio se l'informazione trovata è stata marcata come falsa. Inoltre, puoi chiedere ad un bibliotecario. Ecco una lista di alcuni siti web fact-checking (in base al tuo paese d'origine, potrebbe essere interessante trovare siti web fact-checking su notizie nazionali. Quelli che ti mostriamo sono per la maggior parte americani)

- FactCheck.org: https://www.factcheck.org/
- PolitiFact: trovare la verità nella politica: https://www.politifact.com/truth-o-meter/
- Urban Legends: politica - https://www.snopes.com/fact-check/category/politics/
- Truth or Fiction: https://www.truthorfiction.com/
- Observador Fact-Check (Portogallo): https://observador.pt/seccao/observador/fact-check/

1.2.5. Attività pratiche

Step 1: Vero o falso?

Per parlare del tema riguardante il modo di valutare la veridicità delle informazioni in cui ci imbattiamo online, inizia con un veloce gioco vero/falso. Dovrai prima preparare alcune tessere del vero/falso e dividere gli studenti in gruppi di tre. Presenterai alcune affermazioni sull'argomento e ogni gruppo dovrà mostrare la carta del vero/falso, secondo le loro risposte. Puoi correggere le risposte e aggiungere qualche informazione sui temi man mano che prosegui.

Lista di affermazioni:

	Affermazione	V/F
1	Tutte le informazioni pubblicate online sono affidabili.	Falso
2	Chiunque può aggiungere informazioni online, anche sulle enciclopedie.	Vero
3	Ci sono modi per controllare l'attendibilità delle informazioni.	Vero
4	C'è un fenomeno di "fake news" nel mondo.	Vero
5	Per individuare le fake news si potrebbe controllare il dominio web	Vero
6	Più una cosa è condivisa, maggiore è la possibilità che sia vera	Falso
7	Controllare la data della notizia non è qualcosa che vale la pena considerare	Falso
8	I valori personali possono influenzare la percezione della verità	Vero
9	Spesso è molto facile identificare una fake news	Falso
10	Sono disponibili siti web fact-checking	Vero

Tabella 7: Lista di affermazioni e risposte corrette.

Step 2: In che modo si diffonde la disinformazione?

Al fine di supportare l'apprendimento su come valutare i dati online, puoi presentare un breve video che mostri il modo in cui le fake news si diffondono.

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

Su questa scia, ogni studente potrebbe condurre la propria ricerca al fine di trovare **due notizie verosimilmente vere e due probabilmente false**. Considerata l'informazione data dall'educatore riguardo la valutazione dell'attendibilità dei dati, gli studenti dovranno usare alcune di queste strategie al fine di selezionare le informazioni ed essere in grado di spiegare ai colleghi le strategie utilizzate.

Step 3: Attività di storytelling

La seguente storia parla di due contadini che cercano di gestire la loro attività in un piccolo villaggio. Uno di loro è molto colto in materia di strumenti digitali ma l'altro non è molto bravo. La storia evidenzia il potenziale dell'uso di Internet per diffondere pettegolezzi e fake news. Lo scopo principale di questa storia è di suscitare pensieri personali su cosa sia una fake news e su come qualcuno possa facilmente suscitarlo ma anche quello di pensare all'impatto che queste possano avere sulla nostra vita quotidiana e a livello mondiale.

Inoltre, il nostro scopo è di favorire il dibattito sui vantaggi dell'Internet e su come questo possa essere utile per aiutarci nell'ottenimento rapido di informazioni, aiutandoci a connetterci con gli altri che, a loro volta, potrebbero essere in grado di aiutarci… Suggeriamo all'educatore di presentare la seguente storia:

C'erano due uomini in un piccolo villaggio: Robert e Peter. Entrambi lavoravano sodo per mandare avanti grandi fattorie e le proprie attività. Erano soliti parlare in maniera molto fieri dei prodotti venduti ai mercati viste le procedure sempre seguite al fine di garantire alti standard di qualità.

Peter e Robert sono sempre stati vicini e si conoscono da più di 10 anni ormai. Tuttavia, non possiamo dire che il loro rapporto sia sempre stato buono, vista la competizione per i regolari clienti del villaggio e della piccola città limitrofe. Credono che non sia posto per entrambe le attività in un'area così piccola.

In una delle sue passeggiate mattutine, Robert trova Peter molto preoccupato per le sue piantagioni, in quanto la sua lattuga è rovinata da quello che sembra essere una malattia. È turbato in quanto non si è accorto prima del problema e si lamenta del fatto che questa settimana non avrà lattuga da vendere al mercato cittadino. Si preoccupa anche per il fatto che, se i clienti scoprono l'accaduto, potrebbero considerarlo un incompetente, perdendo così fiducia riguardo la qualità dei suoi prodotti. Inoltre, non sa come gestire la malattia visto che sembra essere un virus del tutto nuovo mai visto prima.

Nel frattempo, Robert sta pensando che in realtà questo spiacevole evento potrebbe essere un'ottima possibilità per lui per affondare l'attività del vicino una volta per tutte! Quindi, decide di creare un profilo Facebook di un cliente fittizio che ha acquistato i prodotti di Peter e che è molto insoddisfatto. Per coprire ancora meglio la bugia, Robert ha trovato alcune immagini online e le ha aggiunte al profilo come se fossero

le foto dei prodotti "malati" di Peter. Poi ha iniziato a mandare richieste di amicizia alle persone del villaggio e molto velocemente il messaggio è stato diffuso.

Dopo qualche girono, Peter si rende conto che i suoi profitti sono scesi considerevolmente, anche durante la vendita dei prodotti non affetti dalla malattia. Tuttavia, non ha la minima idea di cosa Robert abbia fatto, alle sue spalle, su Internet…

Domande consigliate per il dibattito di gruppo:

- Perché pensi che il profitto di Peter abbia iniziato a calare?
- Se fossi un cliente di Peter, come pensi di sentiresti guardando immagini di lattuga andata a male? Continueresti a compare i suoi prodotti?
- Quanto pensi sia facile diffondere una diceria o cattive informazioni online?
- Considerando l'impatto che le fake news hanno avuto sull'attività di Peter, quale pensi possa essere il loro impatto su politica, ad esempio, o problemi relativi alla salute pubblica legati al Covid-19? Ti viene in mente qualche notizia riguardante il Covid-19 che hai sentito e che non fosse vera?
- Ora, immagina di essere nei panni di Peter… Avresti usato Internet per trovare una soluzione contro la mattia? In che modo?

1.3. Gestire dati, informazioni e contenuti digitali

Unità 1.3	Gestire dati, informazioni e contenuti digitali
Durata	8 ore
Obiettivi	Salvare e archiviare le informazioni usando dispositivi diversi Gestire, individuare e recuperare i dati Capire il *copyrighting* e le norme di *licensing* Essere consapevoli delle leggi in materia di protezione dei dati
Contenuti	1.3.1 Dispositivi per salvare e ripristinare le informazioni 1.3.2 Copyright e protezione dei dati 1.3.3 Attività pratiche
Risorse	Manuale di formazione, computer con accesso Internet, un cappello, fogli di carta, una scala di valutazione da 1 a 5 (puoi usare 5 fogli numerati da 1 a 5), fogli mobili, pasta adesiva o qualsiasi altro materiale per attaccare i fogli sul muro, pennarelli colorati, sedie, tavoli, un cucchiaio, un corno o qualsiasi oggetto che emetta un allarme sonoro. Se online, accesso ad una piattaforma di apprendimento collaborativo (es. LAMS, Padle).
Metodo di formazione	Presentazione da parte dell'educatore Discussione/dibattito di gruppo Lavoro a coppie/piccoli gruppi Presentazione da parte partecipanti Selezione dei contenuti

Tabella 8: Struttura dell'unità di competenza 1.3. Gestire dati, informazioni e contenuti digitali del Modulo 1 (Informazioni e data literacy).

1.3.1. Dispositivi per salvare e ripristinare le informazioni

Nelle ultime unità, hai imparato ad usare gli strumenti del computer al fine di navigare online, prendendo in considerato la tua sicurezza e la tua privacy. Abbiamo anche affrontato un tema molto importante che ti permette di essere un cittadino digitalmente responsabile durante la condivisione di informazioni tramite la valutazione della veridicità dei dati.

Il nostro obiettivo è quello di farti conoscere gli strumenti per salvare, archiviare e ripristinare le tue informazioni in qualsiasi momento tu voglia.

Nello stesso modo in cui tieni i tuoi vestiti in ordine nei cassetti, hai molte risorse, all'interno del tuo computer, per archiviare le informazioni. Qui di seguito te ne presentiamo alcune.

Memoria e dispositivi di archiviazione

La ROM (Read Only Memory) è un tipo di memoria interna e permanente, usata solo per la lettura.

La RAM (Random Access Memory) è una memoria oeprativa nella quale i dati analizzati e i programmi sono archiviati mentre il computer è in funzione. Permette di leggere e scrivere dati e, quando il computer viene spento, viene cancellata/pulita.

CD (Compact Disc) è un disco ottico utilizzato per l'archiviazione dai dati. La capacità standard di un CD è di 700MB. Il CD-R è usato per leggere e scrivere dati solo una volta, mentre il CD-RW per leggere e crivere dati più volte.

DVD (Digital Versatile Disc) è un disco ottico che, grazie ad una maggiore capacità (circa 4.7 GB), viene maggiormente usato per l'archiviazione dei video. BD (Blu-ray disc) il successore dei DVD, è un'unità di archiviazione su disco ottico, con diverse capacità, in base ai livelli che possiede e alle capacità di ogni livello.

La Scheda di memoria è un tipo di memoria istantanea utilizzata per archiviare i dati in fotocamere digitali, cellulari, MP3...

La chiavetta USB è un dispositivo di archiviazione dei dati. Ha piccole dimensioni, una capacità relativamente alta, affidabilità e velocità. Appartiene al tipo di memoria istantanea che memorizza i dati, anche quando non è sotto tensione, non hanno quindi bisogno di elettricità per mantenere i dati integri.

Figura 7: Identificazione e breve descrizione dei dispositivi di memoria e di archiviazione.

Per archiviare le informazioni esiste anche un dispositivo chiamato **disco rigido interno**, incorporato nel telaio del computer, e un **disco rigido esterno**, collegato al computer attraverso il corretto uso di un cavo o di una porta USB, ed è spesso usato per trasferire dati da un computer ad un altro oppure per il backup.

Quando si effettua il download delle informazioni da Internet, è importante ricordare che stiamo usando i lavori degli altri come articoli, libri, immagini, video, composizioni, videogiochi ecc. Inoltre, dobbiamo capire che i concetti di ***copyrighting*, *licensing*, e protezione dei dati**. Tuttavia, nell'era digitale, è stato difficile stabilire norme relative al copyright riguardanti le informazioni pubblicate online. Per fare un esempio, un social media come Facebook non possiede i lavori pubblicati sul sito web, tuttavia, devi accettare una licenza in cui Facebook può usare il tuo lavoro per altri scopi.

1.3.2. *Copyrighting* e protezione dei dati

Il **Copyright** è un diritto usato per proteggere la proprietà intellettuale dell'autore. Se qualcuno vuole usare un lavoro soggetto a copyright, quest'ultimo deve rispettare le condizioni con le quali l'autore, in qualità di proprietario, ha permesso l'uso del suo lavoro (pagamento di tasse, riferimenti all'originale…).

Protezione dei dati personali

La Carta dei Diritti Fondamentali dell'Unione Europea afferma che i cittadini europei hanno il diritto alla protezione dei dati personali.

"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano" e "ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica"[11]

La Commissione Europea ha presentato la riforma delle norme UE sulla protezione dei dati nel gennaio 2012 al fine di adattare l'Europa all'era digitale.

La **Direttiva 95/46/EC** è il testo di riferimento, a livello europeo, sulla protezione dei dati personali. Stabilisce un quadro normativo che ha lo scopo di trovare un equilibrio tra un elevato livello di protezione per la privacy degli individui e il libero movimento di dati personali all'interno dell'Unione Europea (UE). Per fare ciò, la direttiva stabilisce limiti severi riguardo la raccolta e l'uso dei dati personali e chiede che ogni Stato Membro stabilisca un organo nazionale indipendente responsabile della protezione dei suddetti dati. La Direttiva ha lo scopo di proteggere i diritti e le libertà delle persone rispettando il trattamento dei dati personali redigendo linee guida per determinare quando questi trattamenti siano legittimi. Le linee guida riguardano:

[11] Fonte: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en

La qualità dei dati

- I dati personali devono essere trattati in maniera imparziale e lecita, e raccolti per fini specifici, espliciti e legittimi. Devono inoltre essere accurati e, se necessario, aggiornati.

La legittimità del trattamento dei dati

- I dati personali possono essere trattati solo se l'interessato ha inequivocabilmente espresso il suo consenso o quando il trattamento sia necessario.

Categorie particolari di trattamento

- È vietato trattare dati personali attestanti orgini etniche o di razza, opinioni politiche, o credi religiosi o filifoci, l'appartenenza a sindacati e il trattamento dei dati riguardanti salute o vita sessuale. Questa disposizione comporta alcune abilitazioni riguardanti, ad esempio, casi in cui il trattamento è necessario al fine di proteggere interessi fondamentali dell'interessato o per scopi di medicina preventiva e diagnosi mediche.

Informazioni da fornire al soggetto interessato

- Il responsabile del trattamento deve fornire al soggetto interessato, dal quale i dati sono raccolti, informazioni riguardanti lo stesso (l'identità del resopnsabile del trattamento, gli scopi del trattamento, destinatari...).

Il diritto dell'interessato all'accesso ai dati

Ogni soggetto interessato dovrebbe avere il diritto ad ottenere dal responsabile del trattamento:

1. conferma del trattamento dei suoi dati e comunicazione della tipologia di dati sotto trattamento.
2. modifica, cancellazione o blocco dei dati sotto trattamento il cui processo non osservi le disposizioni della presente Direttiva in particolare, a causa della natura imprecisa o incompleta dei dati e comunicazione di queste modifiche a parti terze alle quali sono stati rivelati i dati.

Esenzioni e restrizioni

- L'obiettivo dei principi in materia di qualità dei dati, delle informazioni da fornire al soggetto interessato, del diritto all'accesso e della divulgazione del trattamento potrebbe essere limitato in modo da tutelare aspetti come la sicurezza nazionale, la difesa, la pubblica sicurezza o il perseguimento dei reati criminali.

Figura 8: Linee guarda sulla protezione dei dati personali stabilite dalla Direttiva 95/46/EC.

1.3.3. Attività pratiche

Step 1: Fai girare il cappello

Tutti si siedono in cerchio. Al centro del cerchio, l'educatore colloca una scala di gradimento da 1 a 5: può essere un foglio con i numeri scritti oppure 5 fogli, ognuno con un numero. Poi, l'educatore spiega che farà passare un cappello con dentro delle frasi. Queste frasi parlano di informazioni personali di persone reali che sono state pubblicate online. Ogni persona deve prendere un foglietto all'interno del cappello, leggerlo ad alta voce e collocarlo vicino ad un numero in cui 1 significa "questione non grave" e 5 "questione molto grave).

Possibili situazioni:

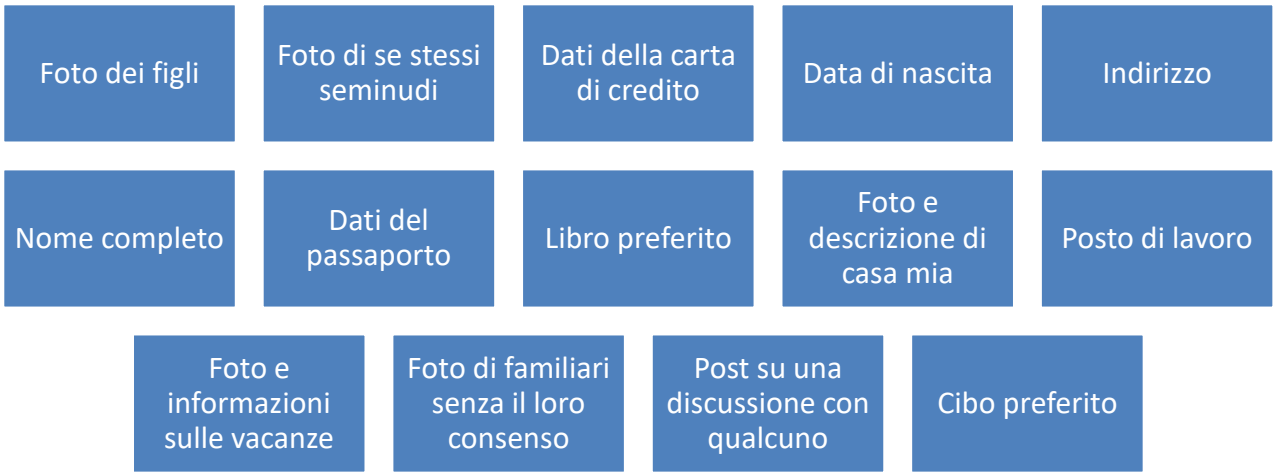


Figura 9: Individuazione di possibili situazioni da considerare durante questa attività

Questi sono solo alcuni esempi che puoi usare per iniziare la conversazione intorno alle informazioni personali che tutti condividono online, senza pensarci due volte.

Alla fine dell'attività, quando tutte le frasi hanno ricevuto una valutazione da 1 a 5, sarebbe interessante discutere su come le persone hanno valutato ogni situazione. Per esempio, perché condividere il proprio cibo preferito non è così grave come la condivisione di foto di familiari senza il loro consenso?

Step 2: *Brainstorming* in movimento

Quest'attività introduce il tema riguardante regole di *copyrighting*, *licensing* e protezione dei dati. L'educatore attaccherà 3 fogli mobili sul muro (suggeriamo di farlo con una pasta adesiva) dandogli i seguenti titoli: "copyrighting", "licensing", e "protezione dei dati".

Ai partecipanti vengono dati pennarelli di diversi colori; dovranno girare per la stanza e scrivere una o più parole su ogni foglio, in base a quello che viene loro in mente pensando a quel tema. È importante far presente che non ci sono risposte giuste o sbagliate.

Una volta che tutti hanno scritto almeno una parola, devi dar inizio alla discussione e presentare le informazioni sul tema. Puoi adattare questa attività anche online usando piattaforme

Step 3: Verifica le tue conoscenze

Questa attività si basa sulle conoscenze acquisite dagli studenti che hanno seguito la presentazione degli argomenti della presente unità.

L'educatore dice alla classe che avranno a disposizione 30 minuti per rivedere tutto quello che è stato detto nell'unità. Scaduto il tempo, la classe verrà divisa in due gruppi. L'educatore mette un cucchiaio su un tavolo e i due gruppo dovranno mettersi in due file frontali, nella direzione del tavolo (vedi figura 10).

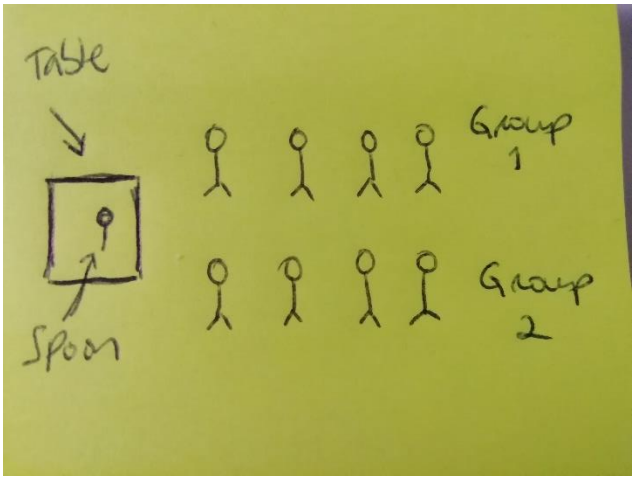


Figura 10: Divisione degli studenti in due gruppi.

- I due studenti più vicini al tavolo (devono essere alla stessa distanza) dovranno prendere il cucchiaio quando sentono l'allarme (l'educatore emetterà un suono). La squadra che prenderà prima il cucchiaio avrà il diritto di rispondere alla domanda.
- Gli educatori devono preparare una serie di domande inerenti agli argomenti insegnati.
- Ogni risposta corretta vale 1 punto.
- Per ogni risposta sbagliata verrà tolto 1 punto.
- Il tempo per le risposte è di 1 minuto (gli educatori possono aumentarlo).
- Per ogni round, la quadra cambierà il membro che deve prendere il cucchiaio, in modo che tutti abbiano la possibilità di farlo. Se l'attività venisse svolta online, potresti doverla riadattare in una sorta di "chi vuol essere milionario?".

Congratulazioni, hai completato il Modulo 1.

Non dimenticarti di controllare le Appendici per maggiori risorse e documenti forniti al fine di supportare lo studio da autodidatta!

Modulo 2: Comunicazione e collaborazione

Il secondo modulo contiene informazioni riguardanti le piattaforme collaborative e descrive argomenti legati alla comunicazione e alla collaborazione online.

Si prega di notare che le attività pratiche descritte in ogni unità potrebbero prevedere il supporto di un educatore esperto. Nonostante le informazioni presenti nel manuale siano scritte in modo facilmente comprensibile, alcune azioni, legate alle informazioni presentate, potrebbero richiedere il supporto di esperti.

Modulo 2	**Comunicazione**					
Durata	25h					
Obiettivi	• Essere in grado di usare le tecnologie online al fine di collaborare con gli altri, come scambiarsi i dati e le informazioni o organizzare il lavoro in gruppo. • Essere in grado di comportarsi appropriatamente nell'ambiente online. • Essere consapevole dei rischi e dei benefici nell'avere un'identità online.					
Unità	2.1 Interagire attraverso le tecnologie digitali	2.2 Condividere informazioni attraverso le tecnologie digitali	2.3 Coinvolgere la cittadinanza attraverso le tecnologie digitali	2.4 Collaborare attraverso le tecnologie digitali	2.5 Netiquette	2.6 Gestire l'identità digitale
Organizzazione della formazione[12]	Lezioni frontali *E-learning*	Lezioni frontali *E-learning*	Lezioni frontali *E-learning*	Lezioni frontali *E-learning*	Lezioni frontali *E-learning*	Lezioni frontali *E-learning*
Durata	4h	4h	5h	3h	5h	4h

Tabella 9: Struttura generale del Modulo 2: Comunicazione e collaborazione.

[12] Lezioni frontali, E-Learning, apprendimento misto o da autodidatta.

2.1. Interagire attraverso le tecnologie digitali

Unità 2.1	Interagire attraverso le tecnologie digitali
Durata	4 ore
Obiettivi	• Le basi della comunicazione (Come comunicare meglio) • Gli studenti prenderanno in considerazione l'importanza delle e-mail, della ricerca su Internet e dei documenti digitali. • Gli studenti useranno strumenti digitali per azioni quotidiane su diverse piattaforme. • Gli studenti entreranno in confidenza con i social media.
Contenuti	2.1.1 Il processo di comunicazione e gli stili comunicativi 2.1.2 Comunicazione e-mail efficace 2.1.3 Formazione sui Social Media per i principianti 2.1.4 Attività pratiche
Risorse	Proiettore per la presentazione power-point (scaricare la presentazione dal sito) Dispositivi mobili/postazioni informatiche/tablet Cuffie Esempi di progetti
Metodo di formazione	• Presentazione da parte dell'educatore • Discussione/dibattito di gruppo • Lavoro a coppie/piccoli gruppi • Presentazione da parte partecipanti • Selezione dei contenuti • Apprendimento basato sui problemi (PBL) • Insegnamento capovolto

Tabella 10: Struttura dell'unità di competenza 2.1. – Interagire attraverso le tecnologie digitali del Modulo 2 (Comunicazione e collaborazione).

2.1.1 Il processo di comunicazione e gli stili comunicativi

Le basi della comunicazione

Canali digitali e mezzi

Un **CANALE** digitale può essere definito come l'interfaccia connessa al *world wide web* attraverso la quale può essere creata la comunicazione.

- Sul Web: siti web
- Ricerca: risultati dei motori di ricerca
- Comunicazione: e-mail e app di messaggistica
- Eventi online: webinar
- Mezzi digitali: streaming di video and siti di musica
- Giochi: giochi virtuali

Un **MEZZO** è un una modalità fisica per salvare o archiviare i dati e può contenere:

- Dati
- Grafica
- Audio e video

I mezzi digitali sono conosciuti come media digitali, ossia la forma dei media che possono essere creati, visti, modificati e distribuiti dai dispositivi elettronici.

Stili comunicativi

- **Passivo:** i comunicatori passive si comportano spesso in maniera indifferente e non riescono ad esprimere le loro emozioni o bisogni permettendo alle persone di esprimersi per loro.

"Non è così importante, in realtà."

- **Aggressivo:** i comunicatori aggressive spesso si esprimono in maniera "rumorosa" e tendono a dare comande, porre domande maleducatamente e non riescono ad ascoltare gli altri.

"Io ho ragione, tu hai torto."

- **Passivo – Aggressivo:** questi comunicatori comunicano spesso con il linguaggio del corpo e sembrano essere consapevoli dei loro bisogni, ma a volte fanno fatica a far sentire la loro.

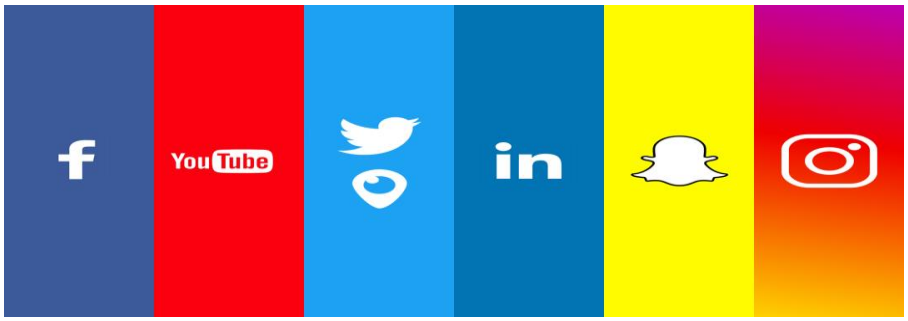
"Per me va bene, ma non sorprenderti se qualcuno si arrabbia."

- **Assertivo:** i comunicatori assertive sono in grado di esprimere le loro esigenze, desideri, idee e sentimenti considerando anche i bisogni degli altri.

"Rispetto i diritti degli altri."

Social Media

La parola Social Media fa riferimento ai mezzi di interazione tra le persone con cui creano, condividono e scambiano informazioni e idee in comunità virtuali e network. Le app più conosciute dei social media sono: ***Facebook***, ***Instagram, Twitter, LinkedIn, YouTube.***



Attività pratiche

Modulo	2
Unità	2.1
Durata	3-4 ore
Tipo di attività	Attività pratiche
Obiettivi	Alla fine dell'attività gli studenti saranno in grado di: ♦ Comunicare e interagire meglio attraverso gli strumenti digitali ♦ Usare piattaforme online in base al destinatario e al contenuto che l'utente desidera comunicare. ♦ Capire come usare gli strumenti digitali e acquisire familiarità con i social media.
Materiali	Per lo svolgimento di questa attività sono richiesti: ♦ Un proiettore ♦ Slide PowerPoint (scaricare la presentazione dal sito) ♦ Carta e penna ♦ Dispositivi mobili ♦ Computer ♦ Una lavagna ♦ Gessetti
Attività di *debriefing*	Alla fine dell'attività gli studenti devono pensare a: ♦ Cosa significa comunicare e interagire attraverso le tecnologie digitali. ♦ A quali vantaggi porta? Quali sono gli svantaggi? ♦ In che modo questi strumenti hanno cambiato la comunicazione personale e di gruppo negli ultimi anni?

Step 1: 40-50 min

- L'educatore, dopo aver conosciuto tutti gli studenti, inizia a introdurre il modulo con una presentazione PowerPoint, fornendo una definizione generale di cosa siano la comunicazione e l'interazione, e della definizione di strumenti digitali.
- L'educatore assegnerà ad ogni studente un partner e poi un computer ad ogni coppia.
- L'educatore chiederà ad ogni coppia di studenti di scegliere un'app come, ad esempio, Word per scrivere una breve lettera o un paragrafo
- Discuti con gli studenti il tipo di comunicazione o di interazione sia una lettera.

Step 2: 30-40 min

L'educatore presenterà, tramite PowerPoint, le basi della comunicazione.

L'educatore chiederà ad ogni studente di identificare, per la lettera o il paragrafo, chi è

a. Il mittente
b. Il destinatario
c. Il messaggio
d. Il codice

Attività di *debriefing*

- L'educatore parlerà con tutti gli studenti e chiederà loro cosa considerano canali di comunicazione, e chiederà loro di fornire alcuni esempi.
- L'educatore farà tutti gli esempi dei canali di comunicazione e dei mezzi forniti dagli studenti sulla lavagna.
- L'educatore presenterà con PowerPoint la comunicazione e i mezzi.
- L'educatore chiederà in che modo gli studenti classificherebbero i canali: formali, informali, non ufficiali.

Step 3: 60 min

Questa attività più pratica rispetto alle prime due ma comprenderà anche una parte teorica perché l'educatore presenterà gli strumenti digitali con un focus sull'uso di un account online.

- L'educatore presenterà i termini "username, "password" e "account online".
- L'educatore guiderà gli studenti nella creazione del proprio account online, attraverso google.com
- Gli studenti, attraverso questa attività, lavoreranno in coppia e ogni coppia condividerà un account.
- Una volta che gli studenti hanno creato il loro account Google, l'educatore mostrerà loro Gmail e spiegherà il format e la struttura di questo strumento.

- Chiedi agli studenti di comporre una breve lettera o paragrafo nella nuova finestra di messaggio.

Attività di *debriefing*

L'educatore farà alcune domande di *debriefing*:

- Chi è il destinatario delle vostre e-mail? Che tono usereste e perché?
- Per quale tipo di comunicazione è adatta una e-mail?
- Quale genere di media o files possono essere allegati in una e-mail?

Step 4: 30-40 min

- L'educatore, in base all'attività di debriefing precedente, presenterà, attraverso una presentazione PowerPoint, gli stili comunicativi e quelli usati attraverso gli strumenti digitali.
- L'educatore presenterà e nominerà tutti i Social media.
- L'educatore guiderà gli studenti, passo dopo passo, nella creazione di un account Facebook attraverso l'uso dell'indirizzo mail Gmail ed effettueranno la registrazione.
- L'educatore guiderà gli studenti al fine di conoscere tutte le funzionalità di Facebook e inviare messaggi ad altri colleghi.
- L'educatore fornirà anche informazioni, passo dopo passo, nella creazione di un breve post.

2.2. Condividere informazioni attraverso le tecnologie digitali

Unità 2.2	Condividere informazioni attraverso le tecnologie digitali
Durata	4 ore
Obiettivi	Connettersi con gli altri attraverso gli strumenti digitali Creare cartelle condivise su una piattaforma condivisa Utilizzare e modificare un file condiviso
Contenuti	2.2.1 Utilizzo di account online su una piattaforma digitale 2.2.2 Creazione di un file condiviso su una piattaforma 2.2.3 Utilizzo di commenti o effettuazione di modifiche su un file condiviso 2.2.4 Attività pratiche
Risorse[13]	Computer/tablet con accesso a Internet Presentazione PowerPoint (scaricare la presentazione dal sito) Proiettore Cuffie
Metodo di formazione	Presentazione da parte dell'educatore Discussione/dibattito di gruppo Lavoro a coppie/piccoli gruppi Selezione dei contenuti Apprendimento basato sui problemi (PBL) Stazioni di apprendimento

Tabella 11: Struttura dell'unità di competenza 2.2. – Condividere informazioni attraverso le tecnologie digitali del Modulo 2 (Comunicazione e collaborazione).

Condividere informazioni attraverso le tecnologie digitali

Le tecnologie digitali sono strumenti, sistemi, dispositive e risorse che generano, archiviano e processano i dati. Le più comuni tecnologie digitali includono i social media, i giochi online, multimedia e dispositivi mobili.

Cosa vuol dire condividere con le tecnologie digitali?

Secondo il *Digital competence Framework 2.0* significa condividere dati, informazioni e contenuti digitali con gli altri attraverso tecnologie digitali appropriate come detto in precedenza.

[13] Materiali e attrezzature.

Strumenti digitali

- **Programmi**: Word, Paint, Notes
- **Siti web:** Google.com (Google drive)
- **Risorse online:** Podcasts, Videos, social media

Vediamo come condividere un file su Google Drive…

Cos'è Google Drive?
Google Drive è uno spazio di archiviazione sviluppato da Google. È un servizio Internet disponibile sotto forma di sito web e app e permette di archiviare file nel "cloud" a sincronizzarli nei diversi dispositivi.
Diamogli un'occhiata!

1. Vai su drive.google.com dal tuo computer
2. Effettua il login con username e password di Google
3. Carica il file creato in precedenza su Google Drive
4. Clicca sul file caricato e clicca "condividi"
5. Sotto la dicitura "persone" digita l'indirizzo e-mail del tuo collega
6. Clicca "invia"

Attività pratiche

Modulo	2
Unità	2.2
Durata	2 – 3 ore
Tipo di attività	Attività pratiche
Obiettivi	Alla fine dell'attività gli studenti saranno in grado di: ♦ Connettersi con gli altri attraverso gli strumenti digitali ♦ Creare documenti condivisi su una specifica piattaforma ♦ Utilizzare e modificare un file condiviso
Materiali[14]	Per lo svolgimento di questa attività sono richiesti: ♦ Un proiettore ♦ Slide PowerPoint (scaricare la presentazione dal sito) ♦ Carta e penna ♦ Dispositivi mobili ♦ Computer
Attività di *debriefing*	Alla fine dell'attività gli studenti devono pensare a: ♦ Cosa significa condividere informazioni attraverso le tecnologie digitali. ♦ A quali vantaggi porta? Quali sono gli svantaggi? ♦ In che modo questi strumenti hanno cambiato la condivisione delle informazioni negli ultimi anni?

Step 1: 10 min

L'educatore presenterà agli studenti il concetto della condivisione, fornendo anche la sua definizione.

Attività di *debriefing*

L'educatore porrà alcune domande di *debriefing*:

- Di solito, quale genere di informazioni condividi?

[14] Si prega di individuare gli strumenti, i materiali, i documenti e ogni supporto necessario al fine di svolgere questa attività. Nel caso in cui si crei un documento a supporto, anche questo può essere aggiunto.

- In che modo condividi queste informazioni?
- Quali strumenti digitali o piattaforme potrebbero essere usate per condividere queste informazioni?

Step 2: 30-40 min

- L'educatore introdurrà gli strumenti digitali come Word, Notes o Paint, attraverso una presentazione PowerPoint per creare i contenuti.
- L'educatore chiedere agli studenti di selezionare una delle app spiegate per creare un contenuto specifico, sia scritto che sotto forma di immagini.
- Una volta che tutti gli studenti hanno creato i loro file, l'educatore chiederà loro di salvarlo localmente sul computer della loro postazione.
- L'educatore presenterà le piattaforme più comuni per condividere contenuti: Facebook, Instagram, mail, YouTube, Google Drive, Dropbox.

Step 3: 20 min

- L'educatore chiederà agli studenti di aprire uno strumento digitale specifico come Dropbox e li guiderà passo dopo passo nell'individuazione dei file in precedenza creati attraverso Dropbox con il resto degli studenti.
- L'educatore chiederà poi agli studenti di aprire una piattaforma social come Facebook e chiederà loro di condividere i file creati sotto forma di post.

Step 4: 10-20 min

- L'educatore presenterà, tramite slide, mostrerà semplici passi per modificare un file condiviso su Dropbox.
- L'educatore chiederà ai discenti di modificare tutti i file condivisi nella cartella comune della piattaforma Dropbox.

2.3. Coinvolgere la cittadinanza attraverso le tecnologie digitali

Questa unità introdurrà due concetti principali:

- Cittadinanza digitale
- Sensibilizzazione alla sicurezza informatica

Cercheremo di capire il modo in cui identificare i rischi relativi alla sicurezza informatica, prevenirli e risolverli.

Unità 2.3	**Coinvolgere la cittadinanza attraverso le tecnologie digitali**
Durata	5 ore
Obiettivi	• Capire la cittadinanza digitale così come il concetto di sensibilizzazione alla sicurezza informatica • Identificare i rischi relativi alla sicurezza informatica • Come prevenire gli attacchi informatici
Contenuti	2.3.1 Cittadinanza digitale 2.3.2 Concetti fondamentali 2.3.3 Sicurezza e Privacy 2.3.4 Attività pratiche
Risorse	Computer e dispositivi mobile con accesso Internet Cuffie Proiettore Presentazione PowerPoint (**scaricare la presentazione dal sito**) Lavagna
Metodo di formazione	• Presentazione da parte dell'educatore • Discussione/dibattito di gruppo • Simulazione/giochi di ruolo • Selezione dei contenuti • Apprendimento basato sui problemi (PBL) • Apprendimento cooperativo • Insegnamento capovolto

Tabella 12: Struttura dell'unità di competenza 2.2. – Coinvolgere la cittadinanza attraverso le tecnologie digitali del Modulo 2 (Comunicazione e collaborazione).

2.3.1 Cittadinanza digitale

La cittadinanza digitale fa riferimento al comportamento, il coinvolgimento positivo che le persone vivono quando entrano nel mondo digitale. Più nel dettaglio, un **cittadino digitale** è una persona che ha le conoscenze e le abilità per poter adeguatamente usare le tecnologie digitali al fine di comunicare con gli altri, partecipare alla vita sociale e creare e utilizzare i contenuti attraverso gli strumenti digitali.

2.3.2 Concetti fondamentali

Sicurezza online

Questo concetto è diventato un tema fondamentale nel mondo digitale e include la conoscenza personale riguardante la privacy di Internet e il modo in cui il comportamento degli individui può contribuire alla creazione di un'interazione salutare con l'uso di Internet.
Pericoli comuni: Phishing, Malware, cyberbullismo, accesso e pubblicazione di informazioni private.

Reputazione

Spostarsi dall'Era dell'Informazione all'Era della Reputazione

La nostra reputazione digitale è il modo in cui veniamo percepiti online ed è plasmata e pensata nel modo in cui un individuo presenta se stesso e le informazioni di se stessi che gli altri individui postano.

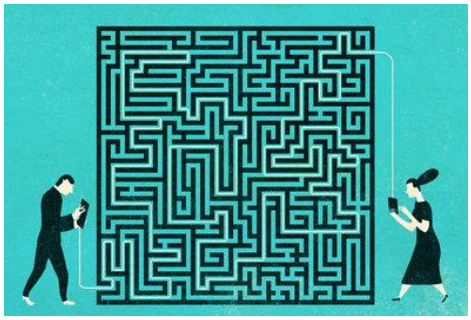
La reputazione digitale è un concetto che è stato plasmato tanto da diventare più permanente che mai prima ancora che noi, come individui, ponessimo più fiducia nei risultati di ricerca che in qualsiasi altra fonte.

Relazioni

Le relazioni digitali includono l'utilizzo di tecnologie al fine di sviluppare un'interazione tra gli individui più rilevante e interattiva.

Queste tecnologie possono contribuire sia in maniera positiva sia negativa, nello specifico, in relazioni personali che dipendono dal modo in cui gli individui usano la tecnologia e potrebbero creare problemi tra gli interlocutori, scatenando conflitti e insoddisfazione nel rapporto.

O



Etica

L'etica digitale è lo studio del modo in cui gestire sé stessi eticamente, professionalmente, online e con mezzi digitali.

Alcuni esempi di comportamento etico si manifestano quando un individuo:

1. Chiede il permesso di raccogliere e archiviare dati sugli utenti.
2. Chiede il permesso di vendere dati personali archiviati.
3. Ha il diritto di chiedere che tali dati, loro riguardanti, vengano cancellati.
4. Ha l'accesso ai dati personali raccolti e archiviati.

Impronte digitali

Le impronte o tracce digitali sono le prove lasciate da un individuo quando cerca, visita, crea, condivide, pubblica e installa attraverso strumenti digitali su un dispositivo mobile o un computer.

Un buon cittadino

- Sostiene i pari diritti umani
- Tratta gli altri con rispetto
- Non ruba o danneggia la proprietà altrui
- Comunica chiaramente in maniera rispettosa e con empatia
- Parla in modo onesto e non riporta dicerie infondate
- Protegge se stesso e gli altri dai pericoli
- Mostra un'immagine positiva di se stesso.

Un buon cittadino digitale

- Sostiene i pari diritti digitali per tutti
- Cerca di comprendere tutte le prospettive
- Rispetta la privacy digitale, la proprietà intellettuale e gli altri diritti delle persone online
- Comunica e agisce con empatia verso gli altri tramite i canali digitali
- Applica una pensiero critico a tutte le risorse online, fake news comprese
- È consapevole della salute fisica, emotiva e mentale durante l'uso degli strumenti digitali
- Capisce l'inalterabilità del mondo digitale e gestisce proattivitamente l'identità digitale.

2.3.3 Sicurezza e Privacy

Sicurezza – Numerosi processi che proteggono le informazioni personali di un individuo dalle altre persone. Questo può essere ottenuto in diversi modi:

- VPN, *Virtual Private Networks* (Rete Virtuale Privata)
- Programmi antivirus
- Password sicure

Privacy – Il diritto di una persona di preservare e proteggere la propria identità e il mantenimento di uno spazio sicuro e protetto attorno a: integrità, presenza fisica, pensieri, emozioni e attività personali di un individuo.

Nel mondo digitale la privacy deve essere vista come un diritto estremamente importante per gli individui sia come società sia come collettività.

2.3.4 Attività pratiche

Modulo	2
Unità	2.3
Durata	5 ore
Tipo di attività	Attività pratiche
Obiettivi	Alla fine dell'attività gli studenti saranno in grado di: ♦ Capire i concetti di Cittadinanza Digitale e di Sensibilizzazione alla sicurezza informatica. ♦ Identificare i rischi relativi alla sicurezza ♦ Prevenire gli attacchi informatici
Materiali[15]	Per lo svolgimento di questa attività sono richiesti: ♦ Computer e dispositive mobile con accesso ad Internet ♦ Cuffie ♦ Proiettore ♦ Lavagna ♦ Gessetti
Attività di *debriefing*	Alla fine dell'attività gli studenti devono pensare a: ♦ Come le persone interagiscono online ♦ Essendo online, devi essere molto attento al modo in cui comunichi con gli altri ♦ Come prevenire gli attacchi informativi ♦ Come proteggere i computer o i dispositivi mobili durante la navigazione online ♦ Come filtrare informazioni su Internet e contenuti condivisi

[15] Si prega di individuare gli strumenti, i materiali, i documenti e ogni supporto necessario al fine di svolgere questa attività. Nel caso in cui si crei un documento a supporto, anche questo può essere aggiunto.

Step 1: 30-40 min

- L'educatore avrà a disposizione un programma sotto forma di slide per tenere sotto controllo la lezione e assicurarsi che gli studenti sapranno e capiranno cosa aspettarsi durante la formazione.
- L'educatore presenterà il modulo agli studenti attraverso slide di PowerPoint e spiegherà il concetto di Cittadinanza Digitale.
- Chiedi agli studenti, sul proprio computer, di guardare due video basati sui problemi con un focus sul perché la Cittadinanza Digitale sia importante.

Attività di *debriefing*

- L'educatore si confronterà con gli studenti su ciò che hanno capito sul concetto di Cittadinanza Digitale
- L'educatore approfondirà, inoltre, con gli studenti le minacce e i rischi che si incontrano facendo ricerca su siti web non sicuri e il modo in cui gestire i problemi relativi ai social media.

Step 2: 60 min

- L'educatore presenterà i concetti principali relativi alla Cittadinanza Digitale
- L'educatore fornirà agli studenti gli esempi e li aiuterà a diventare attenti ai pericoli di Internet
- L'educatore incoraggerà gli studenti a scambiarsi idee e dimostrare la consapevolezza dei pericoli mostrando le diverse ipotesi
- L'educatore illustrerà le due ipotesi e parlerò dei punti chiave di ognuna
- Una volta elaborare le ipotesi, l'educatore creerà, sulla lavagna, una tabella a tre colonne con i termini "sicuro", "responsabile" e "rispettoso" scritti all'inizio di ogni colonna.
- Invita gli studenti a fornire parole o frasi che descrivano il modo in cui le persone possano agire in maniera sicura, responsabile e rispettosa online e scrivile nelle colonne appropriate.
- Fai in modo che ogni studente abbia un pezzo di plastica da rompere in piccoli pezzi, spiega loro cosa questo comportamento causa all'ambiente e collegalo all'impronta digitale di una persona che non agisce in maniera sicura, responsabile e rispettosa.

Step 3: 50 min

- L'educatore presenterà il concetto e la definizione di traccia e impronta digitale
- L'educatore fornirà agli studenti delle dispense su cui scrivere ciò che già sanno, cosa vorrebbero conoscere e cosa hanno imparato.
- L'educatore chiederà a due volontari di fare un gioco di ruolo
  Dovrai dire: "Immagina che stai camminando in una strada piena di gente e un completo sconosciuto si avvicina e ti dice che hai appena vinto un viaggio gratis (tutto ciò che devi fornirgli è il tuo nome, età, numero di telefono e password degli account social (Google+, Facebook ecc.). Gli crederesti?"

Attività di *debriefing*

L'educatore distribuirà una valutazione consuntiva che verrà trattata tra gli studenti

Step 4: 45 min

- L'educatore inizierà chiedendo quanto sia importante la privacy e gli studenti dovranno esprimere un giudizio da 1 a 5 e registrare le informazioni alla lavagna.
- L'educatore chiederà poi agli studenti chi dice che avere la propria privacy non è importante e incoraggerà il dibattito sul tema.
- Usando alcuni esempi del dibattito, approfondisci la questione sulla comprensione da parte degli studenti dei termini Sicurezza e Privacy
- L'educatore fornirà la definizione di Privacy e Sicurezza dando alcuni esempi sugli strumenti digitali

Alla fine, l'educatore farà un riassunto di ciò che è stato detto all'interno dell'unità e spiegherà i diritti posseduti da tutti in qualità di cittadini digitali e chiederà le impostazioni di privacy e sicurezza dei social media degli studenti sui loro computer.

2.4. Collaborare attraverso le tecnologie digitali

Unità 2.4	Collaborare attraverso le tecnologie digitali
Durata	3 ore
Obiettivi	Insegnare agli studenti il modo in cui usare gli strumenti digitali al fine di collaborare online con gli altri
Contenuti	2.4.1 Collaborare attraverso le tecnologie digitali (concetti principali) 2.4.2 Attività pratiche
Risorse	Lavagna Carta e penna Un barattolo Computer
Metodo di formazione	Presentazione da parte dell'educatore Discussione/dibattito di gruppo Lavoro a coppie/piccoli gruppi Selezione dei contenuti

Tabella 13: Struttura dell'unità di competenza 2.5. – Collaborare attraverso le tecnologie digitali del Modulo 2 (Comunicazione e collaborazione).

2.4.1 Collaborare attraverso le tecnologie digitali (concetti principali)

Lo scopo di questa unità è quello di insegnare agli studenti il significato di collaborare attraverso le tecnologie digitali, conoscere gli strumenti più comuni utili alla collaborazione online ed essere in grado di individuare lo strumento adatto ad una particolare esigenza.

Definizione di "collaborare attraverso le tecnologie digitali":

Secondo la definizione del *Digital Competence Framework 2.0*, *collaborare attraverso le tecnologie digitali* significa: "usare gli strumenti e le tecnologie in processi collaborativi e per la co-costruzione e la co-creazione di risorse e conoscenza ".

Perché la collaborazione attraverso le tecnologie digitali è così importante?

Al giorno d'oggi siamo sempre più abituati ad usare le tecnologie digitali, nella nostra vita privata e lavorativa per interagire con gli altri.

Scambiare documenti, foto, informazioni o usare l'ambiente online per organizzare il lavoro o lo studio è diventato estremamente importante, in particolar modo da quando il Covid-19 ci ha costretti a vivere, lavorare e studiare a casa. Ci sono diversi strumenti che ci permettono di scambiare informazioni online, in modo facile e veloce.

Essere in grado di interagire con i colleghi o con altre persone online, scambiarsi documenti e informazioni ed essere in grado di gestire attività, organizzare riunioni… è diventato di estrema importanza specialmente nel mondo lavorativo. Gli strumenti digitali ci aiuteranno a gestire il lavoro (non solo da remoto), velocizzare lo scambio di informazioni e aumentare la produttività del gruppo.

Quali sono gli strumenti più utili per collaborare online?

Come giù detto, ci sono diversi strumenti che ci aiutano a collaborare con gli altri online. Qui di seguito ne condividiamo e raccomandiamo alcuni:

Skype, GoToMeeting, Zoom Meetings, Google Meet, Microsoft Teams: tutti questi strumenti sono strumenti di Conferenze via web e riunioni online che permettono alle persone di organizzare meeting da remoto o vedersi facilmente quando le persone si trovano lontano. Puoi anche condividere il tuo schermo e mostrare la presentazione e i file ai partecipanti.

Google Drive, Dropbox: con queste app puoi salvare file e archiviarli in uno spazio online, separato dai tuoi dispositivi. Questo è utile perché puoi accedere a file anche se i tuoi dispositivi hanno dei problemi, nel caso in cui tu li abbia archiviati li. Inoltre, grazie a questi strumenti sarai in grado di lavorare e collaborare con altre persone avendo la possibilità di condividere il tuo spazio o i tuoi documenti con i colleghi, gli amici, la famiglia…

Google Calendar, Teamup: queste app sono state create come un'agenda, un calendario che puoi organizzare e personalizzare. L'interfaccia è molto semplice in entrambi i casi e puoi decidere se visualizzare un giorno singolo una settimana o addirittura intervalli di tempo maggiori. Puoi segnare i tuoi appuntamenti, programmare le riunioni e addirittura condividerli con gli altri.

Trello, Redbooth, Asana: questi sono strumenti per la gestione dei progetti che ti aiutano durante le attività lavorative. Puoi creare liste, assegnare attività ad altri membri del tuo gruppo che condividono lo stesso spazio, fissare le scadenze e personalizzare tutto in modo più efficiente possibile.

Google Form: l'applicazione di Google ti permette di creare sondaggi in modo facile e del tutto gratis. Puoi personalizzare i sondaggi e usare modi diversi per porre le domande: risposta multipla, risposte aperte, scale di gradimento…

2.4.2 Attività pratiche

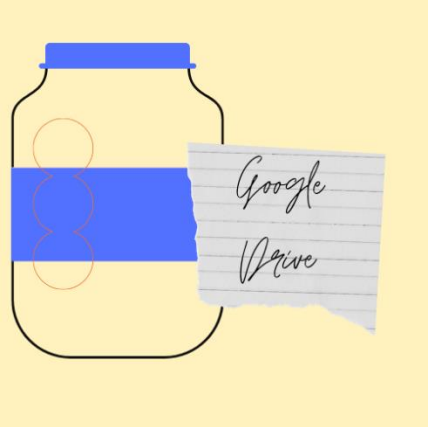
Step 1: Il barattolo degli strumenti

L'educatore fa una lista dei diversi strumenti da proporre agli studenti.

Tutti gli strumenti digitali che suggeriamo sono open-source. L'educatore può inserire tutti gli strumenti che vuole (almeno uno a studente)

Suggeriamo i seguenti: Google Drive, Trello, Dropbox, Google Calendar Google Form...

L'educatore scrive il nome dello strumento su un pezzo di carta e lo inserisce nel barattolo.



Ora è il turno degli studenti: uno alla volta, gli studenti prendono un pezzo di carta dal barattolo e leggono ad alta voce lo strumento pescato.

L'educatore fa alcune domande allo studente e alla classe:

- Per cosa viene usato questo strumento?
- L'hai mai visto?
- Sai come funziona
- Conosci altri strumenti che lavorano allo stesso modo?
- Credi che questo strumento sia utile a favorire la collaborazione?

L'educatore guiderà la discussione ma cercherà di stimola la conversazione tra gli studenti.

Quando tutti i bigliettini all'interno del barattolo saranno stati pescati, l'educatore scriverà alla lavagna i nomi degli strumenti pescati e spiegherà meglio il loro funzionamento agli studenti.

Alla fine dell'attività, l'educatore farà qualche domanda di *debriefing*:

- Sai cosa vuol dire collaborare attraverso le tecnologie digitali?
- In che modo gli strumenti analizzati possono aiutare le persone a collaborare in maniera più facile e veloce?

Step 2: Proviamoci!

Quest'attività è più pratica rispetto alla prima e serve a mettere in pratica le conoscenze teoriche acquisite durante la prima parte.

Gli studenti lavorano in coppia.

L'educatore assegna loro uno strumento da provare, tra quelli menzionati nella prima attività.

A questo punto, in base allo strumento assegnato, l'educatore chiederà agli studenti di svolgere delle piccole attività

Possono essere attività di vario genere, in base agli strumenti presentati dall'educatore.

Creare una cartella condivisa, inviare un file pesante, organizzare una riunione online e invitare alcuni contatti…

Gli studenti avranno a disposizione 30 minuti e potranno cambiare coppia in modo che ognuna possa provare il maggior numero di strumenti.

Alla fine dell'attività, l'educatore farà qualche domanda di *debriefing*:

- Hai trovato utili gli strumenti che hai provato?
- Li conoscevi già?
- Credi siano utili in contesti lavorativi e non solo?
- Per cosa li utilizzeresti

2.5. *Netiquette*

Unità 2.5	*Netiquette*
Durata	5 ore
Obiettivi	Insegnare agli studenti il comportamento corretto da tenere online
Contenuti	2.5.1 Cosa vuol dire *Netiquette*? 2.5.2 Attività pratiche
Risorse	Lavagna Gessetti Post-it Carta e penna Caso studio 1 Caso studio 2
Metodo di formazione	Discussione/dibattito di gruppo Lavoro a coppie/piccoli gruppi

Tabella 14: Struttura dell'unità di competenza 2.6. – Netiquette del Modulo 2 (Comunicazione e collaborazione).

2.5.1 Cosa significa *Netiquette*?

Lo scopo di questa unità è di insegnare agli studenti a mantenere un comportamento corretto online. Rispettare gli altri e i posti in cui ci si trova è importante sia nell'ambiente fisico sia online. Insegnare queste cose è molto importante, perché online le persone diventano più aggressive e cattive nei confronti degli altri. Ci sono diversi esempi di fenomeni legati ad un cattivo comportamento online, cyberbullismo e *body-shaming* sono solo due dei tanti comportamenti a cui assistiamo giornalmente sul web, per non menzionare episodi di razzismo e odio nei confronti delle minoranze in generale. L'educazione al rispetto degli altri è essenziale per evitare tali comportamenti.

Definizione di *Netiquette*

Secondo la definizione del *Digital Competence Framework 2.0*, *netiquette* significa: "Essere consapevoli delle norme comportamentali e del know-how durante l'uso di tecnologie digitali e durante l'interazione in ambienti digitali. Adattare le strategie di comunicazione ad un pubblico specifico ed essere consapevoli delle diversità culturali e generazionali negli ambienti digitali".

Quali comportamenti sono considerati un cattivo esempio di *netiquette*?

In generale, possiamo considerare un cattivo esempio di netiquette tutti quei comportamenti online che sono irrispettosi nei confronti degli altri. Queste attitudini possono essere di varia natura.

Mancare di rispetto alla proprietà intellettuale: condividere contenuti, foto, materiali di altri senza citarne le fonti è considerato sbagliato ed è un esempio di cattiva *netiquette* (oltre a implicare questioni legali di cui non discuteremo qui).

Dovremmo sempre controllare da dove stiamo prendendo questo contenuto e vedere se si tratta di un *open source* oppure se dobbiamo citare la fonte quando la usiamo.

Non rispettare le opinion altrui: non rispettare le opinion altrui, adottare un comportamento ostile e insultare le persone sono degli esempi di cattiva *netiquette*. Dovremmo sempre cercare di stabilire un dialogo con gli altri senza usare parole o toni inappropriati o offensivi.

Esprimerci in maniera irrispettosa: quando scriviamo un messaggio, una mail o un post dobbiamo essere consapevoli del modo in cui scriviamo ed esprimiamo noi stessi o le nostre idee. Ricorda sempre che le persone dall'altro lato non vedono il modo in cui ci poniamo e non sentono il tono della voce e questo potrebbe portare a incomprensioni. Ecco perché è importante essere cauti quando ci si esprime online. Usare un linguaggio ambiguo o ostile, così come messaggi in maiuscolo, senza firma, senza un contesto sono alcuni esempi di cattiva *netiquette*. Ricorda anche di usare un linguaggio formale o informale in base alla persona con cui stai avendo a che fare, che si tratti di un amico, un conoscente, un collega o uno sconosciuto.

Non rispettare la privacy altrui: molte persone condividono diverse foto o informazioni private sui social network, ma attenzione a rispettare sempre la privacy altrui e a non condividere mai dati sensibili senza il permesso dell'altra persona.

2.5.2 Attività pratiche

Step 1: Trova l'intruso

L'educatore scrive sulla lavagna diversi tipi di comportamento online inerenti alla *netiquette*, alcuni esempi positivi ed altri negativi.

In questa prima attività, gli studenti dovrebbero trovare gli elementi che non hanno nulla a che fare con gli altri nel gruppo dei buoni e dei cattivi esempi della *netiquette*.

Lo scopo dell'esercizio è di identificare le cattivi abitudini all'interno di quelle buone.

Chiama uno studente alla volta alla lavagna e chiedigli di cerchiare gli esempi di cattiva *netiquette*.

Alla fine, l'educatore correggerà le risposte date dagli studenti.

Alla fine di questa attività, l'educatore invita gli studenti a riflettere sul comportamento che le persone hanno online. L'educatore farà alcune domande di *debriefing*:

- Quali sono i comportamenti che ti mettono a disagio online?
- Hai mai notato cattivi comportamenti da parte degli utenti online?
- Hai mai provato a spiegare agli altri cosa sia la *netiquette*?

Suggerimenti:

- Questa attività può anche essere svolta usando post-it da attaccare al muro.
- Questa attività può anche essere svolta online utilizzando strumenti come *jamboard* (https://jamboard.google.com/).

Step 2: Leoni da tastiera

Per questo esercizio, l'educatore propone agli studenti diversi testi in cui le persone interagisco tra di loro online (chat, e-mail, faq, commenti…).

Per questa attività possono essere usati due casi studio.

Caso studio 1

Scambio di e-mail tra due colleghi

Anna ed Elisabeth sono due college che lavorano nella stessa azienda. Anna lavora nell'ufficio commerciale amministrativo mentre Elisabeth gestisce le relazioni con i clienti e l'organizzazione di eventi. Elisabeth ha ordinato alcuni volantini e poster per pubblicizzare l'evento, ma ci sono stati dei ritardi nella consegna.

Oggetto: Ritardo consegna *Summer Festival*

Anna:

Cara Elisabeth, ti scrivo in riferimento all'ordine dei volantini e dei poster da te richiesti per la festa dell'estate. Sfortunatamente, a causa della pandemia da Covid-19, il nostro tipografo ci ha informati che ci saranno dei ritardi nella consegna.

Ti aggiornerò non appena riceveremo i materiali.

Cordialmente,

Anna

Elizabeth:

Ciao Anna. Capisco che il Covid abbia causato molti problemi, ma questa è una questione grave per l'organizzazione del festival. Io devo parlare con il cliente, cosa dovrei dirgli?

ORA COME PROMUOVO L'EVENTO?

Il cliente vuole i materiali entro la fine della settimana. NIENTE SCUSE

CAMBIATE TIPOGRAFIA se necessario! CAPITO?

Anna:

Cara Elizabeth,

Mi dispiace che questi ritardi stiano causando dei problemi con il tuo lavoro.

Sfortunatamente, abbiamo pagato in anticipo per il materiale e non possiamo ricevere indietro il denaro. Per favore, cerca di spiegare la situazione al cliente, sono sicura che capirà.

Certa della tua cooperazione, ti auguro una buona giornata.

Cordialmente,

Anna

Elizabeth:

Cercherò di spiegargli la situazione e gli chiederò più tempo, ma non mi assumerò le responsabilità per questo problema, se necessario, fornirò al cliente il numero del direttore dei servizi.

ECCO COME GESTIRÒ IL PROBLEMA.

Elizabeth

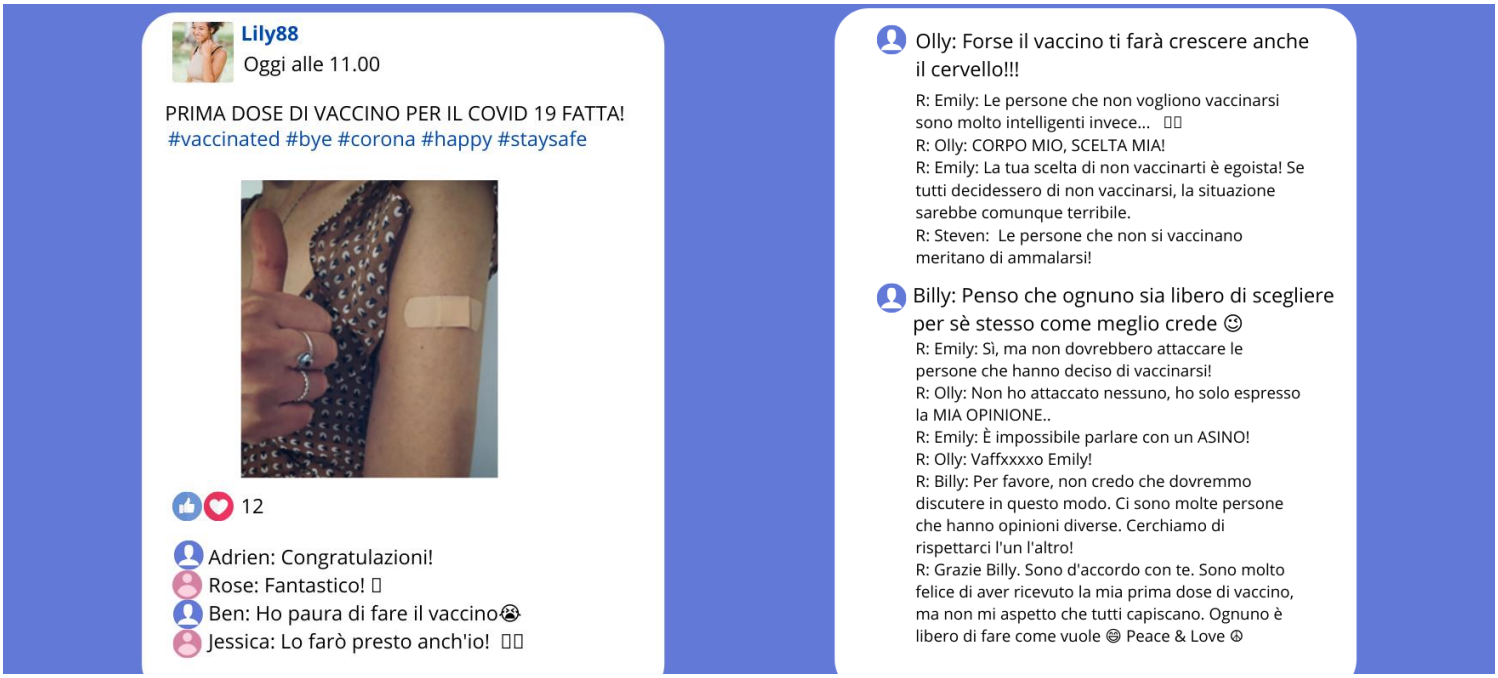
L'educatore invita gli studenti a riflettere sul testo:

- Come appare Anna? Ha un comportamento carino nei confronti di Elisabeth oppure no?
- Ed Elisabeth nei confronti di Anna?
- Qual è l'atteggiamento di Elisabeth verso il problema? È comprensiva nei confronti della collega o no?
- Nel testo, ci sono alcuni esempi di cattiva *netiquette*? Puoi identificarli?

Dopo aver risposto alle domande dell'educatore, i partecipanti dovrebbero provare a riscrivere il testo trasformando il comportamento negativo in positivo.

Caso studio 2

Una ragazza, Lily, pubblica suo profilo Facebook una foto dopo l'inoculazione della prima dose del vaccino contro il Covid-19:



L'educatore invita gli studenti a riflettere sul testo:

- Quali commenti rientrano nella definizione di cattiva *netiquette*?
- Come avresti reagito al commento di Olly?
- Credi che Emily abbia risposto a Billy in modo corretto?
- Chi pensi sia la persona che si è comportata meglio nei commenti?
- Puoi trovare dei buoni e dei cattivi esempi di *netiquette* nel testo?
- Perché credi sia più facile essere cattivi online?
- Sei mai stato un leone da tastiera?
- Cosa fai quando ti accorgi che qualcuno sta usando un comportamento inadeguato online?

Dopo aver risposto alle domande dell'educatore, I partecipanti dovrebbero provare a riscrivere il testo trasformando i comportamenti negativi in comportamenti positivi.

Step 3: Il Manifesto della *Netiquette*

Nell'ultima attività, l'educatore va alla lavagna e chiede agli studenti di redigere insieme il "Manifesto della *Netiquette*" come, ad esempio, i comportamenti positivi che gli studenti pensano possano essere accettati online.

Gli studenti dovrebbero discutere sulle regole principali e fare una lista di dieci esempi di buona *netiquette*.

Questo è il "Manifesto della Netiquette" della classe, e tutti devono impegnarsi a rispettarlo.

Una volta creato il manifesto, l'educatore potrebbe illustrare agli studenti una breve parte teorica relativa alla *netiquette*.

Alla fine dell'attività, l'educatore invita gli studenti a riflettere attentamente sul modo in cui le persone dovrebbero interagire online e il modo in cui gli studenti vorrebbero diffondere e insegnare agli altri le regole che hanno scritto (usando i social media? Condividendo il manifesto?).

2.6. Gestire l'identità digitale

Unità 2.6	Gestire l'identità digitale
Durata	4 ore
Obiettivi	Insegnare agli studenti cosa vuol dire avere un'identità digitale e il modo in cui dovrebbero gestirla.
Contenuti	2.6.1 Definizione e protezione dell'identità 2.6.2 Attività pratiche
Risorse	Carta e penna Computer
Metodo di formazione	Discussione/dibattito di gruppo Lavoro a coppie/piccoli gruppi Simulazioni / giochi di ruolo

Tabella 15: Struttura dell'unità di competenza 2.7. – Gestire l'identità digitale del Modulo 2 (Comunicazione e collaborazione).

2.6.1 Definizione e protezione dell'identità

Questo modulo ha lo scopo di rendere gli studenti consapevoli di tutte le nostre informazioni che lasciamo online e che rappresentano la nostra identità digitale. L'identità digitale è qualcosa che si lega a noi e alla nostra persona. Ad esempio, quando usiamo un ID e una password per autenticarci su un sito web, stiamo usando la nostra identità digitale. Oggi, viviamo in un mondo dove sempre più servizi di richiedono di effettuare il login con i nostri dispositivi, pubblici e privati. E-commerce, banca, servizi per la salute, servizi di pagamento delle tasse sono solo alcuni esempi. Ogni volta che registriamo la nostra identità digitale o svolgiamo alcune azioni online, i nostri dati privati vengono presi e registrati, spesso che l'utente se ne accorga. Ecco perché dobbiamo essere consapevoli e imparare il modo migliore per gestire la nostra identità online.

Definizione di gestione dell'identità digitale

Secondo la definizione del *Digital Competence Framework 2.0, gestire l'identità digitale* vuol dire: "Creare e gestire una o più identità digitali, essere in grado di proteggere la propria reputazione, avere a che fare con i dati prodotti attraverso diversi strumenti digitali, ambienti e servizi".

Perché dobbiamo preoccuparci dei nostri dati?

Ogni volta che approviamo la privacy per accedere ad un sito, scaricare un'app, rispondere a sondaggi sui social o entrare in un sito usato le tue informazioni, stiamo generando dati. Questi dati sono rilevanti per molte aziende perché mostrano il comportamento del consumatore. Spesso diamo via i nostri dati o consentiamo il loro uso senza nemmeno saperlo.

Online non solo lasciamo tracce di ciò che ci piace o meno come consumatori, ma anche importanti informazioni private che, se usate, possono essere molto dannose per noi. Si pensi, ad esempio, ai dettagli della carta di credito o gli account social con foto e informazioni personali.

Furto di identità

Quando la nostra identità digitale viene hackerata e i nostri dati personali o finanziari rubati, possiamo parlare di criminali informatici, ossia persone che sono specializzate nei furti online. Entrano nei nostri sistemi o usano trucchetti per farci credere che possono aiutarci a mettere i nostri dati al sicuro su siti o app, ma in realtà ce li stanno solo rubando.

Fingendosi te, questi criminali ti rubano denaro e informazioni. Ad esempio, alcune influencer (persone molto famose sui social), hanno annunciato il furto di identità da parte di hacker che hanno rubato i loro account social chiedendo un riscatto per riaverlo indietro.

Come difendersi dai criminali informatici?

Prima di tutto con la conoscenza. Conoscere il modo in cui gli hacker operano e il modo in cui riescono a rubare la tua identità digitale è un fattore chiave per la prevenzione.

Poi devi essere molto attento. Ad esempio, non aprire mai e-mail o messaggi sospetti. Spesso questi hacker si fingono aziende con le quali abbiamo a che fare (ad esempio una banca), quindi dobbiamo essere in grado di riconoscere se le informazioni che riceviamo sono vere o false. È scritto in un linguaggio corretto? Ci sono delle cose strane? Parla di operazioni di cui non sei al corrente? Se hai anche il minimo sospetto, non cliccare o scaricare nulla. Se si tratta della tua banca, ad esempio, chiama la tua filiale e chiedi spiegazioni. Mai cliccare su link sospetti.

Questo fenomeno è chiamato phishing ed è molto pericoloso per gli utenti colpiti.

In che modo possiamo proteggere la nostra identità digitale?

- **Usa l'autenticazione a due fattori:** autenticare la tua identità non si fa solo con un passaggio (password), ma anche con altre fasi come, per esempio, l'inserimento di un codice di autorizzazione tramite il telefono.
- **Cambia e diversifica le password:** non usare le stesse password per tutti i tuoi account e cerca di cambiarle spesso.
- **Evita di condividere dati sensibili**: stai attento al genere di dati che pubblichi, come il tuo indirizzo di casa, e cerca di condividere solo le cose essenziali online (attenzione alla geolocalizzazione delle foto nei tuoi post social).

I diritti del Cittadino Digitale

- La cittadinanza digitale, secondo il Consiglio d'Europa, fa riferimento all'abilità di impegnarsi in maniera positiva, critica e competente nell'ambiente digitale attingendo dalle abilità della comunicazione effettiva e della creatività. Tuttavia, si riferisce anche all'abilità che il cittadino utilizza quando partecipa in maniera rispettosa verso i diritti umani e la dignità attraverso un uso responsabile della tecnologia.
- Un cittadino digitale deve godere dei diritti di Privacy, Sicurezza, Accertamento ed Inclusione e libertà di espressione. Tuttavia, in qualità di cittadino con questi diritti, il cittadino digitale ha alcune responsabilità come l'etica e l'empatia e altre responsabilità al fine di garantire un ambiente digitale sicuro e responsabile per tutti i cittadini.

2.6.2 Attività pratiche

Step 1: Il gioco dell'investigatore

Immagina che stai parlando con un amico che ti dice di aver incontrario un tuo compagno di classe delle superiori.

Sei curioso di sapere di più su quella persona con cui se stato legato da ragazzo.

Cerca di ottenere il suo nome su Internet e poi allarga la ricerca (puoi anche fare la ricerca su di te o su persone che conosci).

- Cosa hai trovato sulla persona?
- Quali strumenti hai usato per aiutarti nella ricerca?
- Quali piattaforme hai consultato?
- Cerca di rispondere alle seguenti domande:
    - In che città vive?
    - È sposato/a?
    - Cosa ha studiato?
    - Che lavoro fa?

Alla fine dell'attività, l'educatore invita gli studenti a riflettere in maniera attenta sulle informazioni che si condividono online.

Step 2: Quanto è sicura la tua password?

In questa attività, l'educatore vuole insegnare agli studenti l'importanza di avere una password sicura del proprio account.

L'educatore chiede agli studenti di immaginare di dover creare delle password per una delle seguenti persone:

Helen Smith	Alejandro Garcia	María Ivanov
• Nato il: 25 giugno 1988 • Vive a: Los Angeles (USA) • Sposato • Ha avuto un cane di nome Oliver.	• Nato il: 11 marzo 1965 • Vive a: Madrid (Spagna) • Single • Adora le moto	• Nato il: 1° dicembre 1952 • Vive a: Sofia (Bulgaria) • Sposato • Ha tre figli

Figura 11: Profili da considerare per creare delle password.

- **Cerca di scrivere le diverse password per ogni persona giocando con le parole (almeno 5).** Pensa ad una password in base all'account che devono creare (banca, Facebook, e-mail personale, e-mail di lavoro, e-commerce…).
- Ora testa la sicurezza della password online (puoi usare diverse piattaforme come ad esempio https://howsecureismypassword.net/).

Alla fine di questa attività, l'educatore invita gli studenti a riflettere attentamente sul modo in cui creare una buona password al fine di garantire un certo livello di sicurezza online.

L'educatore proporrà alcune domande di *debriefing*:

- In che modo crei le tue password? Usi sempre la stessa per tutti i siti o ne hai di diverse?
- Pensi che ci siano siti in cui sia necessario un livello maggiore di sicurezza della password rispetto ad altri?
- Quali trucchi dovrebbero essere usati per creare password sicure online?
- Quanto spesso le password dovrebbero essere cambiante?
- Sai in che modo le tue password possono essere rubate?

Congratulazioni, hai completato il Modulo 2.

Non dimenticarti di controllare le Appendici per maggiori risorse e documenti forniti al fine di supportare lo studio da autodidatta!

Modulo 3: Creazione di contenuti digitali

Il Modulo 3 si concentra sulla ***creazione di contenuti digitali*** per il cittadino digitalmente competente. Lo scopo è quello di creare un pensiero condiviso sul concetto dell'essere un cittadino digitalmente competente così come quello di sviluppare e provare materiali che possano aprire una strada chiara al fine di migliorare le competenze nei campi digitali più importanti.

All'interno del modulo si toccheranno i seguenti punti:

- Sviluppare contenuto digitale per creare e modificare contenuti digitali in diversi formati, al fine di esprimersi attraverso i mezzi digitali.

- Interagire e rielaborare contenuti digitali per modificare, perfezionare, migliorare e integrare informazioni e contenuti in un vero bagaglio di conoscenze al fine di creare contenuti e competenze che siano nuove, originali e rilevanti.

- Copyright e licenze per capire il modo in cui questi si applichino a dati, informazioni e contenuti digitali.

- Programmazione per pianificare e sviluppare una sequenza di istruzioni comprensibili per i sistemi informatici al fine di risolvere problemi specifici o eseguire particolari attività.

Delineeremo il modo in cui poter creare e modificare contenuti digitali al fine di migliorare e integrare le tue informazioni in un bagaglio di conoscenze, evidenziando i problemi più importanti riguardo *copyrighting* e *licensing* digitali. Sfioreremo anche gli aspetti della programmazione e del modo in cui usare i sistemi informatici.

Si prega di notare come le unità descritte possano prevedere il supporto di un docente esperto. Nonostante le informazioni presenti nel manuale siano scritte in maniera da comprenderle facilmente, alcune azioni, inerenti alle informazioni presentate, potrebbero richiedere la supervisione e il supporto di esperti.

Modulo 3	Creazione di contenuti digitali			
Durata	10 ore			
Obiettivi	Capire le sfumature elaborare le competenze sulla creazione di contenuti			
Unità	3.1. Sviluppare contenuti digitali	3.2 Integrare e rielaborare i contenuti digitali	3.3 Copyright e licenze	3.4 Programmazione
Organizzazione della formazione	*E-Learning*	*E-Learning*	*E-Learning*	*E-Learning*
Durata	2.5 h	2.5 h	2.5 h	2.5 h

Tabella 16 - Struttura generale del Modulo 3 – Creazione di contenuti digitali.

Nota: le attività pratiche del modulo 3 sono presentate attraverso slide PowerPoint che puoi scaricare dalla sezione "risorse" sul sito del progetto.

3.1 Sviluppare contenuti digitali

Unità 3.1	Sviluppare contenuti digitali
Sviluppare contenuti digitali	2.5 ore
Obiettivi	Conoscenza approfondita degli strumenti Mojo, modi pratici per registrare contenuti e capire il posizionamento, le luci e le angolazioni. Panoramica generale di Facebook live e app telefoniche per lo sviluppo di contenuti digitali. Infine, un salto nella programmazione dei contenuti digitali
Contenuti	Risorse autonome e flessibili da poter usare lungo il percorso, E-learning
Risorse	PC, telefono o tablet per l'E-learning Presentazione PowerPoint (**scaricare la presentazione dal sito**)
Metodo di formazione	Presentazione da parte dell'educatore Insegnamento capovolto

Tabella 17: Struttura dell'unità di competenza 3.1.- Sviluppare contenuti digitali del Modulo 3 (Creazione di contenuti digitali).

3.1 Sviluppare contenuti digitali

5 tipologie di contenuti digitali

Blogging

I post dei blog sono un modo facile per creare contenuti coinvolgenti per i tuoi utenti online! Un po' come un giornale vecchio stile, molte persone amano sedersi e godersi una lettura scritta bene, che sia un articolo o un post. Puoi condividere tantissime informazioni in modo informale, presentarti ai tuoi lettori, creare un rapporto con loro e invogliarli a leggere altri tuoi contenuti. Mandare avanti un blog di successo potrebbe richiedere molto tempo, quindi, prima di iniziare, è bene raccogliere tutti i materiali. Trova delle idee per i post dei primi 2 o 3 mesi, e migliora la tabella di marcia per caricare i file e coinvolgere i tuoi lettori. Questo ti aiuterà ad essere un blogger coerente e costante.

Vuoi creare un blog? Trovi maggiori informazioni qui:

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

Contenuti Long-form

Nel mondo dell'istantaneità in cui viviamo oggi, i contenuti *long-form* potrebbero essere un po' azzardati. A molte persone piace ricevere informazioni corte e dolci, come dei bocconcini. Tuttavia, la definizione di *long-form* è adattarsi e riflettere ciò. Alcuni definiscono i contenuti *long-form* come articoli con più di 700 parole, mentre altri pensano che per essere tali, debbano superare le 1800 parole. Questi tipi di articoli *long-form* potrebbero piacere ai tuoi più avidi lettori, coinvolgendoli e dando loro un luogo in cui rifugiarsi.

Questo genere di contenuti potrebbe funzionare molto bene grazie al focus sull'ottimizzazione per i motori di ricerca, compresa l'ottimizzazione delle parole chiave. Creando tag per le parole usate di frequente e quelle di maggior interesse per il tuo pubblico target puoi fare in modo che il tuo contenuto atterri sui loro schermi! Sii intelligente e astuto con i tuoi contenuti e tutto andrà a meraviglia.

Consigli per rendere il tuo contenuto interessante e valido: https://medium.com/swlh/10-tips-to-make-long-form-content-readable-and-valuable-5b6e117965ae

Infografica

Accattivante, coinvolgente e facile da creare! L'infografica è uno degli strumenti digitali più usati online, perché è accattivante agli occhi dell'utente, che vuole scoprire di più. Può essere davvero coinvolgente, fornendo immagini di alta qualità e molte informazioni in maniera compatta e veloce. Inoltre, è molto facile da creare.

Puoi usare strumenti come Canva o Microsoft PowerPoint al fine di creare i tuoi contenuti visivi in breve tempo, da condividere con il tuo pubblico. Non aver pausa di condividerli sulle tue piattaforme social per un maggior impatto.

Clicca qui per provare Canva: https://www.canva.com/

Podcast

Negli ultimi cinque anni la prevalenza dei podcast è decuplicata. Se sei seduto a tavola chiedi chi ascolta i contenuti dei podcast e possiamo garantirti che ci sarà un tasso di almeno il 50% di feedback positivi! I podcast sono il modo nuovo e innovativo di ricevere informazioni di ogni genere. Dalla cronaca nera, alla commedia fino alle scienze biologiche se hai interessi strani e particolari, ci sono concrete possibilità che ci sia già un podcast che li abbia trattati nel dettaglio.

Questo tipo di contenuti permette alle persone di assimilare contenuti digitali anche in movimento, ad esempio quando sei fuori per una corsa o bloccato nel traffico, puoi facilmente ascoltare un podcast, continuando a concentrarti sulle tue attività con una buona dose di intrattenimento o istruzione.

Clicca qui per capire come avviare il tuo podcast - https://www.thepodcasthost.com/planning/how-to-start-a-podcast/

*Infine, **Video**!*

Il video è il **RE** del contenuto digitale, nella società visiva di oggi, il video è il modo migliore per entrare in contatto con il tuo pubblico in modo da avere un grande impatto! Si stima che YouTube abbia più di 2 miliardi di utenti attivi AL MESE. Se stai per scegliere un contenuto digitale per cui spendere il tuo tempo e le tue risorse orientati verso la creazione di video. I contenuti video sono molto diversi, adattabili e possono essere molto accattivanti per l'utente. Tutti conosciamo la sensazione di scorrere le pagine social e vedere post e immagini e farci catturare da un video realizzato con immagini immersive, musica e messaggi.

Il video marketing è un fenomeno che intrattiene tutti, YouTube ha generato $19,7 miliardi di incassi da gennaio 2021.[16] TikTok ha superato Facebook, Instagram e SnaPChat diventando la piattaforma social più popolare. Brevi video introduttivi o esplicatori possono essere molto più efficaci al fine di coinvolgere i tuoi utenti, prendendo un po' del loro tempo ricambiandoli con tantissime informazioni!

All'interno di questo modulo discuteremo sul modo in cui registrare i tuoi contenuti video, usando la migliore posizione, le luci e le angolazioni così come le app del telefono che possono rendere la tua vita migliore per la creazione di contenuti di video marketing di alta qualità.

3.2 Integrare e rielaborare i contenuti digitali

Unità 3.2	**Integrare e rielaborare i contenuti digitali**
Durata	2.5 ore
Obiettivi	Presentazione delle tipiche forme della creazione di contenuti e della sua archiviazione. Indicazioni di quelli che sono i modi di pubblicare e mantenere i contenuti su Internet.
Contenuti	Presentazione PowerPoint (**scaricare la presentazione dal sito**) Risorse autonome e flessibili da poter usare lungo il percorso, E-learning
Contenuti	PC, telefono o tablet per l'*E-learning*
Metodo di formazione	Presentazione da parte dell'educatore Presentazione da parte dei partecipanti

Tabella 18: Struttura dell'unità di competenza 3.2. – Integrare e rielaborare i contenuti digitali del Modulo 3 (Creazione di contenuti digitali).

3.2 Integrare e rielaborare i contenuti digitali

Integrazione e creazione di contenuti. Per modificare, perfezionare e integrare nuove informazioni e contenuti all'interno di un bagaglio di conoscenze già esistente e risorse al fine di creare contenuti e saperi nuovi, originali e rilevanti.

Abbiamo affrontato il tema della creazione di contenuti altamente coinvolgenti per il tuo pubblico, considerando il contesto d'uso. Chi stati cercando di raggiungere? Usa i tuoi punti di forza per raggiungere il tuo gruppo target, svolgi qualche ricerca di mercato per essere sicuro di star facendo la giusta scelta per te! Ci occuperemo anche della pubblicazione e dell'archiviazione del contenuto online. Oltre a integrare i tuoi contenuti in risorse già esistenti, ti mostreremo come usare software di produttività e applicazioni per raggiungere questo risultato in modo utile ed efficiente! Utilizzare strumenti già esistenti vuol dire spendere

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

meno denaro ed energie, continuando a perseguire l'obiettivo finale ossia la creazione di contenuti, altamente coinvolgente, andando incontro ai tuoi bisogni e a quelli del tuo pubblico di destinazione!

Come affermato in precedenza, YouTube ha un grande archivio di materiali disponibili pubblicamente che possono essere estremamente utili. I contenuti dei Podcast sono altrettanto disponibili e gratuiti e possono aiutarti ad integrare le risorse che stai creando

Nel capitolo 3.2 ti verranno mostrati diversi strumenti che possono rendere il tuo viaggio verso l'integrazione e l'elaborazione dei contenuti molto più entusiasmante e sicuramente perfetta.

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

Archiviare i tuoi contenuti

Dal momento in cui hai passato il tuo tempo e speso le tue energie creando e integrando i tuoi contenuti digitali, è di fondamentale importanza possedere competenze e conoscenza del posto più sicuro per poter salvare questi contenuti per un accesso più facile e allo stesso tempo sicuro.

La condivisione dei file sul Cloud potrebbe essere uno strumento che fornisce agli utenti l'abilità di accedere ai propri contenuti da qualsiasi dispositivo. Questa flessibilità comporta il fatto che non sei legato ad un PC fisico ed è di massima importanza in uno spazio di lavoro dinamico e mai statico. Scopri Dropbox, Google Drive e One Drive e cambia il modo in cui condividi I tuoi materiali.

Pubblicazione e condivisione

Condividere i tuoi lavori online è un processo di pubblicazione di contenuti su piattaforme online., che siano un canale YouTube o il tuo sito personale o una pagina di un blog o ancora il tuo account social. I contenuti pubblicati possono contenere testo, immagini, video e altri tipi di supporti digitali.

La pubblicazione online può essere a basso costo, altamente efficace ed efficiente per il tuo uso; quindi, possiamo aiutarti a trovare gli strumenti migliori per pubblicare i tuoi contenuti. Scopri maggiori informazioni su WIX, WordPress, Linkedin e Pinterest.

3.3 Copyright e licenze

Unità 3.3	Copyright e licenze
Durata	2.5h
Obiettivi	Il copyright è un tipo di diritto di proprietà intellettuale (DPI) che fornisce protezione riguardo qualcosa: • che puoi creare • posseduta da una o più persone o un'azienda
Contenuti	Risorse autonome e flessibili da poter usare lungo il percorso, E-learning
Risorse	Presentazione PowerPoint (scaricare la presentazione dal sito) PC, telefono o tablet per l'*E-learning*
Metodo di formazione	Presentazione da parte dell'educatore

Tabella 19: Struttura dell'unità di competenza 3.3.- Copyright e licenze del Modulo 3 (Creazione di contenuti digitali).

3.3 Copyright e licenze

Cos'è il copyright?

Il possesso del copyright fornisce al proprietario il diritto esclusivo di utilizzare un'opera, con alcune eccezioni. Quando una persona crea un lavoro originale, all'interno di un supporto tangibile, possiede automaticamente il copyright dell'opera:

Alcuni tipi di lavori hanno i requisiti per la protezione da copyright, ad esempio:

- Opere audiovisive, come programmi TV, film, video online
- Registrazioni sonore e composizioni musicali
- Opere scritte, come letture, articoli, libri e composizioni musicali
- Opere visive, come disegni, poster e pubblicità
- Videogame e software informatici
- Opere teatrali come spettacoli e musical.

È possibile usare un'opera protetto da copyright senza commettere violazioni?

Si, in alcuni casi, è possibile usare un'opera protetta da copyright senza violare i diritti del proprietario. Alcuni creatori di contenuti scelgono di rendere le proprie opere disponibili per l'utilizzo con il rispetto di alcune condizioni. Per saperne di più potrebbe interessarti conoscere la *Creative Commons license*.[17]

Le norme sul copyright dell'Unione Europea

Le norme sul copyright dell'Unione Europea sono leggi applicabili all'interno dell'Unione Europea. Le norme relative al diritto d'autore sono uniformi, nonostante ci sia qualche differenza di Paese in Paese. Il corpus normativo è stato implementato nell'UE attraverso diverse direttive, che gli Stati membri devono emanare all'interno delle legislazioni nazionali. Le principali direttive relative al copyright sono la Direttiva sui diritti d'autore, la Direttiva concernente l'armonizzazione della durata di protezione del diritto d'autore e di alcuni diritti connessi e la Direttiva sul diritto d'autore nel mercato unico digitale.[18]

Le norme sui diritti d'autore dell'UE consistono in 11 direttive e 2 statuti che conciliano i diritti essenziali di autori, artisti, produttori ed emittenti. Creando standard comuni, le norme sui diritti d'autore dell'UE riducono le discrepanze nazionali e garantiscono il livello di protezione richiesto al fine di dare spazio alla creatività e all'investimento della stessa. Standard comuni promuovono la diversità culturale e permettono un migliore accesso, ai consumatori e alle imprese, ai contenuti digitali e ai servizi in tutta Europa.[19]

All'interno del capitolo 3.3 approfondimento i requisiti del copyright, il modo di utilizzare una *creative common license* e come questi tipi di licenze possano essere utili ai tuoi contenuti!

[17] https://support.google.com/legal/answer/3463239?hl=en-GB

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

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

3.4 Programmazione

Unità 3.4	Programmazione
Durata	2.5 ore
Obiettivi	L'obiettivo di questo modulo è quello di capire le strutture principali del linguaggio Python.
Contenuti	Risorse autonome e flessibili da poter usare lungo il percorso, E-learning
Risorse	Presentazione PowerPoint (**scaricare la presentazione dal sito**) PC, telefono o tablet per l'E-learning
Metodo di formazione	Presentazione da parte dell'educatore Insegnamento capovolto

Tabella 20: Struttura dell'unità di competenza 3.4. – Programmazione del Modulo 3 (Creazione di contenuti digitali).

3.4 Principi fondamentali di programmazione e *coding*

Cosa significa programmare a basso livello?

La codificazione è una letteratura basilare nell'epoca digitale e, per ogni individuo è fondamentale essere in grado di codificare con semplicità e utilizzare la tecnologia attorno a sé. Esistono diversi linguaggi di codificazione. Noi abbiamo scelto Python. Python è semplice e intuitivo da apprendere grazie alla sua sintassi e alla sua leggibilità chiare.

Python è un linguaggio di programmazione potente e facile da comprendere.

Python è un linguaggio di programmazione in vigore facile da capire e potente. Durante la scrittura del codice, ti focalizzerai principalmente nella risoluzione del problema, non sulla sintassi e struttura del linguaggio in cui programmerai.

Variabili in Python

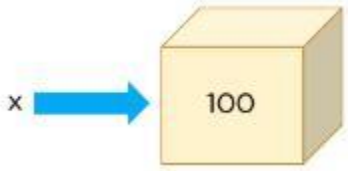
1. Operatore di assegnazione della variabile

La Variabile è un concetto fondamentale di qualsiasi linguaggio di programmazione. Si tratta di una locazione di memoria riservata che immagazzina e modifica i dati. Pensa alla variabile come un nome associato ad un oggetto in particolare. In Python, le variabili non hanno bisogno di essere dichiarate o definite in anticipo, come avviene in diversi altri linguaggi di programmazione. Per creare una variabile, dovrai semplicemente assegnarle un valore e iniziare ad utilizzarla. Un compito viene assegnato con un singolo segno di uguale (=):

Le variabili sono la struttura di un programma che detiene un valore. Ecco un esempio di variabile:

x=100

Nella figura sottostante, la scatola detiene il valore di 100 ed è denominata x. Inoltre, la variabile è x e i dati che contiene corrispondono al valore.



La tipologia di dati per una variabile corrisponde alla tipologia di dati che la stessa ha. [20]

Nell'esempio sopra, x ha un valore di 100, che rappresenta un numero e la tipologia di dati di x è un numero.

In Python, esistono tre tipi di numeri: interi, in virgola mobile (Float) e complessi.

Gli Interi sono i numeri senza cifre decimali. I numeri In virgola mobile sono quelli con cifre decimali. I numeri complessi sono quelli contenenti una parte reale e una parte immaginaria.

Un'altra tipologia di dati, completamente differente dai numeri è chiamata stringa, formata da una raccolta di caratteri.

Vediamo ora una variabile con una tipologia di dati interi:

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

x=100

Per verificare la tipologia di dati di x, utilizza la funzione type ():

type(x)

Python ti permette di assegnare delle variabili durante lo svolgimento di operazioni aritmetiche.

x=654*6734

type(x)

Per visualizzare il risultato della variabile, utilizza la funzione print().

Print(x) #Restituisce il prodotto dei due numeri

Ora vediamo un esempio di un numero in virgola mobile (float):

x=3.14

print(x)

type(x) #Qui la variabile è float

```
x=3.14

print(x)

3.14

type(x)

float
```

Le Stringhe sono dichiarate all'interno di una riga singola o doppia.

x='Simplilearn'

print(x)

x=" Simplilearn."

print(x)

type(x)

```
x='Simplilearn'
print(x)

Simplilearn

x="Simplilearn"
print(x)

Simplilearn

type(x)

str
```

Per saperne di più, ecco il link di una pagina interessante con delle eccellenti infografiche:

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

Congratulazioni, hai completato il Modulo 3.

Non dimenticarti di controllare le Appendici per maggiori risorse e documenti forniti al fine di supportare lo studio da autodidatta!

Modulo 4: Sicurezza

Il Modulo 4 è incentrato sulla sicurezza online e ha lo scopo ti portare la tua attenzione su questo problema, oltre a fornire informazioni su come ridurre i rischi e mantenere un buon livello di sicurezza.

Si prega di notare come le unità descritte possano prevedere il supporto di un docente esperto. Nonostante le informazioni presenti nel manuale siano scritte in maniera da comprenderle facilmente, alcune azioni, inerenti alle informazioni presentate, potrebbero richiedere la supervisione e il supporto di esperti.

Modulo 4	**Sicurezza**			
Durata	**25h**			
Obiettivi	All'interno della presente unità, allo studente verrà insegnato a: • Proteggere dispositivi, contenuti, dati personali e privacy in ambienti digitali; • Proteggere la salute fisica e psicologica ed essere consapevoli delle tecnologie digitali per il benessere e l'inclusione sociale; • Essere consapevoli dell'impatto ambientale delle tecnologie digitali e del loro uso.			
Unità	4.1 Proteggere i dispositivi	4.2 Proteggere i dati personali e la privacy	4.3 Proteggere la salute e il benessere	4.4 Proteggere l'ambiente
Organizzazione della formazione	Lezioni frontali *E-Learning* *B-learning*	Lezioni frontali *E-Learning* *B-learning*	Lezioni frontali *E-Learning* *B-learning*	Lezioni frontali *E-Learning* *B-learning*
Durata	6h	9h	5h	5h

Tabella 21: Struttura generale del Modulo 4: Sicurezza.

4.1 Proteggere i dispositivi

Unità 4.1	Proteggere i dispositivi
Durata	6h
Obiettivi	Capire che un computer è incline ad attacchi informatici di rete Sapere in che modo creare una password sicura Essere in grado di installare un browser Chrome ed aggiornarlo periodicamente Capire lo sforzo che l'occhio umano fa per leggere informazioni da dispositivi elettronici Capire che una posizione lavorativa sorretta piò portare a problemi alla spina dorsale. Capire i costi operativi degli strumenti Capire che i componenti elettronici fisici non sono amici dell'ambiente.
Contenuti	4.1.1 Dispositivi di protezione 4.1.2 Aggiornamenti software 4.1.3 Password e sicurezza 4.1.4 Aumentare la sicurezza 4.1.5 Cos'è il codice maligno? 4.1.6 Attività pratiche
Risorse	Manuale di formazione Computer con accesso a Internet Programma di editing Carta e penna
Metodo di formazione	Presentazione da parte dell'educatore Selezione dei contenuti

Tabella 22: Struttura dell'unità di competenza 4.1. – Proteggere i dispositivi del Modulo 4 (Sicurezza).

4.1.1 Dispositivi di protezione

Perché la sicurezza informatica è così importante?

Considerando che i computer hanno un ruolo critico nella nostra vita e visto che vediamo e inseriamo così tante informazioni personali rintracciabili, migliorare e mantenere la sicurezza del computer diventa un imperativo. Una maggior sicurezza informatica garantisce una più sicura elaborazione e archiviazione delle nostre informazioni.

Come posso migliorare la sicurezza del mio computer?

I prossimi sono passaggi importanti che dovresti considerare al fine di rendere più sicuro il tuo computer. Mentre un singolo passaggio non eliminerebbe alcun rischio, se usati insieme, queste pratiche di difesa aumentata aumenteranno la sicurezza del tuo computer aiutandoti a minimizzare le minacce.

➢ Proteggi la rete domestica

Quando connetti un computer a Internet si connette anche a milioni di altri computer (una connessione che potrebbe permettere agli hacker di avere accesso al tuo computer). Nonostante i router cablati, le DSL (*digital subscriber lines*) e gli ISP (*Internet service providers*) abbiano un certo livello di sicurezza, è cruciale proteggere il tuo router (il primo dispositivo in assoluto che riceve informazioni dall'Internet). Assicurati di proteggerlo prima di connetterti alla rete in modo da implementare la sicurezza del tuo computer.
Cos'è la sicurezza della rete domestica e perché dovrebbe interessarmi?

➢ Sicurezza della rete domestica

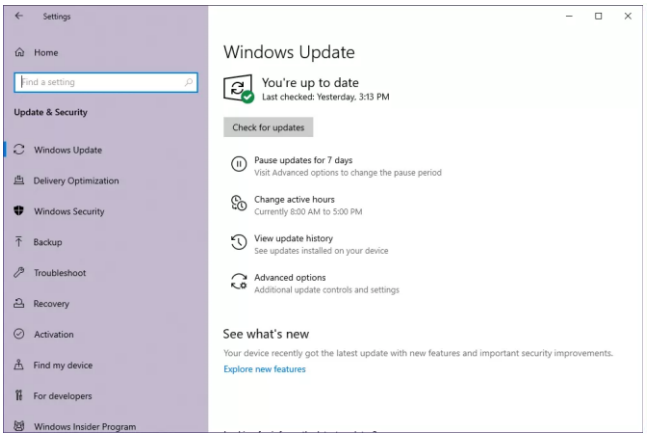
La sicurezza della rete domestica fa riferimento alla protezione di una rete che connette i dispositivi (router, computer, smartphone, apparecchi domestici, baby monitor Wi-Fi, telecamere) gli uni agli altri e a Internet, all'interno di una casa.
Molti utenti condividono due preconcetti comuni riguardanti la sicurezza delle proprie reti di comunicazione:

- La loro rete domestica è troppo piccola per essere a rischio di un attacco informatico
- I loro dispositivi sono "sicuri a sufficienza" fin dal primo utilizzo.

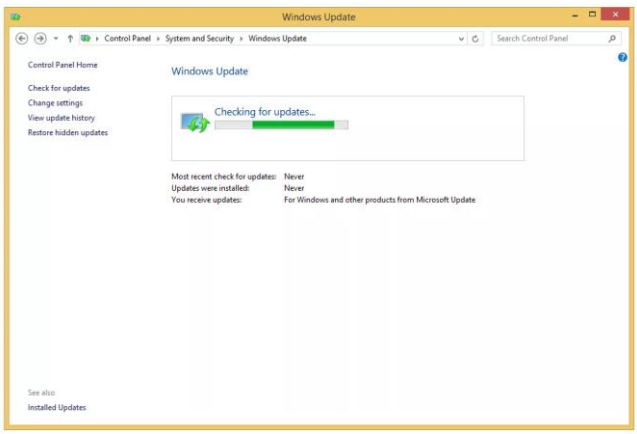
Molti attacchi non sono di natura personale e possono avvenire su ogni tipo di rete, piccola o grande, domestica o aziendale. Se una rete di comunicazione si collega ad Internet è sicuramente più vulnerabile e suscettibile alle minacce esterne.
IN che modo posso migliorare la sicurezza della mia rete domestica?
Seguendo alcune delle tecniche di mitigazione dei rischi sottostanti, semplici ma efficaci. Puoi ridurre in maniera importante la portata dell'attacco della tua rete domestica e rendere più difficile il lancio di un attacco informatico di successo ad un hacker.

➢ Aggiorna regolarmente il software

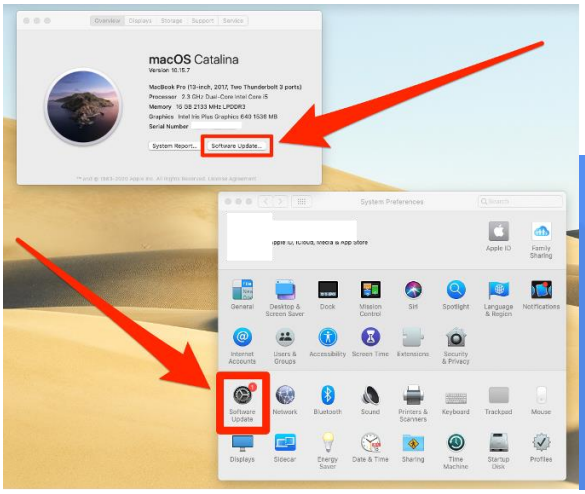
Gli aggiornamenti software regolari sono il passo più efficacie che tu possa fare per migliorare la sicurezza informatica dell'intera rete domestica e dei tuoi sistemi. Oltre ad aggiungere nuove caratteristiche e funzionalità, gli aggiornamenti software spesso includono patch critiche e aggiornamenti di sicurezza per soccombere alle nuove minacce e vulnerabilità. Le applicazioni software più moderne controlleranno automaticamente la disponibilità di aggiornamenti. Se gli aggiornamenti automatici non sono disponibili, considera l'idea di acquistare un programma software che identifichi e gestisca contemporaneamente tutti gli aggiornamenti dei software installati.



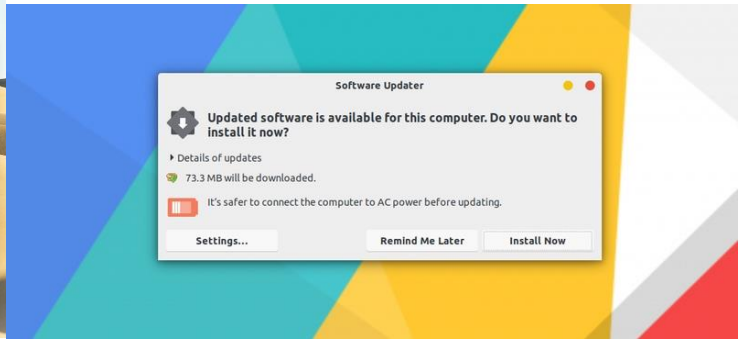
Windows 10



Windows 8,7, Vista



Aggiornamento MacOS



Aggiornamento Ubuntu (Linux)

Cosa sono le patch?

Le patch sono software e aggiornamenti di sistemi operativi (OS) che lavorano sulle vulnerabilità della sicurezza all'interno di un programma o di un prodotto. I venditori di software potrebbero scegliere di rilasciare un aggiornamento per sistemare i bug nelle prestazioni ma anche fornire funzionalità di sicurezza avanzata.

4.1.2 Aggiornamenti software

Come capire quale aggiornamento software devi installare?

Dal momento in cui sono disponibili gli aggiornamenti software, i produttori provvedono a metterli sui loro siti web in modo che gli utenti effettuino il download. Installa gli aggiornamenti il prima possibile al fine di proteggere il tuo computer, il telefono o un dispositivo digitale contro gli hacker che altrimenti sfrutterebbero le vulnerabilità del sistema. Gli hacker potrebbero osservare le vulnerabilità per mesi o addirittura anni dopo l'uscita degli aggiornamenti.

Alcuni software controllano automaticamente gli aggiornamenti, e molti produttori offrono agli utenti la possibilità di ricevere aggiornamenti automatici. Se le opzioni automatiche sono disponibili puoi sfruttarle al meglio. Se non sono disponibili, controlla periodicamente la disponibilità di aggiornamenti sul sito web del tuo produttore.

Assicurati di scaricare aggiornamenti software solo da siti web affidabili. Non fidarti di link contenuti all'interno di e-mail (gli hacker hanno usato messaggi e-mail per indirizzare gli utenti verso siti web con file maligni travestiti da aggiornamenti legittimi). Gli utenti dovrebbero inoltre diffidare da messaggi e-mail in cui è allegato un aggiornamento di sistema (questi allegati potrebbero contenere malware).

Se possibile, utilizza aggiornamenti automatici provenienti solo da reti conosciute (casa, lavoro). Evita di aggiornare il software (automaticamente o manualmente) se sei connesso a reti poco attendibili (aeroporto, hotel, bar). Se gli aggiornamenti devono essere installati con una rete non attendibile usa una rete VPN (*Virtual Private Network)* e scarica gli aggiornamenti.

Qual è la differenza tra un aggiornamento manuale e uno automatico?

Gli utenti possono installare gli aggiornamenti manualmente oppure optare per l'aggiornamento automatico.

Gli aggiornamenti manuali richiedono all'utente o all'amministrazione di visitare il sito web del produttore al fine di scaricare e installare i file del software.

Gli aggiornamenti automatici richiedono il consenso dell'utente o dell'amministratore durante l'installazione o la configurazione del software. Una volta dato il consenso, gli aggiornamenti di sistema vengono installati automaticamente.

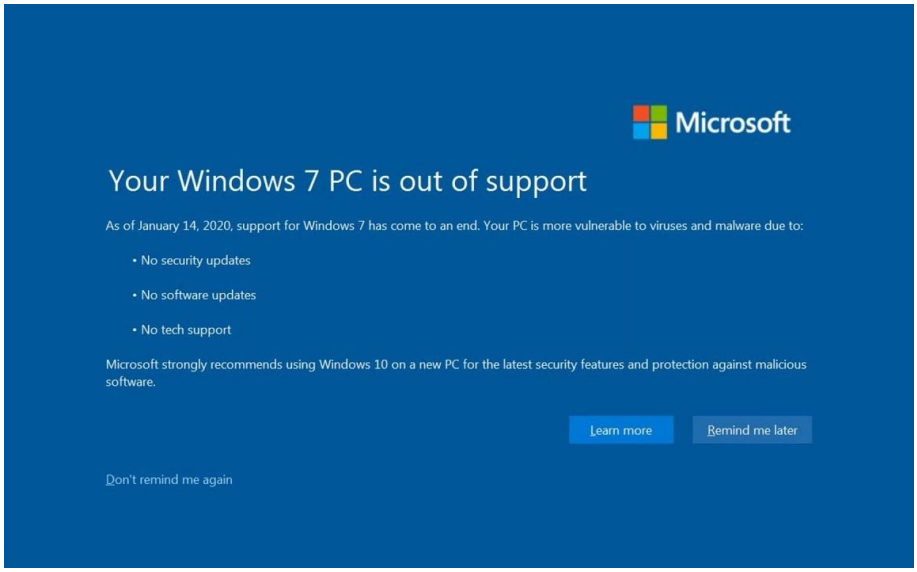
Cos'è un software a fine vita?

A volte i produttori smettono di darti supporto per gli aggiornamenti di un programma o di un software (conosciuti anche come software a fine vita – EOL). Un uso continuo di software EOL pone conseguenti rischi al tuo sistema permettendo agli hacker di sfruttare le vulnerabilità della sicurezza. L'uso di software non supportati

può inoltre causare problemi di incompatibilità di software così come una diminuzione delle performance e della produttività del sistema.

Buone pratiche per gli aggiornamenti di sistema

- Abilita gli aggiornamenti automatici di sistema quando possibile. Questo assicura che gli aggiornamenti siano installati il più velocemente possibile.
- Non usare software EOL non supportarti.
- Visita sempre i siti dei fornitori invece di cliccare sulle pubblicità o link di e-mail
- Evita aggiornamenti di sistema quando usi reti sconosciute.
- Emergono sempre nuove vulnerabilità ma la miglior difesa contro gli hacker che sfruttano le vulnerabilità delle patch è semplice: mantieni aggiornato il tuo software. Questa è la misura più efficace da adottare al fine di proteggere il tuo computer, telefono o altri dispositivi elettronici.



Windows 7 EOL

Rimuovi i servizi e i software non necessari

Disabilità tutti i servizi non necessari al fine di ridurre la portata degli attacchi alla tua rete e ai tuoi dispositivi, incluso il router. Servizi e software non utilizzati o non voluti possono creare mancanze di sicurezza nel sistema di un dispositivo, che potrebbe portare ad un maggiore spazio di attacco dell'ambiente della tua rete. Questo è particolarmente vero con i nuovi sistemi informatici in cui i fornitori spesso preinstallano un grande numero di applicazioni e software di prova, definiti *bloatware* che gli utenti potrebbero non trovare utili.

Sistemare la configurazione delle impostazioni di fabbrica su software e hardware

Alcuni prodotti software e hardware “escono dalla scatola” con configurazioni di fabbrica troppo permissive con lo scopo di essere user-friendly e ridurre i tempi di risoluzione dei problemi per il servizio clienti. Sfortunatamente, queste configurazioni di default non sono orientate verso la sicurezza. Lasciarle abilitate dopo l’installazione potrebbe favorire la creazione di strade che un hacker potrebbe percorrere. Gli utenti dovrebbero prendere provvedimenti per rinforzare i parametri delle configurazioni di default al fine di ridurre le vulnerabilità e proteggersi dalle intrusioni.

4.1.3 Password e sicurezza

Cambia gli username e le password di default per i tuoi log-in

La maggior parte dei dispositivi di rete è preconfigurata con password di amministratore di default per semplificarne la configurazione. Queste credenziali di default non sono sicure, poiché potrebbero essere disponibili immediatamente in Internet o potrebbero essere fisicamente stampate sull’etichetta del dispositivo stesso. Lasciando queste password invariate, apriresti la strada a potenziali attacchi informatici da parte di attori che otterrebbero l’accesso non autorizzato alle informazioni, installerebbero software dannosi e potrebbero causare altri problemi.

Utilizza password uniche e sicure

Scegli password sicure per contribuire a proteggere il tuo dispositivo. Inoltre, non usare la stessa password per account diversi. In questo modo, se uno dei tuoi account risulta compromesso, l’hacker non sarà in grado di entrare negli altri tuoi account.

Perché hai bisogno di password sicure?

Molto probabilmente, ogni giorno userai dei numeri di identificazione personale (PIN), password o *passphrase*: dai prelievi agli sportelli bancomat, all’utilizzo della tua carta di debito nei negozi, al login nella tua mail o nel sito di un venditore online. Tenere traccia di tutti i numeri, delle lettere e delle combinazioni di parole può essere frustrante, ma queste forme di protezione sono fondamentali perché gli hacker rappresentano una minaccia concreta per le tue informazioni. Molto spesso, un attacco non mira nello specifico al tuo account ma all’ottenimento delle tue informazioni per lanciare un attacco più grande.

Uno dei modi migliori per proteggere le informazioni o la proprietà fisica e quello di assicurarsi che solamente le persone autorizzate vi abbiano accesso. Il prossimo passo è quello di verificare che le persone che richiedono

l'accesso siano chi dicono di essere. Questo processo di autenticazione è più importante e più difficile nel mondo digitale. Le password sono il mezzo più comune di autenticazione, ma funzionano solamente se sono complesse e confidenziali. Diversi sistemi e servizi sono stati violati con successo a causa di password non sicure e inadeguate. Una volta che il sistema è compromesso, esso è aperto allo sfruttamento da parte di altre fonti indesiderate.

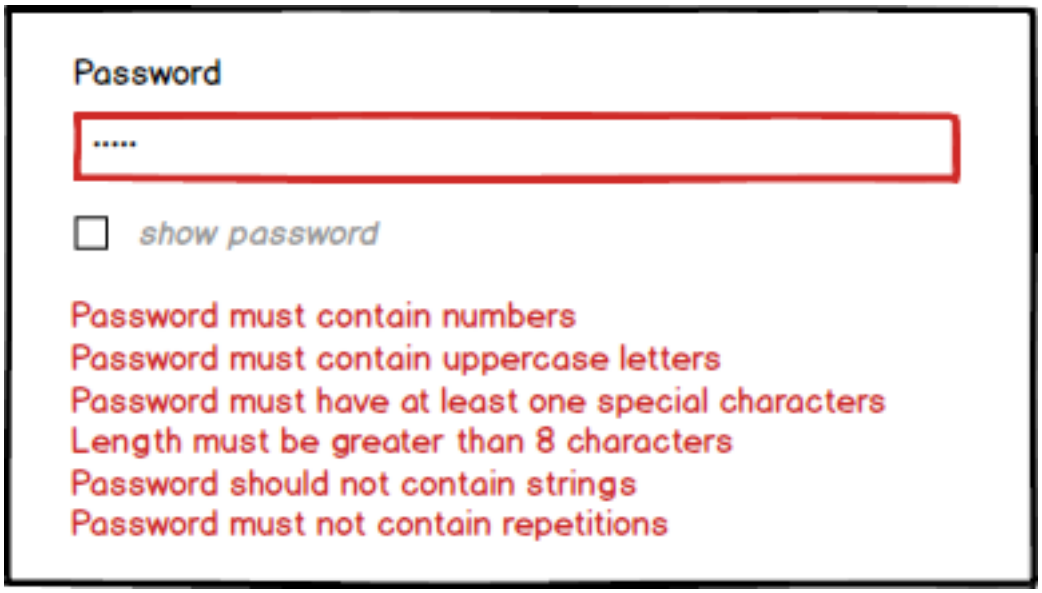
Evitare gli errori comuni

La maggior parte delle persone utilizza password basate su informazioni personali, facili da ricordare. Ad ogni modo, questo rende più semplice il lavoro di un hacker che se ne vuole impossessare. Considera un PIN di quattro cifre. Si tratta di una combinazione del mese, del giorno o dell'anno della data del vostro compleanno? Contiene per caso il vostro indirizzo o il vostro numero di telefono? Pensa a quanto sia semplice trovare la data di nascita di qualcuno o informazioni simili. E la password della tua casella e-mail? Si tratta di una parola che può essere trovata sul dizionario? Se così fosse, potrebbe essere suscettibile ad un attacco a dizionario, che cerca di indovinare password basate su frasi o parole comuni.

Nonostante possa essere fatto in maniera involontaria, un errore di battitura ("datta" invece di "data"), potrebbe offrire una forma di protezione contro gli attacchi a dizionario; un ulteriore metodo, ancora più efficace, è quello di affidarsi ad una serie di parole e utilizzare le tecniche di memoria o mnemoniche, per aiutarti a decodificarle. Per esempio, invece della password "hoops", utilizza "IlTpbb" per la frase ""[I] [l]ike [T]o [p]lay [b]asket[b]all." Utilizzando sia le lettere maiuscole che quelle minuscole, aggiungerai un ulteriore livello di segretezza. Modificando lo stesso esempio utilizzato sopra in "Il!2pBb." creerai una password molto diversa da una qualsiasi parola di dizionario.

Lunghezza e difficoltà

Dovresti considerare l'idea di utilizzare la password o la *passphrase* più lunga possibile (8-64 caratteri) quando puoi. Ad esempio, "Pattern2baseball#4mYmiemale!" sarebbe una password forte perché ha 28 caratteri e incluse lettere maiuscole e minuscole, numeri e caratteri speciali. Potresti aver bisogno di provare diverse varianti di una *passphrase*, ad esempio, alcune applicazioni limitano la lunghezza delle password e altre non accettano spazi o alcuni caratteri speciali. Evita le frasi comuni, le domande famose e i testi delle canzoni.



Cose da fare e da non fare

Una volta inventata una password sicura e facile da ricordare è arrivato il momento di utilizzarla di nuovo. Non farlo! Riutilizzare una password, anche una forte, mette a rischio i tuoi account così come usare una password debole. Se gli hacker indovinassero la tua password, avrebbero accesso a tutti i tuoi account con la stessa password. Usa le seguenti tecniche per creare password uniche per ognuno dei tuoi account:

- Usa password diverse su diversi sistemi e account.
- Usa la password o la *passphrase* più lunga possibile per ogni sistema.
- Sviluppa una memoria mnemonica al fine di ricordare le password complesse.
- Considera l'idea di usare un programma per password al fine di tener traccia delle tue password (maggiori informazioni qui sotto).
- Non usare password basate sulle informazioni personali che possano essere facilmente indovinate o scoperte.
- Non usare parole che possano essere trovate sui dizionari di qualsiasi lingua.

Come proteggere le tue password

Dopo aver scelto una password facile da ricordare ma difficile da indovinare non scriverla e lasciarla in un posto in cui gli altri possono trovarla. Scriverla e lasciarla sulla tua scrivania, di fianco al computer, o peggio, incollata al tuo computer, la rende più accessibile a qualcuno con un accesso fisico al tuo ufficio. Non dire la tua password a nessuno, e attento agli hacker che ti ingannano attraverso chiamate telefoniche o messaggi in cui ti chiedono di dire loro le tue password.

I programmi chiamati gestori di password offrono la possibilità di creare password generate casualmente per tutti i tuoi account. Puoi così avere accesso a queste password forti con una password master. Se usi un gestore di password, ricordati di usare una password master forte.

I problemi relativi alla password possono derivare dall'abilità dei tuoi browser di salvare le password e le tue sessioni online nella loro memoria. In base alle impostazioni del tuo browser, ognuno con l'accesso al tuo computer potrebbe essere in grado di scoprire tutte le tue password e avere accesso alle tue informazioni. Ricordati sempre di effettuare il log out quando usi un computer pubblico (in biblioteca, in un bar, ma anche un computer condiviso in ufficio). Evita di usare computer pubblici e connessioni Wi-Fi pubbliche per accedere ad account sensibili come Internet banking o la casella mail.

Non vi è garanzia che queste tecniche vietino ad un hacker di conoscere la tua password, ma sicuramente lo renderanno molto più difficile.

Non dimenticare i principi fondamentali relativi alla sicurezza

- Mantieni il tuo Sistema operativo, il browser e gli altri software aggiornati.
- Utilizza e mantieni il software antivirus e il firewall.
- Effettua una scansione regolare per la ricerca di spyware (alcuni programmi antivirus hanno il rilevamento spyware)
- Stai attento agli allegati e-mail e ai link sospetti
- Tieni d'occhio le attività sospette sui tuoi account.

4.1.4 Aumentare la sicurezza

Esegui un software antivirus aggiornato

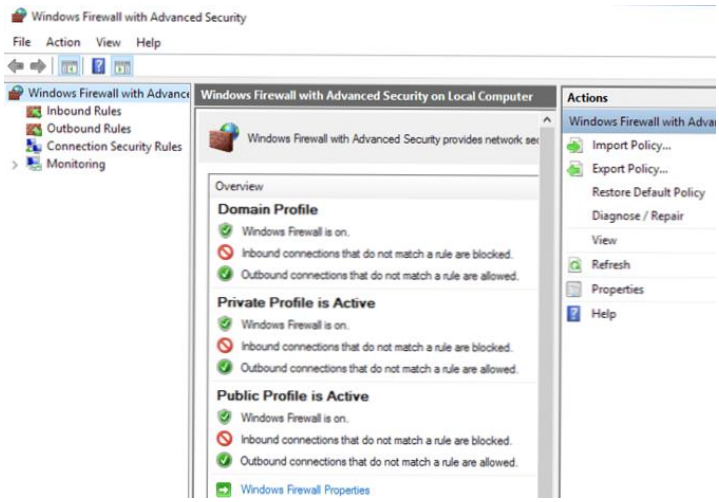
L'utilizzo di un software antivirus affidabile è una misura di protezione importante contro le minacce pericolose. Può automaticamente rilevare, mettere in quarantena e rimuovere diversi tipi di malware, come virus, *worm* e *ransomware*. Alcune soluzioni antivirus sono estremamente facili da installare e intuitive. Si raccomanda di eseguire un software antivirus su tutti i computer e i dispositivi mobili di casa tua. Inoltre, assicurati di consentire gli aggiornamenti automatici della definizione dei virus per assicurare la massima protezione contro le nuove minacce. Nota bene: visto che l'individuazione dei virus è basata su firma (modelli conosciuti che possono identificare un codice come malware) anche i migliori antivirus potrebbero non essere in grado di proteggerti adeguatamente da minacce nuove e avanzate, come gli attacchi *0-day* e i virus polimorfi.

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

Installa un firewall di rete

Installa un firewall delimitando la rete domestica per difenderti dalle minacce esterne. Un firewall può bloccare i traffici dannosi così da non entrare nella tua rete domestica avvisandoti dell'attività potenzialmente pericolosa. Se adeguatamente configurato, il firewall può fungere anche da barriera per le minacce esterne, evitando che software indesiderati o dannosi entrino attraverso Internet. Molti router Wi-Fi hanno un firewall di rete integrato, configurabile, che include funzionalità aggiuntive (difesa tramite controllo accessi, *web-filtering* e il *denial-of-service,* DoS) che puoi personalizzare al meglio per il tuo ambiente di rete. Ricorda che alcune funzionalità firewall, incluso lo stesso firewall, potrebbero essere spente di default. Assicurarsi che il firewall sia acceso e che tutte le funzionalità siano adeguatamente configurate rafforzerà la sicurezza della tua rete. Nota bene: il tuo fornitore di servizi Internet (ISP) potrebbe aiutarti a determinare quando il tuo firewall ha i parametri più appropriati per i tuoi dispositivi e per l'ambiente.

Oltre al firewall di rete, considera l'idea di installare un firewall su tutti i computer connessi alla tua rete. Spesso riferiti a *host*- o *software-based* virus, questi firewall ispezionano e filtrano il traffico di rete in entrata e in uscita basato su politiche o regole predefinite. I sistemi operativi più moderni di Windows e Linux hanno già un firewall integrato, personalizzabile e ricco di funzionalità. Inoltre, molti produttori arricchiscono i loro pacchetti di antivirus con funzionalità di sicurezza aggiuntive come il *parental control*, la protezione delle mail e il blocco dei siti web potenzialmente pericolosi.



Esegui il backup dei dati regolarmente

Esegui e salva regolarmente copie di backup (usando memorie esterne o servizi cloud) di tutte le informazioni del tuo dispositivo. Considera l'idea di utilizzare un servizio backup di applicazione di terze parti, che può semplificare e automatizzare il processo. Assicurati di crittografare il tuo backup al fine di proteggere la confidenzialità e l'integrità delle tue informazioni. I backup di dati sono cruciali al fine di minimizzare l'impatto nel caso di perdita, corruzione, infezione o furto dei dati.

Aumenta la sicurezza wireless

Potresti aver bisogno di consultare le istruzioni del tuo router o contattare il tuo fornitore di servizi per istruzioni specifiche su come cambiare una particolare impostazione sul tuo dispositivo.

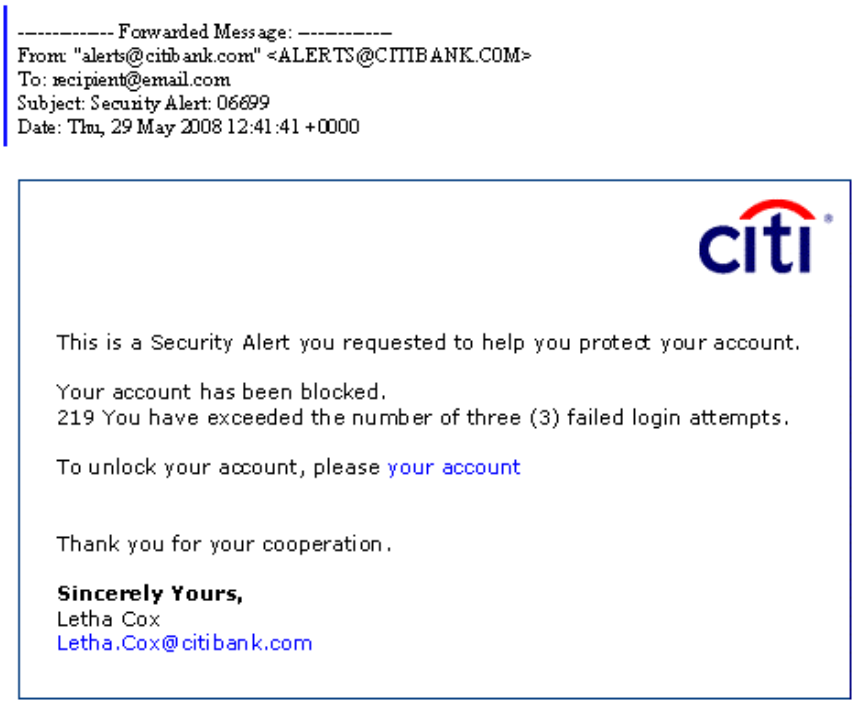
Usa il protocollo di crittografia più sicuro disponibile. Si raccomandano il *Wi-Fi Protected Access 3* (WPA3) il *Personal Advanced Encryption Standard* (AES) e il *Temporary Key Integrity Protocol* (TKIP), che è la configurazione router per uso domestico più sicura al momento disponibile. Comprende l'AES ed è in grado di utilizzare le chiavi crittografiche di 128, 192 e 256 bit. Questo standard è stato approvato dal *National Institute of Standards and Technology* (NIST).
Cambia la password di default dell'amministratore del router. Cambia la tua password di default dell'amministratore del router per aiutarti a proteggerlo da attacchi usando le credenziali di default
Cambia il *service set identifier* (SSID) di default. Alcune volte denominata "nome della rete," una SSID è un nome unico che identifica una particolare *wireless local area network* (rete senza fili di area locale) (WLAN). Tutti I dispositive wireless su una WLAN devono usare la stessa SSID per poter comunicare. Visto che la SSID di default del dispositivo fa tipicamente riferimento al produttore o al dispositivo corrente, un hacker potrebbe usarla per identificare il dispositivo e sfruttarne le vulnerabilità. Assicurati che la tua SSID sia unica e non collegata alla tua identità o alla tua posizione, altrimenti sarebbe più semplice per un hacker identificare la tua rete domestica.

Disabilita il *Wi-Fi Protected Setup* (WPS). Il WPS fornisce meccanismi semplificati affinché un dispositivo wireless si unisca alla rete Wi-Fi senza dover inserire password. Tuttavia, un difetto di progettazione all'interno delle specifiche del WPS relativo all'autenticazione del PIN riduce esponenzialmente il tempo in cui un hacker possa forzare il PIN, perché questo lo informa quando la prima parte del PIN ad 8 caratteri è corretto. Molti router non hanno una giusta politica di blocco dopo un numero di tentativi sbagliati, facilitando l'attuazione di un attacco forzato. Vedi attacchi di forza bruta effettuati da hacker.
Riduci la forza del segnale wireless. Il tuo segnare Wi-Fi si propaga molto spesso oltre il perimetro di casa tua. L'emissione di segnale estesa permette l'intercettazione della rete da parte di terze persone fuori dal tuo perimetro di rete. Inoltre, pensa attentamente alla posizione dell'antenna, al tipo di antenna e ai livelli di trasmissione. Fare prove con la posizione del router e con i vari livelli di potenza del segnale puoi ridurre la copertura della tua rete Wi-Fi e ridurre i rischi di compromissione. Nota bene: mentre questo riduce i tuoi rischi, un hacker motivato potrebbe ancora essere in grado di intercettare un segnale con copertura limitata.
Spegni la rete quando non la usi. Spegnere e accendere il segnale Wi-Fi potrebbe risultare scomodo, quindi, prova a considerare l'idea di disabilitarlo quando viaggi o durante lunghi periodi di assenza online. Inoltre, molti router offrono l'opzione di configurare un timer wireless che spegne automaticamente il Wi-Fi ad orari precisi. Quando il tuo Wi-Fi è disabilitato, gli hacker non riescono a sfruttare la tua rete domestica.
Disabilita l'Universal Plug and Play (UPnP) se non necessario. L'UPnP è una funzionalità utile che permette ai dispositivi connessi alla rete di scoprire e stabilire una comunicazione tra di loro sulla rete. Tuttavia, nonostante le funzionalità UPnP facilitino la configurazione iniziale della rete, potrebbe essere anche un rischio di sicurezza. I recenti attacchi alle reti su larga scala provano che i malware all'interno della tua rete possono usare L'UPnP per bypassare il firewall del tuo router, permettendo agli hacker di prendere il controllo dei tuoi dispositivi da remoto e diffondere i malware ad altri dispositivi. Non dovresti comunque disabilitare l'UPnP a meno che tu non ne abbia bisogno.
Aggiorna il firmware. Controlla il sito web del produttore del tuo router per essere sicuro di avere l'ultima versione del firmware. Gli aggiornamenti firmware migliorano le performance del prodotto, sistemano gli errori e mirano alle vulnerabilità relative alla sicurezza. Nota bene: alcuni router hanno l'opzione di aggiornamento automatico.
Disabilita la gestione da remoto. La maggior parte dei router offrono l'opzione di vedere e modificare le impostazioni relative a Internet. Disabilita questa funzione al fine di proteggerti dagli accesi non autorizzati da parte di altre persone e da cambiamento di configurazione del router.
Controlla le connessioni dei dispositivi sconosciuti. Usa il sito web del produttore per controllare i dispositivi non autorizzati che cercano accedere alla tua rete. Controlla il sito web del produttore anche per suggerimenti relativi alla prevenzione riguardante la connessione alla tua rete di dispositivi non autorizzati.

Mitiga le minacce via mail

Le e-mail di phishing continuano ad essere uno dei vettori di attacco iniziale più comuni utilizzati per il trasporto dei malware e l'ottenimento delle credenziali. L'attacco alla componente umana (considerata la più debole nella maggior parte delle reti) continua ad essere estremamente efficace. Per infettare il sistema l'hacker deve semplicemente convincere l'utente a cliccare un link o aprire un allegato. La buona notizia è che ci sono diversi indicatori che puoi usare per identificare rapidamente un'e-mail di phishing. La miglior difesa contro questi

attacchi consiste nel diventare un utente formato in materia e cauto e prendere confidenza con gli elementi più comuni di un attacco 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

Evitare gli attacchi di ingegneria sociale

Non fornire informazioni sensibili ad altri a meno che tu non sia sicuro che loro siano effettivamente chi dicono di essere e debbano avere accesso alle informazioni stesse.

Che cos'è un attacco di ingegneria sociale?

In un attacco di ingegneria sociale, un hacker utilizza l'interazione umana (abilità sociali) per ottenere o compromettere informazioni riguardanti un'azienda o i suoi sistemi informatici. Un hacker potrebbe sembrare senza pretese e rispettabile, magari richiedendo di essere assunto come dipendente, tecnico o ricercatore offrendo persino delle credenziali a supporto della sua identità. Ad ogni modo, semplicemente facendo domande, l'hacker potrebbe essere in grado di mettere assieme informazioni sufficienti per infiltrarsi nella rete di un'azienda. Se un hacker non fosse in grado di raccogliere abbastanza informazioni da una fonte, potrebbe contattare un'altra fonte all'interno della stessa azienda e utilizzare le informazioni della prima fonte aumentare la sua credibilità.

Cos'è un attacco di phishing?

Il Phishing è una forma di ingegneria sociale. Gli attacchi di Phishing utilizzano le mail o siti pericolosi per richiedere informazioni personali fingendosi un'organizzazione affidabile. Per esempio, un hacker potrebbe inviare una mail apparentemente proveniente da un istituto bancario o finanziario richiedendo informazioni relative al conto, spesso indicando la presenza di problemi. Quando gli utenti rispondono inviando i dati richiesti, gli hacker possono utilizzarli per ottenere l'accesso ai conti.

Gli attacchi di Phishing potrebbero provenire da altri tipi di organizzazioni, come gli enti di beneficienza. Gli hacker spesso traggono vantaggio dagli eventi attuali o da periodi particolari dell'anno, come per esempio:

- Disastri naturali (es. Uragano Katrina, Tsunami in Indonesia)
- Epidemie e Allarmi sanitari (es H1N1, COVID-19)
- Problemi economici (truffe IRS)
- Elezioni politiche di rilievo
- Feste

Cos'è un attacco *vishing*?

Il *vishing* è un approccio di ingegneria sociale che sfrutta la comunicazione vocale. Questa tecnica può essere associata ad altre forme di ingegneria sociale che invogliano una vittima a chiamare un determinato numero e divulgare informazioni sensibili. Attacchi vishing avanzati possono verificarsi attraverso la comunicazione vocale sfruttando le soluzioni e i servizi di trasmissione del *Voice over Internet Protocol* (VoIP). Il VoIP permette alla persona che chiama (ID) di falsificare la voce, traendo i vantaggi dalla fiducia mal risposta delle persone per quanto riguarda la sicurezza dei servizi telefonici, specialmente per i servizi di rete fissa. La comunicazione di rete fissa non può essere intercettata senza un accesso fisico alla linea. Tuttavia, questo non è vantaggioso quando si comunica direttamente con un soggetto pericoloso.

Cos'è lo *smishing*?

Lo *smishing* è una forma di ingegneria sociale che sfrutta gli SMS, o testi e messaggi. I messaggi di testo possono contenere link di pagine web, indirizzi e-mail o numeri telefonici che, se cliccati, potrebbero aprire automaticamente una finestra di browser o un messaggio di posta elettronica o un numero digitato. Questa funzionalità integrate di e-mail, voce, messaggi di testo e browser aumentano la possibilità per gli utenti di cadere vittime di attività di ingegneria dannosa.

Quali sono gli indicatori comuni di un tentativo di phishing?

Indirizzo del mittente sospetto: l'indirizzo del mittente potrebbe imitare un'attività legale. Gli hacker informatici spesso usano un indirizzo mail che assomiglia molto a quello di un'azienda seria, alterando o omettendo qualche carattere.

Saluti e firma generici: sia un saluto generico, come "Caro cliente" o "Signore/Signora", e la mancanza di informazioni di contatto nel blocco della firma sono forti indicatori di un'e-mail di phishing. Un'azienda affidabile normalmente si rivolge al cliente per nome e fornisce le proprie informazioni di contatto

Hyperlink e siti web fasulli: se si passa il cursore su qualsiasi link nel corpo dell'e-mail, e i link non corrispondono al testo che appare quando ci passi sopra, il link potrebbe essere falsificato. I siti web pericolosi possono sembrare identici a un sito legittimo, ma l'URL potrebbe avere una variazione nell'ortografia o un dominio diverso (ad esempio, .com invece di .net). Inoltre, i criminali informatici potrebbero utilizzare un servizio di abbreviazione di URL per nascondere la vera destinazione del link.

Ortografia e layout: una scarsa grammatica e struttura delle frasi, errori di ortografia e formattazione incoerente sono altri indicatori di un possibile tentativo di phishing. Le istituzioni rispettabili hanno personale dedicato che produce, verifica, e corregge i messaggi dei clienti.

Allegati sospetti: un'e-mail inaspettata che richiede all'utente di scaricare e aprire un allegato è un comune meccanismo di consegna di un malware. Un hacker può usare un falso senso di urgenza o di importanza per convincere un utente a scaricare o aprire un allegato senza prima esaminarlo.

Come evitare di essere vittima di un attacco?

Diffida di telefonate non richieste, visite o messaggi di posta elettronica da parte di individui che chiedono informazioni sui dipendenti o altri dati interni. Se un individuo sconosciuto afferma di essere parte di un'organizzazione legittima, cerca di verificare la sua la sua identità direttamente tramite l'azienda.

Non fornire informazioni personali o informazioni sulla tua azienda, compresa la sua struttura o le sue reti, a meno che tu non sia certo dell'autorità della persona che richiede le informazioni.

Non rivelare informazioni personali o finanziarie nelle e-mail e non rispondere alle richieste mail relative a queste informazioni. Questo include anche il seguire i link inviati via e-mail.

Non inviare informazioni sensibili su Internet senza aver verificato la sicurezza di un sito web. (Vedi: Proteggere la tua Privacy per maggiori informazioni).

Fai attenzione all'*Uniform Resource Locator* (URL) di un sito web. Controlla che gli URL che inizino con "https", una prova del fatto che i siti sono sicuri, piuttosto che "http".

Cerca l'icona di un lucchetto chiuso, in modo che le tue informazioni saranno criptate.

Cosa fare se pensi di essere vittima di un attacco informatico?

Se non sei sicuro che una richiesta via e-mail sia legittima o meno, prova a verificarla contattando direttamente l'azienda. Non usare le informazioni di contatto fornite su un sito web collegato alla richiesta; invece, controlla le indicazioni già esistenti per trovare le informazioni di contatto.

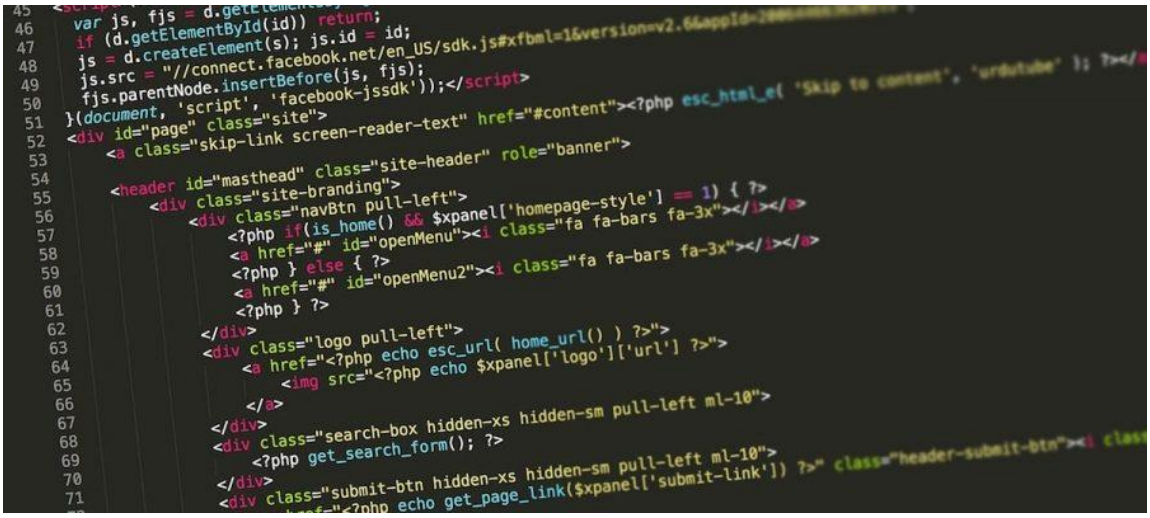
Installa e mantieni un software antivirus, un firewall e filtri di posta elettronica per ridurre parte di questo traffico.

Approfitta di qualsiasi funzione anti-phishing offerta dal tuo client di posta elettronica e browser web.

Utilizza l'autenticazione a più fattori (MFA).

4.1.5 Cos'è il codice maligno?

Il codice maligno è un gruppo di file o programmi indesiderati che possono danneggiare un computer o compromettere i dati archiviati sullo stesso. Esistono diverse tipologie di codici dannosi, tra cui: Virus, Worms e Trojan.



Virus: hanno l'abilità di danneggiare o distruggere i file di un sistema informatico e si diffondono tramite la condivisione di un supporto rimovibile già infetto, l'apertura di allegati mail dannosi, la visita di pagine web dannose.

Worm: sono un tipo di virus che si propaga autonomamente da un computer all'altro. La loro funzionalità è quella di utilizzare tutte le risorse del tuo computer, portando il computer stesso a non rispondere più ai comandi.

Trojan: sono programmi del computer che nascondono un virus o un programma potenzialmente dannoso. Non è inusuale che i software gratuiti contengano Trojan facendo credere agli utenti di star utilizzando dei software validi, invece, il programma sta eseguendo azioni dannose sul tuo computer.

Gli archivi di file dannosi: sono file non-eseguibili (es. documenti Microsoft Word, PDF Adobe, file ZIP o file immagini) che sfruttano i punti deboli dei programmi software usati per aprirli. Gli hacker molto spesso utilizzano archivi di dati danneggiati per installare malware sul sistema della vittima, solitamente distribuendo i file via mail, social media e siti web.

Come scoprire se si è vittima di un codice maligno?

Utilizzare software antivirus è il modo migliore per difendere il tuo computer dagli attacchi di un codice maligno. Se pensi che il tuo computer sia infetto, avvia una scansione con il tuo programma antivirus. Teoricamente, il tuo antivirus dovrebbe rilevare qualsiasi codice dannoso sul tuo computer, mettendoli in quarantena in modo da non poter più infettare il tuo sistema. Dovresti considerare inoltre queste ulteriori misure di sicurezza:

- Minimizzare il danno: se sei al lavoro e puoi contattare un esperto dell'*Information Technology* (IT), contattalo immediatamente. Prima inizieranno ad indagare e "pulire" il tuo computer, minori saranno le probabilità che il codice causi ulteriore danno al tuo computer e ad altri computer della rete. Se invece stai utilizzando un computer domestico o un laptop, scollega il tuo computer dalla rete. Quest'azione non permette all'hacker di accedere al tuo sistema.
- Rimuovi il codice maligno. Se hai un antivirus installato sul tuo computer, aggiorna il software e avvia una scansione manuale dell'intero sistema. Se non hai un software antivirus, puoi acquistarlo online o in un negozio di computer. Se il software non riuscisse ad individuare ed eliminare il virus, potresti aver bisogno di reinstallare il tuo sistema operativo, solitamente con un disco di ripristino del sistema. Considera che la reinstallazione o il ripristino del sistema operativo di norma cancella tutti i file e qualsiasi software aggiuntivo che installato sul computer. Dopo avere reinstallato il sistema operativo e ogni altro software, installa tutte le opportune patch per eliminare le vulnerabilità conosciute.

Le minacce continueranno ad evolvere. Anche se non potrai mai eliminare ogni elemento pericoloso, utilizzando delle precauzioni, installando ed utilizzando l'antivirus e seguendo altre semplici pratiche legate alla sicurezza, potrai ridurre significativamente i rischi e migliorare la tua protezione per quanto riguarda il malware.

Cosa sono i siti di *social networking*?

I siti di *Social networking*, definiti anche siti *friend-of-a-friend*, sono costruiti attorno al concetto dei tradizionali social network in cui sei connesso a nuove persone tramite persone che già conosci. Lo scopo di alcuni di questi siti potrebbe essere meramente sociale, permettendo all'utente di creare amicizie o relazioni amorose, mentre altri potrebbero essere incentrati sulla creazione di rapporti di lavoro.

Nonostante le caratteristiche dei siti di *social networking* differiscano, questi ti permettono di fornire informazioni su di te e offrire alcuni tipi di comunicazione (forum, *chat rooms*, servizi di messaggistica

istantanea), dandoti la possibilità di connetterti con altri utenti. Su alcuni siti puoi cercare persone tramite una ricerca basata su determinati criteri, mentre su altri è richiesto che tu sia "presentato" a nuove persone attraverso una connessione che condividete. Molti siti hanno delle community o dei sottogruppi che potrebbero essere creati in base a particolari interessi.

Quali implicazioni per la sicurezza hanno questi siti?

I siti di *social networking* si basano sulle connessioni e sulla comunicazione, per questo ti esortano a fornire un certo numero di informazioni personali. Mentre decidono la quantità di informazioni da rivelare, le persone potrebbero non utilizzare le stesse precauzioni usate quando incontrano qualcuno di persona perché:

- Internet dà un senso di anonimità
- La mancanza di interazioni fisiche comporta un falso senso di sicurezza
- Personalizzano le informazioni per farle leggere ai loro amici, dimenticandosi che potrebbero essere viste da altre persone
- Vogliono offrire spunti di riflessione per impressionare potenziali amici e colleghi

Mentre la maggior parte delle persone che utilizzano questi siti non costituisce una minaccia, i malintenzionati potrebbero essere attratti da loro, per l'accessibilità e la quantità di informazioni disponibili. Maggiore è la quantità di informazioni che i malintenzionati hanno su di te, più facile sarà approfittarsi di te. Gli adescatori potrebbero stringere rapporti online e, successivamente, convincere degli ignari individui ad incontrarli di persona. Tutto questo potrebbe portare a situazioni pericolose. Le informazioni personali possono essere usate anche per condurre un attacco di ingegneria sociale. Utilizzando le informazioni da te fornite riguardo la posizione, gli hobby, gli interessi e gli amici, un malintenzionato potrebbe fingersi un amico fidato o convincerti di avere l'autorità per accedere ad altri dati finanziari o personali.

Inoltre, a causa della popolarità di questi siti, gli hacker potrebbero usarli per diffondere malware. I siti che offrono applicazioni sviluppate da terze parti sono particolarmente vulnerabili. Gli hacker potrebbero essere in grado di creare delle applicazioni personalizzate che possano sembrare innocue mentre infettano il tuo computer o condividono le tue informazioni a tua insaputa.

4.1.6 Attività pratiche

Step 1: Pulizia del computer

1. Questo problema può essere riscontrato grazie al rumore prodotto dalla velocità delle ventole di raffreddamento, durante l'utilizzo del PC o del laptop.
2. Avrai sicuramente notato che, inizialmente, utilizzando il computer quando nuovo, le ventole di raffreddamento erano silenziose poiché non erano impolverate.
3. In seguito ad un lungo periodo di utilizzo, il computer/laptop diventa molto rumoroso a causa dell'alta velocità delle ventole impolverate, che non riescono più a garantire che arrivi l'aria necessaria per raffreddare le componenti elettroniche, arrivando al punto di bloccarsi comportando la distruzione delle componenti interne e dei microprocessori a causa dell'elevata temperatura di funzionamento.
4. L'aspetto negativo della polvere consiste nell'effetto termico creato dal deposito di polvere sui componenti (sopra e attorno al processore e al radiatore).
5. Pertanto, l'esistenza della polvere nel computer può causare la distruzione di componenti elettroniche. A causa della polvere, queste si surriscaldano portando alla loro stessa distruzione. Per questo motivo, i computer devono essere spolverati regolarmente.
6. Supponendo che tu abbia un computer a casa che utilizzi, poniti questa domanda: "Quand'è stata l'ultima volta che ho pulito il computer dalla polvere?"
7. La pulizia del computer può essere fatta in un negozio specializzato nella risoluzione dei problemi legati ai computer.
8. La pulizia della polvere sui laptop richiede operazioni più complesse, pertanto, è necessario che tu richieda un servizio specializzato.
9. Per capire che cosa significhi pulire un computer impolverato, puoi ricercare su Internet, aprendo un motore di ricerca e digitando "Come pulire la polvere dai computer?". Una pagina web che consigliamo è la seguente: https://www.wikihow.com/Clean-a-Dusty-Computer
10. Tuttavia, considerando il fatto che questo corso è rivolto ai principianti, con meno conoscenze in questo campo, all'inizio, si consiglia di utilizzare un servizio specializzato per pulire il computer.

Step 2: Per un computer è necessario installare un programma di protezione antivirus / firewall

1. Per capire cosa sia un software antivirus, ti consigliamo di accedere al sito web: https://us.norton.com/Internetsecurity-malware-what-is-antivirus.html
2. Naturalmente, ci sono molti software antivirus sul mercato. Una ricerca su Internet, ad esempio, con le parole chiave "confronta software antivirus" può trovare innumerevoli pagine per cercare informazioni sui software esistenti, come ad esempio: https://www.PCmag.com/picks/the-best-antivirus-protection dove nella sezione "OUR 13 TOP PICKS" sono elencati diversi software antivirus.
3. Nel tuo computer, se non hai un altro antivirus installato, ti consigliamo di cercare in una pagina di ricerca le parole chiave "free trial antivirus" e accedere al link https://www.kaspersky.com/downloads/thank-you/antivirus-free-trial e nella pagina aperta, cliccare sul pulsante "DOWNLOAD NOW".
4. Il computer che usiamo, per esempio, ha il sistema operativo WINDOWS 10 e "Google Chrome" come browser Internet.
5. Visto che sull'altro computer che usiamo è stato installato Kaspersky vi raccomandiamo di usare questo, al fine di non generare conflitti con altri tipi di software antivirus.
6. Nella parte inferiore della finestra del browser Chrome, dopo aver premuto il pulsante "DOWNLOAD NOW", viene visualizzato l'archivio eseguibile "kav21.3.10.391en_26075.exe" (naturalmente il nome dell'archivio può variare a seconda della versione scaricata)
7. Dopo il download da Internet e l'installazione, hai installato una soluzione di sicurezza antivirus nel tuo computer! Congratulazioni!
8. L'antivirus funziona sempre ed è attivo in background del sistema operativo
9. In basso a destra dello schermo, accanto all'orologio, appare un'icona con una "K". È possibile che questa icona sia nascosta dal sistema operativo, per questo motivo sarà necessario cliccare prima sul pulsante "^", accanto all'orologio.
10. Se clicchi sull'icona "K", viene aperta l'interfaccia delle impostazioni dell'antivirus Kaspersky.
11. Nell'interfaccia aperta clicca sull'area del pulsante "ATTIVITÀ" e nella finestra aperta nell'area "SCANSIONE COMPLETA" clicca su AVVIA. Notiamo che il software antivirus inizia la scansione del computer alla ricerca di virus, se presenti.
12. Una volta completata la scansione, questa può essere riavviata quando vuoi. L'antivirus può essere impostato per avviare automaticamente il processo di scansione del computer.
13. Sempre in questa finestra aperta quando si clicca su ATTIVITÀ, scorrendo in basso, si raggiunge l'area AGGIORNA. Premendo il pulsante AVVIA in quest'area, l'applicazione antivirus verrà aggiornata all'ultima versione e all'ultimo database fornito dal produttore. Si raccomanda di fare questo aggiornamento periodicamente.
14. Va notato che le soluzioni di sicurezza, possono servire sia per proteggere il computer privato dai virus che per proteggere il computer da accessi non autorizzati, quando è in una rete informatica.
15. Per questa situazione, sul sito web per Kaspersky https://www.kaspersky.com/home-security sono presentati 3 varianti del software di protezione, accanto a ciascuno è specificato per che cosa può garantire la protezione.
16. Per esempio, la soluzione di protezione "Kaspersky Internet Security" è una soluzione integrata che fornisce sia la protezione antivirus che la protezione di reti informatiche (firewall).
17. In generale, tutti i software di protezione antivirus offrono opzioni integrate sia per la protezione antivirus che per la protezione di reti informatiche.

18. Allo stesso modo, altri programmi antivirus possono essere installati accedendo alla pagina dedicata del produttore per scaricare e acquistare le relative licenze.
19. La presentazione non è strettamente limitata all'antivirus Kaspersky! Durante la scelta e secondo le esigenze di ognuno di voi, possono essere installati altri software antivirus sia sul computer che su sistemi elettronici portatili.

4.2 Proteggere i dati personali e la privacy

Unità 4.2	Proteggere i dati personali e la privacy
Durata	9h
Obiettivi	Essere consapevoli dei problemi relativi alla condivisione dei dati personali Essere in grado di configurare le impostazioni di sicurezza per preservare la privacy
Contenuti	4.2.1 Proteggere te stesso online 4.2.2 Linee guida per condividere le informazioni personali 4.2.3 Attività pratiche
Risorse	Manuale di formazione, computer con accesso alla rete
Metodo di formazione	Presentazione da parte dell'educatore Discussione/dibattito di gruppo

Tabella 23: Struttura dell'unità di competenza 4.2. – Proteggere i dati personali e la privacy del Modulo 4 (Sicurezza).

4.2.1 Proteggere te stesso online

Come puoi proteggere te stesso?

Limita la quantità di informazioni personali che pubblichi: non pubblicare informazioni sensibili, come il tuo indirizzo o informazioni relative ai tuoi impegni o la tua routine. Se i tuoi contatti pubblicano informazioni su di te, assicurati che le informazioni combinate ti facciano sentire a tuo agio con agli estranei. Fai attenzione anche quando pubblichi informazioni, comprese le foto, sui tuoi contatti.

Ricorda che Internet è una risorsa pubblica: pubblica solo le informazioni che ti va bene che qualcuno veda. Questo include informazioni e foto nel tuo profilo e nei blog e altri forum. Inoltre, una volta che hai pubblicato informazioni online, non puoi ritrattare. Anche se rimuovi le informazioni da un sito, le versioni salvate o nella cache, possono ancora esistere sui computer di altre persone.

Diffida degli sconosciuti: Internet rende facile per le persone travisare le loro identità e motivazioni. Considera l'idea di limitare le persone che possono contattarti su questi siti. Se interagisci con persone che non conosci, sii cauto sulla quantità di informazioni che riveli o sull'accettare di incontrarli di persona.

Sii scettico: non credere a tutto ciò che leggi online. Le persone possono pubblicare informazioni false o fuorvianti su vari argomenti, compresa la loro stessa identità. Questo non è necessariamente fatto con intenti malevoli; potrebbe essere involontario, un'esagerazione o uno scherzo. Prendi le dovute precauzioni, però, e cerca di verificare l'autenticità di qualsiasi informazione prima di intraprendere qualsiasi azione.

Valuta le tue impostazioni: sfrutta le impostazioni di privacy di un sito. Le impostazioni di default di alcuni siti possono permettere a chiunque di vedere il tuo profilo, ma puoi personalizzare le impostazioni per limitare l'accesso solo a certe persone. C'è ancora il rischio che informazioni private possano essere esposte nonostante queste restrizioni, quindi, non pubblicare nulla che non vorresti che il pubblico vedesse. I siti possono cambiare le loro opzioni periodicamente, quindi controlla regolarmente le tue impostazioni di sicurezza e privacy per assicurarti che le tue scelte siano ancora appropriate.

Diffida delle applicazioni di terze parti: le applicazioni di terze parti possono fornire intrattenimento o funzionalità, ma sii cauto nella decisione delle applicazioni da abilitare. Evita le applicazioni che sembrano sospette e modifica le tue impostazioni per limitare la quantità di informazioni a cui le applicazioni possono avere accesso.

Usa password sicure: proteggi il tuo account con password difficili da indovinare. Se la tua password viene compromessa, qualcun altro potrebbe essere in grado di accedere al tuo account e fingere di essere te.

Controlla le politiche sulla privacy: alcuni siti possono condividere con altre aziende informazioni come indirizzi e-mail o preferenze degli utenti. Questo può portare ad un aumento dello spam. Inoltre, cerca di individuare la politica di gestione di segnalazioni per assicurarti di non iscrivere involontariamente i tuoi amici a messaggi di spam. Alcuni siti continueranno ad inviare messaggi e-mail a chiunque tu faccia riferimento fino a quando non si iscrivono.

Mantieni il software aggiornato, specialmente il browser: installa gli aggiornamenti del software in modo che gli hacker non possano approfittare di problemi o vulnerabilità note. (Vedi: Capire le patch.) Molti sistemi operativi offrono aggiornamenti automatici. Se questa opzione fosse disponibile, dovresti abilitarla.

Usa e mantieni il software antivirus: il software antivirus aiuta a proteggere il tuo computer contro i virus conosciuti, quindi, potresti essere in grado di rilevare e rimuovere il virus prima che possa fare danni. (Vedi: Capire il software antivirus.) Poiché gli hacker creano continuamente nuovi virus, è importante mantenere le versioni aggiornate.

I bambini sono particolarmente suscettibili alle minacce che i siti di social network presentano: anche se molti di siti hanno restrizioni di età, i bambini possono falsificare la loro età per potersi iscrivere. Insegnando ai bambini la sicurezza su Internet, essendo consapevoli delle loro abitudini online e guidandoli verso siti appropriati, i genitori possono fare in modo che i bambini diventino utenti sicuri e responsabili.

Perché è importante ricordare che Internet è pubblico?

Internet è una risorsa accessibile e popolare per comunicare con gli altri ed effettuare ricerche. Si può avere un senso di anonimato mentre si è online, ma si dovrebbe ricordare che non si è anonimi, e la facilità con cui le persone possono avere informazioni che ti riguardano è la stessa con la quale puoi trovare informazioni su di loro.

Molte persone sono diventate così abituate e a proprio agio con Internet che adottano pratiche che le rendono vulnerabili. Per esempio, anche se le persone sono tipicamente diffidenti nel condividere informazioni personali con estranei che incontrano per strada, potrebbero non esitare a pubblicare quelle stesse informazioni online. Una volta online, sono accessibili a un mondo di estranei, e non si ha idea di cosa potrebbero fare con quelle informazioni.

4.2.2 Linee guida per condividere le informazioni personali

Quali linee seguire quando si pubblicano informazioni su Internet?

Considera Internet come un romanzo, non come un diario: assicurati di essere a tuo agio con chiunque veda le informazioni che metti su blog, siti di *social networking* e siti web personali: scrivi sapendo che i contenuti saranno disponibili ad uso pubblico e che persone che non hai mai incontrato troveranno la tua pagina. Anche se alcuni siti usano password o altre restrizioni relative alla sicurezza al fine di proteggere le informazioni, questi metodi non sono usati per la maggior parte dei siti web. Se vuoi che le informazioni siano private o limitate a un piccolo gruppo di persone, Internet non è il posto migliore.

Limita la quantità di informazioni personali che pubblichi: non pubblicare informazioni vulnerabili, come il tuo indirizzo, il numero di telefono, l'e-mail, relative al tuo programma o alla tua routine. Fornire il tuo indirizzo e-mail può aumentare la quantità di spam che ricevi (per saperne di più, vedi: Ridurre lo spam per maggiori informazioni). Fornire dettagli sui tuoi hobby, il tuo lavoro, la tua famiglia e i tuoi amici, o il tuo passato può dare agli hacker informazioni sufficienti per un attacco di ingegneria sociale di successo (per saperne di più, vedi: Evitare l'ingegneria sociale e gli attacchi di phishing e Stare al sicuro sui siti di social network).

Capisci che non potrai tornare indietro: una volta che pubblichi qualcosa online, questa è disponibile per altre persone e motori di ricerca. Puoi cambiare o rimuovere informazioni dopo che qualcosa è stato pubblicato, ma è possibile che qualcuno abbia già visto la versione originale. Anche se si cerca di rimuovere la pagina (o le pagine) da Internet, qualcuno potrebbe aver salvato una copia della pagina o averne usato degli estratti in un'altra fonte. Alcuni motori di ricerca "memorizzano" copie di pagine web. Queste copie memorizzate possono essere disponibili dopo che una pagina web è stata cancellata o alterata. Alcuni browser web possono anche mantenere una cache delle pagine che un utente ha visitato, quindi, la versione originale può essere memorizzata in un file temporaneo sul computer dell'utente. Pensa a queste implicazioni prima di pubblicare informazioni: una volta che qualcosa è là fuori, non puoi garantire di poterlo rimuovere completamente.

Come pratica generale, lascia che il buon senso guidi le tue decisioni relativa a cosa pubblicare online. Prima di pubblicare qualcosa su Internet, determinane il valore e considera le implicazioni di avere informazioni disponibili al pubblico. Il furto d'identità è un problema crescente: più informazioni personali un aggressore riesce raccogliere, più facile sarà per lui fingere di essere te.

Quanto sei anonimo?

Puoi pensare di navigare sui siti web nell'anonimato, ma parti di informazioni personali vengono sempre lasciate. Puoi ridurre la quantità di informazioni rivelate su di te visitando siti legittimi, controllando le politiche sulla privacy e riducendo al minimo la quantità di informazioni personali che fornisci.

Quali informazioni vengono raccolte?

Quando si visita un sito web, una certa quantità di informazioni viene automaticamente inviata al sito. Queste informazioni possono includere:

- Indirizzo IP: ad ogni computer, su Internet, viene assegnato un indirizzo IP (protocollo Internet) specifico e unico. Il tuo computer può avere un indirizzo IP statico o dinamico. Se hai un indirizzo IP statico, questo non cambierà. Tuttavia, alcuni ISP possiedono un blocco di indirizzi e ne assegnano uno aperto ogni volta che ti connetti a Internet: questo è un indirizzo IP dinamico. Puoi determinare l'indirizzo IP del tuo computer in qualsiasi momento visitando www.showmyip.com.
- Nome di dominio: Internet è diviso in domini, e l'account di ogni utente è associato a uno di questi domini. Puoi identificare il dominio guardando la fine dell'URL. Ad esempio, .edu indica un'istituzione educativa, .gov indica un'agenzia governativa statunitense, .org si riferisce a un'organizzazione, e .com è

ad uso commerciale. Molti Paesi hanno anche nomi di dominio specifici. La lista dei nomi di dominio attivi è disponibile presso l'*Internet Assigned Numbers Authority (*IANA).

- Dettagli sul software: un'organizzazione potrebbe determinare il browser, versione inclusa, utilizzato per accedere al suo sito. L'organizzazione potrebbe anche determinare il sistema operativo che il tuo computer sta utilizzando.
- Visite alle pagine: le informazioni relative alle pagine che hai visitato, il tempo trascorso su una data pagina e il percorso del motore di ricerca sono spesso disponibili per l'ente che gestisce il sito web.
- Se un sito web utilizza i cookie, l'azienda può essere in grado di raccogliere ancora più informazioni, come i tuoi *pattern* di navigazione, che includono altri siti che hai visitato. Se il sito che stai visitando è dannoso, i file sul tuo computer, così come le password memorizzate nella memoria temporanea, possono essere a rischio.

Come vengono usate queste informazioni?

Generalmente, le aziende usano le informazioni raccolte automaticamente per scopi legittimi, come la generazione di statistiche sui loro siti. Analizzando le statistiche, le aziende possono capire meglio la popolarità del sito e i contenuti più graditi. Possono utilizzare queste informazioni per modificare il sito per supportare meglio il flusso delle persone che lo visitano.

Un altro modo per sfruttare le informazioni raccolte sugli utenti è il marketing. Se il sito utilizza i cookie per capire quali altri siti o pagine hai visitato, può utilizzare queste informazioni per pubblicizzare determinati prodotti. I prodotti possono essere sul sito stesso oppure essere offerti da siti partner.

Tuttavia, alcuni siti possono raccogliere le tue informazioni a scopi dannosi. Se gli hacker riescono ad accedere a file, password o informazioni personali sul tuo computer, potrebbero utilizzare questi dati a loro vantaggio. Gli aggressori potrebbero rubare la tua identità, usando e abusando delle tue informazioni personali per un guadagno finanziario. Una pratica comune è che gli hacker usino questo tipo di informazioni una o due volte, per poi venderle o scambiarle con altre persone. Gli hacker traggono profitto dalla vendita o dal commercio delle informazioni, e aumentando il numero di transazioni è più difficile risalire a loro. Gli hacker possono anche alterare le impostazioni di sicurezza del tuo computer in modo da poter accedere e utilizzare il tuo computer per altre attività dannose.

Stai rivelando altre informazioni personali?

Mentre l'uso dei cookie può essere un metodo per raccogliere informazioni, il modo più semplice per gli hacker di ottenere l'accesso alle informazioni personali è quello di chiederle. Camuffano un sito dannoso come legittimo, gli hacker possono essere in grado di convincerti a fornire il tuo indirizzo, i dati della carta di credito, il numero di previdenza sociale o altri dati personali.

4.2.3 Attività pratiche

Step 1: blocca il computer con una password

1. Le apparecchiature di oggi offrono molteplici modi per proteggersi! Per esempio, in WINDOWS 10 nella sezione IMPOSTAZIONI -> Opzioni di accesso hai la possibilità di inserire una password al tuo computer attraverso una delle opzioni: riconoscimento facciale, impronta digitale, PIN, chiave di sicurezza, password o riconoscimento dell'immagine.
2. Non è il tema principale, ma occorre dire che ogni computer offre la possibilità di impostare una password (questo può essere fatto dalla sezione IMPOSTAZIONI del tuo dispositivo)
3. Oggi ci concentreremo sulla creazione di una password. La password è una sequenza di caratteri scritti in un dato ordine, che può contenere: maiuscole, minuscole, numeri, caratteri speciali
4. Per esempio, se in WINDOWS impostiamo la password *@calculatorMeuDeNota10* in IMPOSTAZIONI > Opzioni di accesso, quando si accede al computer, al riavvio o dopo lo standby, verrà richiesta la password. Quale password? *@calculatorulMeuDeNota10*, le lettere scritte esattamente nello stesso ordine e lo stesso tipo di lettera. ATTENZIONE: il computer non riconoscerà la password *@CALCULATORULMEUDENOTA10* o *@calculatorulmeudenota10* o *@ calculatorulMeu De Nota 10*. La password riconosciuta dal sistema sarà esattamente come quella creata, *@calculatorulMeuDeNota10*.
5. Attenzione: non dimenticare la password! Sarebbe meglio scriverla da qualche parte dove puoi trovarla. Se hai dimenticato la tua password, ci sono diversi modi per recuperarla, ma questo richiede conoscenze molto più avanzate e spesso porta problemi durante il recupero.
6. Una password deve contenere caratteri speciali (@), lettere minuscole (computer eu e ota), lettere maiuscole (M D N), numeri (10).
7. Più caratteri contiene una password, più forte sarà e più difficile risulterà trovarla.
8. Per capire cos'è una password forte, ti consigliamo di accedere al seguente sito: https://ro.safetydetectives.com/password-meter/
9. Nella parte superiore destra, è possibile impostare la lingua in cui verranno visualizzate le informazioni dal sito
10. Nel campo sotto il titolo "Quanto è sicura la mia password?" è possibile digitare e provare i modelli di password.
11. Più alto è il numero di caratteri che la password contiene e più caratteri sono elencati sopra, più alto sarà il punteggio ottenuto sul lato destro del campo, e il tipo di password passerà da MOLTO DEBOLE a MOLTO FORTE
12. Cerca di trovare una password che ottenga un voto di 100! Ci riesci? La password di questo esercizio che punteggio pensi che otterrà?
13. Infine, ti raccomandiamo di leggere la sezione delle domande frequenti in fondo alla pagina https://ro.safetydetectives.com/password-meter/
14. In questo modo otterrai più informazioni su come creare password forti e sicure.

Step 2: Utilizzo di un browser e aggiornamenti periodici

1. Apri una pagina web, digita l'indirizzo Internet www.google.com e scrivi le seguenti parole "chrome download" nel campo di ricerca
2. Sul computer, cerca e scarica il browser Internet Chrome (se non è già installato) su https://www.google.com/chrome/
3. Dalla pagina aperta premere il pulsante DOWNLOAD CHROME
4. Accedi al file scaricato e segui i passaggi relativi all'installazione
5. Aprire una o più pagine web nel browser Chrome (dipende da te, in base alle pagine a cui vuoi accedere)
6. Nota, nella barra di navigazione, se c'è o meno un lucchetto davanti all'indirizzo Internet raggiunto
7. Quel lucchetto rappresenta un certificato di sicurezza per la pagina a cui si accede e in sua assenza la navigazione sulla pagina non è sicura. Una navigazione sicura può essere fatta su quelle pagine Internet che presentano il lucchetto.
8. In una pagina web sicura (dove c'è il lucchetto), clicca sul lucchetto e osserva, tramite informazioni fornite, se il certificato è valido
9. Clicca su Certificato (Valido) e osserva la data fino alla quale il certificato è valido
10. L'icona "lucchetto" è una conferma che la connessione Internet tra la persona che accede a quel sito e il server di quel sito sia sicura, è una comunicazione criptata (altri utenti non possono accedere o intercettare la connessione stabilita con il sito web)
11. Chiudi la finestra delle informazioni sul certificato e clicca sui 3 punti verticali in alto a destra (situati sotto la X, chiudi finestra) per accedere alle impostazioni di Chrome
12. Clicca su "Aiuto" e nel nuovo menu clicca su "Informazioni su Google Chrome".
13. A questo punto Google Chrome cercherà di aggiornarsi all'ultima versione disponibile del software con il seguente messaggio:
    "Aggiornamento di Google Chrome (50%)
    Versione 90.0.4430.212 (Build ufficiale) (64-bit)"
14. Dopo l'aggiornamento, Chrome potrebbe chiederti di riavviare il browser con un messaggio
    "Quasi aggiornato! Rilancia Google Chrome per finire l'aggiornamento. Le finestre in incognito non si riapriranno.
    Versione 90.0.4430.212 (*Build* ufficiale) (64-bit)"
15. Premere il pulsante "Riavvia".
16. Se non è necessario riaprire il browser o il browser è già aggiornato, apparirà un messaggio:
    "Google Chrome è aggiornato
    Versione 91.0.4472.77 (*Build* ufficiale) (64-bit)"
17. In questo modo il browser Chrome può essere aggiornato
18. Si prega di notare che qualsiasi software e non solo il browser Chrome, offre la possibilità di aggiornare a versioni più recenti, ma non tutti i software offrono questa funzione gratuitamente
19. L'aggiornamento a versioni più recenti offre la sicurezza e la stabilità del software in uso.

4.3 Proteggere la salute e il benessere

Unità 4.3	Proteggere la salute e il benessere
Durata	5h
Obiettivi	Essere in grado di evitare rischi per la salute e minacce al benessere fisico e psicologico mentre si usano le tecnologie digitali; Essere in grado di proteggere sé stessi e gli altri da possibili pericoli negli ambienti digitali; Essere in grado di controllare gli aspetti che distraggono dal lavoro e dalla vita digitale; Essere in grado di prendere misure preventive per proteggere la salute della persona per cui è responsabile
Contenuti	4.3.1 Gli effetti negativi della tecnologia: le cose da sapere 4.3.2 Hai mai sentito parlare di cyberbullismo? 4.3.3 Attività pratiche
Risorse	Manuale di formazione, computer con accesso a Internet
Metodo di formazione	Presentazione da parte dell'educatore

Tabella 24: Struttura dell'unità di competenza 4.3. – Proteggere la salute e il benessere del Modulo 4 (Sicurezza).

4.3.1 Gli effetti negativi della tecnologia: le cose da sapere

Le persone sono più connesse che mai, grazie ai rapidi progressi della tecnologia.

Mentre alcune forme di tecnologia possono aver apportato cambiamenti positivi nel mondo, ci sono anche prove degli effetti negativi della tecnologia e del suo uso eccessivo.

I social media e i dispositivi mobili possono portare a problemi psicologici e fisici, come l'affaticamento degli occhi e la difficoltà a concentrarsi su compiti importanti. Possono anche contribuire a condizioni di salute più gravi, come la depressione.

Effetti psicologici

L'uso eccessivo o la dipendenza dalla tecnologia possono avere effetti psicologici avversi, tra cui l'isolamento. Le tecnologie, come i social media, sono progettate per unire le persone, ma in alcuni casi possono avere l'effetto opposto.

Uno studio del 2017 su giovani adulti di età compresa tra i 19 e i 32 anni ha scoperto che le persone con un uso maggiore dei social media avevano una probabilità tre volte maggiore di sentirsi socialmente isolate rispetto a coloro che non usavano i social media così spesso.

Trovare modi per ridurre l'uso dei social media, come impostare limiti di tempo per le app social, può aiutare a ridurre la sensazione di isolamento in alcune persone.

Depressione e ansia

Gli autori di un esame sistemico della *Trusted Source* del 2016 hanno discusso il legame tra le reti sociali e i problemi di salute mentale, come la depressione e l'ansia.

La ricerca ha trovato risultati contrastanti. Le persone che avevano più interazioni positive e supporto sociale su queste piattaforme sembravano avere livelli più bassi di depressione e ansia.

Tuttavia, era vero anche il contrario. Le persone che percepivano di avere più interazioni sociali negative online e che erano più inclini al confronto sociale hanno sperimentato livelli più elevati di depressione e ansia.

Quindi, mentre sembra esserci un legame tra i social media e la salute mentale, un fattore determinante significativo è il tipo di interazioni che le persone sentono di avere su queste piattaforme.

Effetti fisici sulla salute

L'uso della tecnologia può aumentare anche il rischio di problemi fisici, tra cui:

Affaticamento oculare

Le tecnologie come tablet, smartphone e computer, possono far mantenere l'attenzione di una persona per lunghi periodi di tempo. Questo può portare all'affaticamento degli occhi.

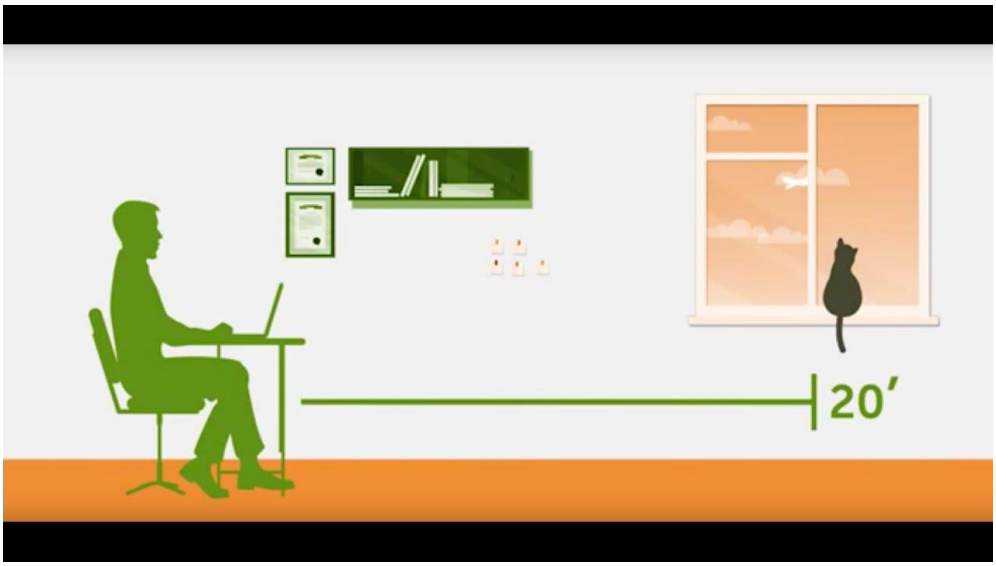
I sintomi dell'affaticamento oculare digitale possono includere visione offuscata e occhi secchi. L'affaticamento degli occhi può anche portare a dolori in altre aree del corpo, come la testa, il collo o le spalle.

Diversi fattori tecnologici possono portare all'affaticamento oculare, come:

- tempo passato davanti dello schermo
- riflesso dello schermo
- luminosità dello schermo
- visione troppo vicina o troppo lontana
- postura scorretta
- problemi visivi latenti

Fare delle pause regolari lontano dallo schermo può ridurre la probabilità di affaticamento degli occhi.

Chiunque avverta regolarmente questi sintomi dovrebbe consultare un optometrista per un controllo.



La regola del 20-20-20 per la visione digitale

Quando si usa qualsiasi forma di schermo digitale per lunghi periodi di tempo, si raccomanda di usare la regola del 20-20-20. Per seguire la regola, ogni 20 minuti di schermo, fare una pausa di 20 secondi per guardare qualcosa ad almeno 20 metri di distanza. Fare questo può aiutare a ridurre la tensione degli occhi che devono fissare lo schermo per un periodo di tempo continuo.

Postura scorretta

Il modo in cui molte persone usano i dispositivi mobili e i computer può anche contribuire a una postura scorretta. Nel tempo, questo può portare a problemi muscoloscheletrici. Molte tecnologie promuovono una posizione dell'utente "giù e in avanti", il che significa che la persona è piegata in avanti e guarda in basso verso lo schermo. Questo può mettere una quantità non necessaria di pressione sul collo e sulla spina dorsale. Uno studio della durata di 5 anni pubblicato sulla rivista *Applied Ergonomics* ha trovato un'associazione tra l'invio di messaggi su un telefono cellulare e il dolore al collo o alla parte superiore della schiena nei giovani adulti. I risultati hanno indicato che gli effetti erano per lo più a breve termine, anche se alcune persone hanno continuato ad avere sintomi a lungo termine.

Tuttavia, alcuni studi contestano questi risultati.

Uno studio del 2018 di *Trusted Source* nell'*European Spine Journal* ha scoperto che la postura del collo mentre si messaggia non fa la differenza in sintomi come il dolore al collo.

Questo studio ha concluso che l'atto di inviare sms e il "*text neck*" non influenzano il dolore al collo nei giovani adulti. Tuttavia, lo studio non ha incluso un *follow-up* a lungo termine. È possibile che anche altri fattori influenzino il dolore al collo, come l'età e i livelli di attività. Correggere i problemi di postura mentre si usa la tecnologia può portare a un miglioramento generale della postura e della forza muscolare, nel collo e nella schiena.

Per esempio, se una persona si trova seduta nella stessa posizione per ore e ore, come quando si siede ad una scrivania mentre lavora, stare regolarmente in piedi o fare stretching può aiutare a ridurre la tensione sul corpo.

Inoltre, fare brevi pause, come camminare in ufficio ogni ora, può anche aiutare a mantenere i muscoli sciolti ed evitare tensioni e posture scorrette.

Problemi di insonnia

Usare la tecnologia prima di andare a letto può causare problemi di insonnia. Questo effetto ha a che fare con il fatto che la luce blu, come quella di cellulari, e-reader e computer, stimola il cervello. Gli autori di uno studio del 2014 hanno scoperto che questa luce blu è sufficiente a disturbare il naturale ritmo circadiano del corpo. Questo disturbo potrebbe rendere più difficile la fase di addormentato o portare una persona a sentirsi meno vigile il giorno dopo. Per evitare il potenziale impatto della luce blu sul cervello, le persone possono smettere di usare dispositivi elettronici che emettono luce blu due ore prima di andare a letto. Attività delicate per rilassarsi invece, come leggere un libro, fare un po' di stretching o fare un bagno, sono delle buone alternative.

Attività fisica ridotta

La maggior parte delle tecnologie digitali quotidiane sono sedentarie. Un uso più esteso di queste tecnologie promuove uno stile di vita più sedentario, noto per gli effetti negativi sulla salute, come:

- obesità
- malattie cardiovascolari
- diabete di tipo 2
- morte prematura

Trovare modi per prendersi delle pause dalle tecnologie sedentarie può aiutare a promuovere uno stile di vita più attivo.

Una ricerca del 2017 indica che le tecnologie attive, come le notifiche delle app, le e-mail e le tecnologie *wearable* che promuovono l'esercizio possono ridurre il comportamento sedentario a breve termine. Questo potrebbe aiutare le persone a impostare modelli salutari e diventare più attivi fisicamente.

4.3.2 Hai mai sentito parlare di cyberbullismo?

Il cyberbullismo consiste nell'usare la tecnologia per molestare o bullizzare qualcun altro. Una volta i bulli erano limitati all'uso di metodi come l'intimidazione fisica, la posta o il telefono, ma i computer, i telefoni cellulari, i tablet e altri dispositivi mobili offrono ai bulli spazi come e-mail, messaggistica istantanea, pagine web e foto digitali.

Le forme di cyberbullismo possono variare in gravità da voci crudeli o imbarazzanti a minacce, molestie o stalking. Può colpire qualsiasi gruppo di età, tuttavia, gli adolescenti e i giovani adulti sono vittime comuni, e il cyberbullismo è un problema crescente nelle scuole.

Perché il cyberbullismo è diventato un tale problema?

Il relativo anonimato di Internet è attraente per i bulli perché aumenta l'intimidazione e rende più difficile rintracciarne l'attività. Alcuni bulli trovano anche più facile essere più cattivi perché non c'è contatto personale. Internet e la posta elettronica possono anche aumentare la visibilità dell'attività. Informazioni o immagini pubblicate online o inoltrate in e-mail di massa possono raggiungere un pubblico più vasto e più velocemente dei metodi tradizionali, causando più danni alle vittime. Una grande quantità di informazioni personali è disponibile online, quindi i bulli possono essere in grado di scegliere arbitrariamente le loro vittime.

Il cyberbullismo può anche indicare una tendenza a comportamenti più gravi. Mentre il bullismo è sempre stato una spiacevole realtà, la maggior parte dei bulli ne esce crescendo. Il cyberbullismo non è esistito abbastanza a lungo per avere una ricerca solida, ma ci sono prove che dimostrano che il bullismo possa essere un avvertimento precoce per un comportamento violento in futuro.

Come puoi proteggere te stesso o i tuoi figli?

- Insegna ai tuoi figli le buone abitudini online. Spiega i rischi della tecnologia e insegna loro ad essere responsabili online. Riduci il rischio che diventino cyberbulli stabilendo delle linee guida e monitorando il loro uso di Internet e di altri mezzi elettronici (cellulari, tablet, ecc.).
- Mantieni aperte le linee di comunicazione. Parla regolarmente con i tuoi figli delle loro attività online, in modo che si sentano a loro agio nel dirti se sono vittime di cyberbullismo.
- Osserva i segnali di avvertimento. Se noti dei cambiamenti nel comportamento di tuo figlio, cerca di identificarne la causa il prima possibile. Se si tratta di cyberbullismo, agire tempestivamente può limitare i danni.
- Limitare la disponibilità di informazioni personali: limitare il numero di persone che hanno accesso alle informazioni di contatto o ai dettagli relativi a interessi, abitudini o occupazione riduce l'esposizione ai bulli che tu o tuo figlio non conoscete. Questo può limitare il rischio di diventare una vittima e può rendere più facile identificare il bullo se tu o tuo figlio siete vittime.
- Evitare il peggioramento della situazione. Rispondendo con ostilità rischi di provocare il bullo e di aggravare la situazione. A seconda delle circostanze, considera la possibilità di ignorare il problema. Spesso i vivono grazie alla reazione delle loro vittime. Altre opzioni includono piccole azioni. Per esempio, bloccare i messaggi sui social network o fermare le e-mail indesiderate cambiando l'indirizzo e-mail. Se continui a ricevere messaggi al nuovo indirizzo e-mail, il caso potrebbe essere più grave ed è possibile avviare un'azione legale.
- Documenta l'attività: tieni un registro di qualsiasi attività online (e-mail, pagine web, messaggi istantanei, ecc.), comprese le date e gli orari rilevanti. Oltre ad archiviare una versione elettronica, considera la possibilità di stamparne una copia.

- Segnalare il cyberbullismo alle autorità competenti: se tu o tuo figlio siete stati molestati o minacciati, segnala l'attività. Molte scuole hanno istituito programmi antibullismo, quindi i dirigenti scolastici potrebbero avere stabilito delle politiche per affrontare l'attività che coinvolge gli studenti. Se necessario, contatta le forze dell'ordine locali.

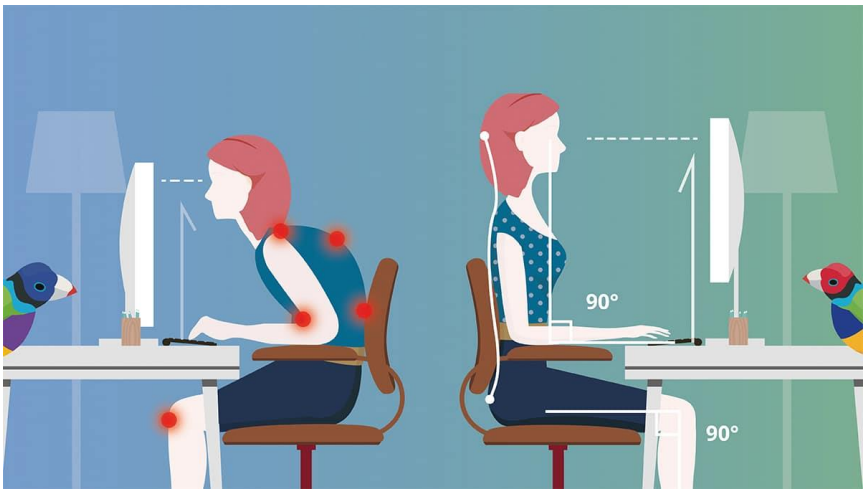
4.3.3 Attività pratiche

Step 1: Protezione degli occhi

1. Sul tuo computer, apri un'applicazione di editing MS Office o Notepad. Noi abbiamo usato Notepad, un software incluso nel sistema operativo Windows.
2. Scrivi un testo di poche lettere/parole, con la dimensione standard definita del carattere, senza cambiarlo.
3. Seleziona con il mouse il testo scritto in Notepad e con il testo selezionato, dalla barra dei menu in alto premi *Formato-> Carattere->* e nell'area denominata *Dimensione carattere* seleziona la dimensione più grande disponibile (nel mio caso 72). Nota come l'occhio ha maggior facilità nel leggere il testo scritto e la sensazione di riposo che si ha quando si legge un testo con un font di dimensioni maggiori.
4. Seleziona ancora con il mouse, il testo scritto in Blocco Note e con il testo selezionato, dalla barra dei menu in alto premi *Formato-> Carattere->* e nell'area chiamata *Dimensione carattere* seleziona la dimensione più piccola disponibile (nel mio caso 8). Nota quanto l'occhio riesce difficilmente a leggere il testo scritto, la sensazione di forzare l'occhio, che si prova quando si legge un testo con un font di dimensioni molto piccole.
5. Se vuoi, per osservare queste 2 differenze, puoi fare questo esercizio più volte.
6. Ora, per favore osserva questo esercizio dalla seguente prospettiva: supponiamo che passi 5 ore al giorno davanti al computer. Sia che tu abbia del lavoro da fare, sia che tu stia guardando un film o delle foto, in ogni momento l'occhio cercherà di adattarsi il più possibile e nel miglior modo possibile per leggere più informazioni possibili dalle immagini visualizzate sul monitor, anche se queste informazioni sono più facili o più difficili da vedere. Questo modo di sforzare l'occhio, nel tempo, può portare a problemi alla vista.
7. Per questo motivo ci sono diversi modi per preservare la salute degli occhi. Google conosce questo problema e nelle estensioni di Google Chrome può essere aggiunta un'estensione chiamata "*eyeCare* – Protezione occhi". Si può cercare nel motore di ricerca di Google con parole chiave come "*Eye Care* Chrome" e dai risultati visualizzati accedere al link eyeCare - Protect your vision - Chrome Web Store (google.com)
8. Nella pagina, accanto all'estensione *eyeCare - Protect your vision*, cliccare sul pulsante "Add to Chrome".
9. Nella nuova finestra aperta clicca sul pulsante Aggiungi estensione
10. Questa estensione è un resto per la regola 20-20-20 (ogni 20 minuti, togli gli occhi dal computer e guarda qualcosa a 20 piedi di distanza per almeno 20 secondi)
11. In questo modo, l'occhio è più incline a guardare ad una diversa distanza dal monitor (6 metri di distanza), contribuendo così alla salute degli occhi.

Step 2: Protezione della salute fisica (postura)

1. La prima cosa da fare in questo esercizio è di essere consapevoli della posizione che hai davanti al computer (non cambiare questa posizione, non allungare la schiena. Rimani esattamente nella stessa posizione in cui sei, per il prossimo punto).
2. Guarda l'immagine sottostante, e determina la posizione in cui ti trovi: quella di sinistra (con la spina dorsale in posizione curva) o quella di destra (con la spina dorsale retta)?



3. Quindi, se ti trovi nella posizione dell'immagine a destra: CONGRATULAZIONI! Ma se ti trovi nella posizione dell'immagine sul lato sinistro, una posizione in cui si trova di solito la maggior parte delle persone, allora devi capire i seguenti aspetti:
4. Dopo un lungo periodo trascorso davanti ad apparecchiature elettroniche, involontariamente, senza rendersene conto, il corpo tende a rilassarsi e dalla corretta posizione di lavoro si può raggiungere la posizione a sinistra dell'immagine, che porta nel tempo a problemi di salute per la colonna vertebrale, soprattutto alle persone che trascorrono molte ore al giorno, e molti giorni a settimana al computer
5. Per questo motivo dobbiamo essere consapevoli della nostra posizione quando lavoriamo al computer e correggerci! Questo piccolo sforzo può mantenere la nostra spina dorsale sana nel tempo.
6. Come sta la tua schiena ora? Hai raddrizzato la tua spina dorsale?

4.4 Proteggere l'ambiente

Unità 4.4	Proteggere l'ambiente
Durata	5 ore
Obiettivi	Essere in grado di selezionare media sicuri, efficienti e convenienti Capire l'impatto dei media digitali Sapere come smaltire i dispositivi elettronici in modo sicuro
Contenuti	4.4.1 Corretto smaltimento dei dispositivi elettronici 4.4.2 Attività pratiche
Risorse	Manuale di formazione, computer con accesso a Internet
Metodo di formazione	Presentazione da parte dell'educatore Discussione/dibattito di gruppo

Tabella 25: Struttura dell'unità di competenza 4.4. – Proteggere l'ambiente del Modulo 4 (Sicurezza).

4.4.1 Corretto smaltimento dei dispositivi elettronici

Perché è importante smaltire i dispositivi elettronici in modo sicuro?

Oltre a proteggere efficacemente le informazioni sensibili sui dispositivi elettronici, è importante seguire le migliori pratiche per lo smaltimento dei dispositivi elettronici. I computer, gli smartphone e le fotocamere permettono di avere una grande quantità di informazioni a portata di mano, ma quando si smaltisce, si regala o si ricicla un dispositivo si possono rivelare inavvertitamente informazioni sensibili, che potrebbero essere sfruttate dai criminali informatici.

I tipi di dispositivi elettronici includono:

- Computer, smartphone e tablet: dispositivi elettronici in grado di memorizzare ed elaborare automaticamente i dati. La maggior parte di essi contiene un'unità di elaborazione centrale e una memoria, e utilizza un sistema operativo che esegue programmi e applicazioni;
- Media digitali: questi dispositivi elettronici creano, memorizzano e riproducono i contenuti digitali. I dispositivi multimediali digitali includono oggetti come fotocamere digitali e lettori multimediali;
- Hardware esterno e dispositivi periferici: dispositivi hardware che forniscono input e output per i computer, come stampanti, monitor e dischi rigidi esterni. Questi dispositivi contengono caratteri digitali memorizzati in modo permanente;
- Console di gioco: dispositivi elettronici, digitali o informatici che emettono un segnale video o un'immagine visiva per visualizzare un videogioco.

Quali sono alcuni metodi efficaci per rimuovere i dati dal dispositivo?

Ci sono diversi metodi per cancellare definitivamente i dati dai tuoi dispositivi (pulizia). Poiché i metodi di pulizia variano a seconda del dispositivo, è importante utilizzare il metodo che si applica a quel particolare dispositivo.

Prima di ripulire un dispositivo, esegui il backup dei tuoi dati: salvare i dati su un altro dispositivo o in un secondo spazio (ad esempio, un disco rigido esterno o il cloud) può aiutare a recuperare i dati se vengono accidentalmente cancellate le informazioni o se il dispositivo viene rubato (questo può aiutarti a identificare le informazioni alle quali un ladro potrebbe aver avuto accesso). Le opzioni per l'archiviazione digitale includono servizi di dati cloud, CD, DVD e unità flash rimovibili o dischi rigidi rimovibili.

I metodi per la pulizia includono:

- Cancellazione dei dati: rimuovere i dati dal dispositivo può essere un metodo di pulizia. Quando si eliminano i file da un dispositivo, anche possono sembrare rimossi, in realtà rimangono anche dopo l'esecuzione di un comando di cancellazione o di formattazione. Non fare affidamento solo sul metodo di cancellazione che usi abitualmente, come spostare un file nel cestino o selezionare "elimina" dal menu. Anche se si svuota il cestino, i file cancellati sono ancora sul dispositivo e possono essere recuperati. La cancellazione permanente dei dati richiede diversi passaggi.
- Computer: utilizzare un software di pulizia del disco progettato per rimuovere definitivamente i dati memorizzati sul disco rigido di un computer per prevenire la possibilità di recupero.
- Cancellazione sicura: questo è un insieme di comandi nel firmware della maggior parte dei dischi rigidi dei computer. Se si seleziona un programma che esegue il set di comandi di cancellazione sicura, cancellerà i dati sovrascrivendo tutte le aree del disco rigido.
- Cancellazione del disco: questa è un servizio che cancella le informazioni sensibili sui dischi rigidi e cancella in modo sicuro le unità flash e le schede digitali sicure.
- Smartphone e tablet: assicurati che tutti i dati vengano rimossi dal tuo dispositivo eseguendo un "*hard reset*". Questo riporterà il dispositivo alle sue impostazioni originali di fabbrica. Ogni dispositivo ha una procedura di *hard reset* diversa, ma la maggior parte degli smartphone e dei tablet possono essere

resettati attraverso le loro impostazioni. Inoltre, rimuovi fisicamente la scheda di memoria e la scheda del modulo d'identità dell'abbonato, se il tuo dispositivo ne ha una.

- Fotocamere digitali, lettori multimediali e console di gioco: esegui un reset di fabbrica standard (cioè un hard reset) e rimuovi fisicamente il disco rigido o la scheda di memoria.
- Apparecchiature da ufficio (ad esempio, fotocopiatrici, stampanti, fax, dispositivi multifunzione): rimuovere qualsiasi scheda di memoria dall'apparecchiatura. Eseguire un reset completo per ripristinare le impostazioni di fabbrica del dispositivo.
- Sovrascrittura: un altro metodo di pulizia consiste nel cancellare le informazioni sensibili sovrascrivendo nuovi dati binari. Usare dati casuali piuttosto che modelli facilmente identificabili rende più difficile per gli hacker scoprire le informazioni originali. Poiché i dati memorizzati su un computer sono scritti con codice binario - stringhe di 0 e 1 - un metodo di sovrascrittura consiste nel riempire zero un disco rigido e selezionare programmi che utilizzano zero nell'ultimo livello. Gli utenti dovrebbero sovrascrivere l'intero disco rigido e aggiungere più strati di nuovi dati (da tre a sette passaggi di nuovi dati binari) per impedire agli hacker di ottenere i dati originali.
- Cipher.exe è un'interfaccia a riga di comando incorporata nei sistemi operativi Microsoft Windows che può essere usata per criptare o decriptare i dati sulle unità *New Technology File System*. Questo strumento cancella anche i dati in modo sicuro, sovrascrivendoli.
- La cancellazione è un livello di pulizia dei media che non permette alle informazioni di essere recuperate da servizi di recupero dati, dischi o file. I dispositivi devono essere resistenti ai tentativi di recupero da dispositivi di input standard (ad esempio, una tastiera o un mouse) e da strumenti di recupero dati.
- Distruzione: la distruzione fisica di un dispositivo è il modo migliore per impedire ad altri di recuperare le tue informazioni. Sono disponibili servizi specializzati che disintegrano, bruciano, fondono o polverizzano l'unità del computer e altri dispositivi. Questi metodi di pulizia sono progettati per distruggere completamente i media e sono in genere eseguiti presso impianti autorizzati di distruzione dei metalli o di incenerimento. Se decidi di non utilizzare il servizio, puoi distruggere autonomamente il disco rigido piantando chiodi o facendo buchi nel dispositivo. I pezzi fisici rimanenti del disco devono essere abbastanza piccoli (almeno 0,2 mm) in modo da rendere impossibile la ricostruzione delle informazioni. Ci sono anche dispositivi hardware disponibili che cancellano CD e DVD distruggendo la loro superficie.
- Smagnetizzatori di supporti magnetici: gli smagnetizzatori espongono i dispositivi a forti campi magnetici che rimuovono i dati memorizzati magneticamente sui supporti magnetici tradizionali.
- Distruzione allo stato solido: la distruzione di tutti i chip di memoria per l'archiviazione dei dati tramite frantumazione, triturazione o disintegrazione è chiamata distruzione allo stato solido. Le unità a stato solido devono essere distrutte con dispositivi specificamente progettati per questo scopo.
- Distruzione di CD e DVD: molti distruggidocumenti da ufficio e da casa possono distruggere CD e DVD (assicurati di controllare che il distruggidocumenti che stai usando possa distruggere CD e DVD prima di tentare questo metodo).

Come si possono smaltire in modo sicuro i dispositivi elettronici scaduti?

Rifiuti elettronici (a volte chiamati *e-waste*) è un termine usato per descrivere i dispositivi elettronici che sono vicini alla fine della loro vita utile e vengono scartati, donati o riciclati. Sebbene la donazione e il riciclaggio di dispositivi elettronici conservi le risorse naturali, puoi comunque scegliere di smaltire i rifiuti elettronici contattando la tua discarica locale e richiedendo di smaltirti in una discarica apposita. Sappi che, sebbene esistano molte opzioni per lo smaltimento, è tua responsabilità assicurarti che il luogo scelto sia affidabile e certificato.

4.4.2 Attività pratiche

Step 1: Consumo di elettricità: costi operativi delle apparecchiature

1. Come tutti sappiamo, le apparecchiature elettroniche possono funzionare solo se alimentate dall'elettricità. Ma quanta energia si consuma per un computer? Per la risposta passiamo al calcolo descritto qui sotto.
2. Consideriamo due unità di computer: un portatile (per esempio quello che uso io) e un computer fisso (un'unità centrale), con caratteristiche tecniche quasi uguali a quelle del portatile
3. Computer portatile: leggo il valore dell'alimentatore del portatile e noto che è 130W (watt)
4. Facciamo insieme il seguente calcolo: portatile usato 7 giorni a settimana (5 giorni al lavoro e 2 giorni nel fine settimana per film, musica, foto, ecc.), circa 8 ore al giorno (h/giorno) in media
5. Stimiamo la durata media di vita del portatile a circa 5-7 anni
6. Calcoliamo il consumo di energia per questo portatile, come segue:

Per un anno di utilizzo	Per 7 anni di utilizzo
• Alimentazione (Watts) x numero di giorni (zile) x giorni medi (h/zi) x 1 anno = 130W x 365 giorni x 8h/giorno x 1 anno = 379.600 Wh/anno = 379,6 kWh/anno (kiloWatts ora in 1 anno)	• Potenza consumata per 1 anno x 7 anni = 379.600 kWh/anno x 7 anni= 2.657.200 Wh = 2.657,2 kWh

Figura 12: Dati per il calcolo del consumo energetico.

7. Calcolo del computer fisso (unità centrale): abbiamo fatto una ricerca su Internet sui migliori alimentatori per un computer: https://www.digitaltrends.com/computing/best-PC-power-supply/ e ho scelto alcuni esempi di alimentatori: "Corsair RM750" 750W, "FSP Dagger" 550W o "Thermaltake Toughpower Grand RGB" 650W

8. Se per il calcolo consideriamo la fonte "FSP Dagger" il valore è 550W (è il più basso in potenza degli esempi). Per la sorgente da 550W applichiamo lo stesso calcolo della figura 12, solo che sostituiamo 130 kWh con 550 kWh e otteniamo 11242 kWh.

9. La differenza (economia) di energia tra computer portatile e computer fisso è approssimativamente: 11.242 - 2.657,2 = 8.584,8 kWh

10. Pensiamo ai seguenti 2 aspetti: da un punto di vista personale se compri un computer portatile avrai un risparmio di elettricità di 8584,8 kWh dopo 7 anni di utilizzo. Se moltiplichi questo valore per il prezzo di un kWh, quanto risparmierai dopo 7 anni di utilizzo?

11. Da un punto di vista globale si usano varie fonti per ottenere elettricità, come l'energia eolica, l'energia idroelettrica, ecc. Se per un solo computer si ottiene un tale risparmio energetico, per 1000 computer della stessa potenza, quante risorse naturali si risparmiano? Per 1.000.000 computer? Quindi in futuro, quando comprerai un computer, dovresti pensare anche alla questione della salvaguardia ambientale.

12. Ora, un piccolo esercizio per te. Se dovessimo scegliere la fonte più potente tra quelle esemplificate da 750W, quanta energia sarebbe stata consumata in 7 anni oltre al computer portatile? Riesci a fare questo calcolo?

Step 2: Riciclo dell'elettronica

Considera l'ipotesi in cui usi una torcia elettrica di notte. Ad un certo punto, avrai la necessità di sostituire la batteria della torcia con una batteria carica. Se questa batteria viene accidentalmente gettata da qualche parte in natura, questa non si dissolverà come le sostanze biodegradabili, ma rimarrà dove è stata gettata per molto tempo. Inoltre, le sostanze acide e tossiche della batteria potrebbero fuoriuscire e contaminare l'area dove è stata gettata, entrare nella falda acquifera e contaminare l'acqua, ecc. Se pensiamo a livello globale, e non solo a questa batteria, ci sono migliaia di tonnellate di rifiuti elettrici che, se non riciclati, possono contaminare l'ambiente. Per questo motivo, è necessario riciclare i rifiuti elettrici, ed esiste una legislazione relativa a questo aspetto.

Come puoi aiutare?

Se hai del materiale elettrico che stai per buttare via (es: un vecchio computer arrugginito o batterie scariche), getta questi rifiuti nei centri di raccolta! In questo modo puoi proteggere l'ambiente!

OPPURE: se non vuoi buttare queste vecchie apparecchiature e vuoi ricevere un piccolo guadagno (supponiamo un vecchio computer) e comprarne uno nuovo, sappi che ci sono programmi governativi (In Romania, per esempio, il Programma di rottamazione per gli elettrodomestici) per stimolare a rinnovare le apparecchiature con altre più economiche e allo stesso tempo riciclarle.

OPPURE: ci sono venditori che, in cambio dei dispositivi vecchi, offrono uno sconto per l'acquisto di nuovo dispositivo della stessa categoria. Queste sono offerte di tipo *BUY-BACK* che contribuiscono al riciclaggio delle apparecchiature elettroniche e sono più efficienti dal punto di vista energetico.

E infine, un piccolo esercizio per te: hai un vecchio computer che vorresti cambiare (non ora, in futuro)? Se è così, prova a svolgere una ricerca su Internet: quali venditori possono offrirti soluzioni di *BUY-BACK*?

Congratulazioni, hai completato il Modulo 4.

Non dimenticarti di controllare le Appendici per maggiori risorse e documenti forniti al fine di supportare lo studio da autodidatta!

Modulo 5: *Problem solving*

Il modulo "*Problem Solving*" è destinato a coloro che sono interessati a identificare e risolvere i problemi più comuni di hardware e software, così come un modo sicuro per selezionare e acquistare gli strumenti necessari per risolvere i problemi quotidiani utilizzando mezzi digitali.

Si prega di notare che le unità descritte possono richiedere il supporto di un istruttore esperto. Anche se le informazioni contenute nel manuale sono scritte in modo da essere facilmente comprensibili, alcune azioni inerenti alle informazioni presentate possono richiedere la supervisione e il supporto di un esperto.

Modulo 5	***Problem solving***			
Durata	**25h**			
Obiettivi	Essere in grado di risolvere comuni e semplici problemi tecnici ICT. Essere in grado di cercare, trovare e scegliere la soluzione adeguata a un determinato problema ICT. Essere in grado di sviluppare sé stessi e rimanere in contatto con lo sviluppo ICT.			
Unità	5.1 Risolvere problemi tecnici	5.2 Individuare i fabbisogni e le risposte tecnologiche	5.3 Utilizzare in modo creativo le tecnologie digitali	5.4 Individuare i divari delle competenze digitali
Organizzazione della formazione	Lezioni frontali *E-Learning*	Lezioni frontali *E-Learning*	Lezioni frontali *E-Learning*	Lezioni frontali *E-Learning*
Durata	7h	7h	6h	5h

Tabella 26: Struttura generale del Modulo 5 (Problem solving).

5.1 Risolvere problemi tecnici

Unità 5.1	Risolvere problemi tecnici
Durata	7h
Obiettivi	Essere in grado di risolvere i problemi legati alla velocità di Internet
Contenuti	5.1.1 Computer e sistemi 5.1.2 Problemi tecnici più comuni 5.1.3 Attività pratiche
Risorse	Manuale di formazione Computer con accesso a Internet Modem
Metodo di formazione	Presentazione da parte dell'educatore

Tabella 27: Struttura dell'unità di competenza 5.1. – Risolvere problemi tecnici del Modulo 5 (Problem Solving).

5.1.1 Computer e sistemi

Il modulo "*Problem Solving*" è destinato a coloro che sono interessati a identificare e risolvere i problemi più comuni di hardware e software, così come un modo sicuro per selezionare e acquistare gli strumenti necessari per risolvere i problemi quotidiani utilizzando mezzi digitali.

Cos'è un computer?

Un computer è un dispositivo elettronico che modifica informazioni o dati. Ha la capacità di memorizzare, recuperare ed elaborare dati. Saprai già che puoi usare un computer per scrivere documenti, inviare e-mail, giocare e navigare sul web. Puoi anche usarlo per modificare o creare fogli di calcolo, presentazioni e persino video.

Quali sono i diversi tipi di computer?

Quando la maggior parte delle persone sente la parola computer, pensa a un personal computer come un desktop o un laptop. Tuttavia, i computer sono disponibili in molte forme e dimensioni, e svolgono molte funzioni diverse nella nostra vita quotidiana

Molti dei dispositivi elettronici di oggi sono fondamentalmente computer specializzati, anche se non sempre pensiamo a loro in questo modo. Ecco alcuni esempi comuni:

I computer tablet o tablet: sono computer palmari sono ancora più portatili dei computer portatili. Invece di una tastiera e un mouse, i tablet utilizzano uno schermo sensibile al tocco per la digitazione e la navigazione. L'iPad è un esempio di tablet.

Smartphone: molti telefoni cellulari possono fare parecchie cose che i computer fanno, tra cui navigare in Internet e giocare. Sono spesso chiamati smartphone e, per molte persone, uno smartphone può effettivamente sostituirsi ad un vecchio computer portatile, ad un lettore di musica digitale e una fotocamera. Tutto nello stesso dispositivo.

Hardware vs. software

Prima di parlare dei diversi tipi di computer, parliamo di due cose che tutti i computer hanno in comune: l'**hardware** e il **software**.

- **L'hardware** è qualsiasi parte del computer che ha una **struttura fisica**, come la tastiera o il mouse. Sono comprese anche tutte le parti interne del computer.
- Il **software** è qualsiasi **insieme di istruzioni** che dice all'hardware **cosa fare** e **come farlo**. Esempi di software includono *browser web*, giochi ed elaboratori di testi.

Cos'è un sistema operativo (OS)?

Un sistema operativo è il software più importante che gira su un computer. Gestisce la memoria e i processi del computer, così come il suo software e l'hardware. Permette anche di comunicare con il computer senza sapere come parlare la lingua del computer. Senza un sistema operativo, un computer è inutile. (esempi di sistemi operativi: Windows, Linux, macOs sono usati per desktop e laptop; Google Android e Apple IOS sono usati per tablet e smartphone).

Cos'è un'applicazione?

Potresti aver sentito persone parlare dell'utilizzo di programma, un'applicazione o un'app, ma cosa significa esattamente? In parole povere, un'applicazione è un tipo di software che ti permette di eseguire compiti specifici. Le applicazioni per computer desktop o portatili sono talvolta chiamate applicazioni desktop, mentre quelle per dispositivi mobili sono chiamate applicazioni mobili.

Se, nella tua vita quotidiana, usi regolarmente i computer, ti imbatterai in problemi tecnici che richiedono la tua attenzione. Anche se la maggior parte dei problemi complessi del computer possono spesso essere risolti da un tecnico specializzato, ci sono molti altri piccoli, ma comuni, problemi che si verificano regolarmente su un computer e sul suo utilizzo nell'ambiente digitale. La buona notizia è che molti problemi con i computer hanno soluzioni semplici, e imparare a riconoscere un problema e risolverlo da soli vi farà risparmiare molto tempo e denaro.

5.1.2 Problemi tecnici più comuni

1. Il computer non si avvia

Un computer che improvvisamente si spegne o ha difficoltà ad avviarsi potrebbe avere un'alimentazione difettosa. Controlla che il computer sia collegato correttamente alla presa di corrente e, se questo non funziona, prova la presa di corrente con un altro dispositivo funzionante per confermare se c'è o meno un'alimentazione adeguata.

2. Lo schermo è nero

Se il computer è acceso ma lo schermo è nero, potrebbe esserci un problema con la connessione tra il computer e lo schermo. Per prima cosa, controlla che il monitor sia collegato a una presa di corrente e che la connessione tra il monitor e il disco rigido del computer sia presente. Se il problema fosse su un computer portatile, allora potrebbe essere necessario affidarsi a un professionista per risolvere il problema in quanto alcuni dei fili interni potrebbero essere usurati.

3. Anomalie di Sistema operativo o Software

Se il sistema operativo o altri software non rispondono o si comportano in maniera anomala, prova a riavviare il computer ed esegui una scansione antivirus. Per evitare che ciò accada, installa un software antivirus affidabile.

4. Windows non si avvia

Se hai problemi ad avviare Windows, allora potresti doverlo reinstallare con il disco di ripristino di Windows.

5. Lo schermo è bloccato

Quando il tuo computer si blocca, potresti non avere altra scelta se non quella di riavviare il computer e rischiare di perdere tutto il lavoro non salvato. I blocchi possono essere un segno di RAM insufficiente, conflitti di registro di sistema, file corrotti o mancanti, o *spyware*. Tieni premuto il pulsante di accensione finché il computer non si spegne, poi riavvialo e mettiti al lavoro per ripulire il sistema in modo che non si blocchi di nuovo.

6. Il computer è lento

Se il tuo computer è più lento del solito, molto spesso, puoi risolvere il problema semplicemente pulendo il disco rigido dai file indesiderati. Puoi anche installare un firewall, strumenti antivirus e antispyware, e programmare scansioni regolari del registro di sistema. I dischi rigidi esterni sono ottime soluzioni di archiviazione per le CPU sovraccariche, e aiuteranno il tuo computer a funzionare più velocemente.

7. Rumori strani

Forti rumori provenienti dal tuo computer sono generalmente un segno di malfunzionamento dell'hardware o di una ventola rumorosa. I dischi rigidi spesso fanno rumore poco prima di cedere, quindi, è il caso di effettuare il backup delle informazioni, per sicurezza. Le ventole sono molto facili da sostituire.

8. Internet lento

Al fine di migliorare le prestazioni del browser di Internet, dovrai eliminare frequentemente i cookie e i file temporanei di Internet. Nella barra di ricercar di Windows, digita '%temp%' e premi invio per aprire la cartella dei file temporanei.

9. Surriscaldamento del PC

Se il computer non ha un sistema di raffreddamento sufficiente, i componenti del computer potrebbero iniziare a generare calore in eccesso durante il funzionamento. Per evitare che il computer si surriscaldi, spegnilo e lascialo riposare. Inoltre, è possibile controllare la ventola per assicurarsi che funzioni correttamente.

10. Interruzione della connessione

L'interruzione della connessione può essere molto fastidiosa. Spesso il problema è semplice e può essere causato da un cavo o una linea telefonica difettosi, questione facilmente risolvibile. Problemi più seri includono virus, una scheda di rete o un modem difettoso, o un problema con il driver.

11. Il tuo smartphone funziona lentamente

Questo è il problema più comune degli smartphone e si verifica soprattutto quando il telefono diventa più vecchio. La ragione che sta dietro la lentezza è l'installazione di applicazioni non necessarie che utilizzano la RAM del dispositivo e salvano un gran numero di file nel telefono.

Elimina tutte le app e i file non necessari dal cellulare, pulisci i dati della cache. Puoi farlo anche con un'app di diagnostica. Se il problema dovesse essere ancora presente, ripristinare i dati di fabbrica.

12. Scarsa durata della batteria

Sfortunatamente, questo problema legato al telefono accade a tutti. I problemi comuni sono: la batteria che si scarica, la ricarica lenta o la carica con caricabatterie difettoso. Siamo incollati al nostro telefono, quindi il problema della batteria che si scarica è comune. Il problema principale si verifica il tuo telefono si sta scaricando senza essere utilizzato.

Scopri se qualche applicazione in particolare sta scaricando troppa batteria, puoi verificarlo in Impostazioni->Batteria, e se identifichi qualche bug, rimuovi le applicazioni in questione. Attiva la modalità di risparmio della batteria, spegni la geolocalizzazione, diminuisci la luminosità.

13. Spazio di archiviazione

La maggior parte della memoria dello smartphone è occupata foto e video. Quando compri un nuovo smartphone dovresti pensare allo spazio di archiviazione perché, dopo un paio di giorni, inizi a farti prendere dal panico per la poca memoria. Pochissimi smartphone hanno una funzione di memoria espandibile al giorno d'oggi.

Prima di tutto, ancella la cache. Usa app come *cache cleaner* che ti permette di pulire la cache per un'app specifica. Disinstalla le app o spostale dal telefono. Trasferisci le immagini sul cloud per liberare lo spazio sul tuo dispositivo.

14. Il telefono o l'app si bloccano

Questo accade quando c'è un bug nelle applicazioni installate o il tuo telefono sta finendo lo spazio. Questo è uno dei problemi più frustranti relativi ai cellulari.

Cancella i dati delle app da "App manager". Evita di usare più app nello stesso momento. Risolvi i problemi del tuo telefono riavviando il dispositivo, rimuovendo la batteria o ripristinando le impostazioni di fabbrica.

15. Surriscaldamento del cellulare

L'uso eccessivo dello smartphone porta al surriscaldamento. Le app pesanti, come i giochi, fanno salire la temperatura del tuo telefono, questo può influire sulle prestazioni della batteria. Forse hai scaricato app dannose che vengono eseguite in background.

Cerca di non usare il tuo telefono mentre è in carica. Non usare app che usano molta CPU e metti da parte il tuo telefono. Se il telefono continua ancora a surriscaldarsi, allora si tratta di un difetto di produzione.

16. Problema di connessione con Bluetooth, Wi-Fi e rete cellulare

Si tratta di un problema temporaneo del cellulare che può essere facilmente risolto. Tieni il telefono in modalità aereo per 30-60 secondi e prova a ricollegarlo. Il problema è ancora presente? Sistema o cambia di nuovo le impostazioni di Bluetooth e Wi-Fi.

17. Le app non vengono scaricate

La causa principale di questo problema è la cache corrotta. Vai sull'app *Google Play Store* e cancella la cache dell'app. Meglio cancellare la cronologia di *Google Play Store*. Assicurati di utilizzare l'ultima versione di *Google Play Store*. Se il problema persiste, cancella i dati e la cache su *Google Play Services*.

18. Problemi di sincronizzazione

Il problema di sincronizzazione si risolve automaticamente dopo qualche tempo. In caso contrario, rimuovi l'account Google e aggiungilo di nuovo. Assicurati che la tua connessione Internet non sia limitata e che funzioni correttamente. Controlla gli aggiornamenti di sistema e aggiornali se necessario.

19. La scheda microSD non funziona sul tuo smartphone

Questo può avvenire quando la tua scheda SD ha errori di lettura/scrittura. Il tuo cellulare non riconosce la scheda SD dopo la formattazione. Controlla la capacità della scheda di memoria e formattala in exFAT se è fino a 32GB. Riavvia il telefono in modalità di ripristino e seleziona pulisci cache su Android. Questo cancellerà la scheda SD e la formatterà in FAT32, più adatto per la memorizzazione in un telefono.

20. Schermo incrinato o immersione in acqua

Il presente problema avviene accidentalmente e non possiamo farci niente. Per evitare tali incidenti, usate una buona protezione per il telefono. Sì, possono essere costosi ma è un investimento degno per evitare questi incidenti.

Un computer è un dispositivo elettronico che gestisce informazioni o dati. Ha la capacità di memorizzare, recuperare ed elaborare i dati. Forse già saprai che è possibile usare un computer per scrivere documenti, inviare e-mail, giocare e navigare sul web. Puoi anche usarlo per modificare o creare fogli di calcolo, presentazioni e persino video.

5.1.2 Attività pratiche

Step 1: Riavvia il tuo modem e i tuoi dispositivi wireless

Una volta collegato il tuo modem e configurata la tua rete domestica, entrambe le connessioni Internet cablate e wireless dovrebbero essere costantemente affidabili. Una scarsa velocità e disconnessioni possono derivare da segnali deboli, vecchie apparecchiature o cavi, interferenze, capacità/limitazioni del dispositivo e, probabilmente, problemi legati a terzi. Se pensi che ci sia un problema con il tuo WiFi, prova queste semplici soluzioni descritte qui di seguito per risolvere i problemi più comuni.

Un semplice riavvio del modem può risolvere molti problemi WiFi o di connessione

1. Scollegare il cavo di alimentazione dal retro del modem WiFi o dalla presa a muro.
2. Attendere 30 secondi.
3. Ricollegare il cavo di alimentazione al modem.

Entro pochi minuti, la tua rete WiFi dovrebbe riapparire nella lista delle reti disponibili sui tuoi dispositivi wireless. Prova a collegare un dispositivo al WiFi per vedere se funziona.

Riavviare i tuoi dispositivi wireless può anche essere la soluzione a molti problemi comuni, compresi ritardi o perdita di accesso a Internet. Vedi il manuale del tuo dispositivo su come eseguire un riavvio standard.

Step 2: Posizionamento e copertura del modem

La posizione del tuo modem in casa gioca un ruolo significativo sulla tua copertura WiFi ed è un fattore chiave per una connessione WiFi stabile. Per una migliore copertura WiFi, il tuo modem dovrebbe essere collocato in una posizione centrale, questo funziona particolarmente bene se hai una casa *open space*. In alternativa, posizionare il tuo modem dove Internet viene usato più spesso è una buona scelta. Assicurati di posizionare il tuo modem

✓ All'aperto

✓ Alzato da terra

Evita di posizionare il tuo modem

✕ In cantina

✕ negli armadi

✕ Dietro altri oggetti

Per evitare interferenze, cerca di tenere il tuo modem lontano da

✕ Elettrodomestici

✕ Oggetti di metallo

✕ Apparecchiature elettriche

Step 3: Controlla i collegamenti

Connessioni lente, cavi danneggiati e splitter di linea possono degradare i segnali Internet prima ancora che raggiungano il tuo modem e impedirti di raggiungere velocità Internet più elevate. Per risolvere questo problema, dovresti assicurarti che i tuoi cavi siano collegati correttamente.

1. Scollega il cavo di alimentazione dal retro del modem.
2. Svita il cavo coassiale dal retro del modem.
3. Ispeziona il cavo coassiale per individuare eventuali pieghe o piegature che indicano un danno.
4. Segui il cavo coassiale fino al jack del cavo sul muro.
5. Determina se il cavo coassiale va direttamente nel jack o se passa attraverso altri dispositivi, come uno splitter.
6. Se è presente uno splitter, rimuovi temporaneamente lo splitter in modo che la linea coassiale possa collegare direttamente il jack del cavo al modem.
7. Ricollega i cavi coassiali e di alimentazione al retro del modem.
8. Aspetta che il modem torni online.

Se stai usando un cavo Ethernet per collegare il tuo computer al router, o il tuo modem a un router di terze parti, ispeziona anche questi cavi e sostituiscili se sembrano danneggiati.

Step 4: Ripristina le impostazioni del modem

In alcune rare circostanze, potrebbe essere utile, come ultima alternativa, ripristinare il modem alle impostazioni di fabbrica, resettando tutte le impostazioni personalizzate che impostate, compresi il nome e la password di default della rete Wi-Fi che si trovano sull'etichetta del modem.

Per ripristinare il modem:

1. Individua il piccolo pulsante di reset a foro stenopeico del tuo modem.
2. Premi e tieni premuto il pulsante con una graffetta o uno spillo per 15 secondi.
3. Guarda le luci del modem lampeggiare e poi, dopo qualche istante, rimanere accese.

Entro pochi minuti, la tua rete Wi-Fi dovrebbe riapparire nella lista delle reti disponibili sui tuoi dispositivi wireless. Prova a collegare un dispositivo al Wi-Fi per vedere se funziona.

5.2 Individuare i fabbisogni e le risposte tecnologiche

Unità 5.2	Individuare i fabbisogni e le risposte tecnologiche
Durata	7h
Obiettivi	Essere in grado di risolvere comuni e semplici problemi tecnici ICT.
Contenuti	5.2.1 Individuare le esigenze e le risposte tecnologiche 5.2.2 Attività pratiche
Risorse	Manuale di formazione Computer con accesso a Internet
Metodo di formazione	Presentazione da parte dell'educatore

Tabella 28: Struttura dell'unità di competenza 5.2. – Individuare i fabbisogni e le risposte tecnologiche del Modulo 5 (Problem Solving).

5.2.1 Individuare le esigenze e le risposte tecnologiche

Il primo passo quando si tratta di risolvere qualsiasi problema informatico è scoprire quale componente non funziona correttamente. A volte è dovuto a qualcosa di semplice come l'audio che non funziona, o non riusciamo a vedere bene lo schermo o la tastiera/mouse hanno smesso di funzionare. Altre volte il computer non si avvia nemmeno, si riavvia improvvisamente o si spegne e non sappiamo cosa stia succedendo. Per identificare il problema, dobbiamo prestare attenzione agli indizi che il computer ci dà.

Ci sono molte cose diverse che potrebbero causare un problema con il computer. Non importa quale sia la causa del problema, la risoluzione sarà sempre un processo di tentativi ed errori, in alcuni casi, potrebbe essere necessario utilizzare diversi approcci prima di trovare una soluzione. Altri problemi potrebbero essere facili da risolvere. Si consiglia di iniziare utilizzando i seguenti suggerimenti.

- **Scrivi i passaggi**: una volta iniziato a risolvere i problemi, potresti scrivere ogni passo che fai. In questo modo, sarai in grado di ricordare esattamente ciò che hai fatto evitando di ripetere gli stessi errori. Se dovessi chiedere aiuto ad altre persone, sarà molto più facile sapere esattamente quello che hai fatto.
- **Prendi nota dei messaggi di errore**: se il tuo computer ti mostra un messaggio di errore, assicurati di scrivere quante più informazioni possibili. Potresti usare queste informazioni in seguito, per scoprire se altre persone stanno avendo lo stesso problema.
- **Controlla sempre i cavi**: se si hanno problemi con un pezzo specifico dell'hardware del computer, come il monitor o la tastiera, un primo passo facile è controllare tutti i cavi per assicurarsi che siano collegati correttamente.
- **Riavvia il computer**: quando le soluzioni provate non funzionano, riavviare il computer è una buona cosa da provare. Questo può risolvere un sacco di problemi di base che si possono verificare con il computer.

- **Usa il processo di eliminazione**: se stai riscontrando un problema con il tuo computer, potresti scoprire cosa c'è di sbagliato grazie al processo di eliminazione. Questo significa che farai una lista di cose che potrebbero essere la causa del problema e poi le proverai una per una al fine di eliminarle. Una volta identificata la fonte del problema del computer, sarà più facile trovare una soluzione.

Ricerca su Internet

È possibile trovare soluzioni attraverso migliaia di video tutorial su YouTube o da fonti online che forniscono istruzioni passo dopo passo sulla risoluzione dei problemi del computer.

Cos'è un video tutorial?

È una guida video su come risolvere un problema specifico.

Qual è lo scopo di un video tutorial?

I video tutorial offrono un'esperienza multidimensionale che può combinare grafici, diapositive, foto, grafica, narrazione, *screenshot*, didascalie, musica e video live. Questo permette agli studenti con diverse capacità di apprendimento di conservare le informazioni nella maniera più adatto a loro.

Per esempio, se volete installare una stampante potete digitare su un motore di ricerca "tutorial installazione stampante". Uno dei risultati è un video chiamato: ***Set up or Install a Printer on Windows 10|How-To*** https://www.youtube.com/watch?v=E83yneh4xCA, cliccaci sopra e segui passo dopo passo le informazioni relative all'installazione della stampante.

Fonti online: siti web che possono fornirti il giusto *know-how* nella risoluzione dei problemi del computer e nel supporto tecnico.

Esempio: *Bleeping Computer*: http://www.bleepingcomputer.com

Il sito è un'eccellente fonte di informazioni, consigli e tutorial su software e hardware, risoluzione dei problemi e sicurezza, per citarne alcuni. Ha un database, in cui poter cercare gli articoli, che viene aggiornato mensilmente dai suoi collaboratori regolari.

Esempi di ciò che necessita un hardware:

- **Telecamera web**: una webcam è una videocamera che alimenta o trasmette un'immagine o un video in tempo reale a/attraverso una rete di computer, come Internet. Le webcam sono in genere piccole telecamere che si trovano su una scrivania, si attaccano al monitor dell'utente o sono integrate nell'hardware.
- **Stampante**: una macchina per stampare testo o immagini, specialmente una collegata a un computer.
- **Scanner:** un dispositivo che scansiona documenti e li converte in dati digitali.
- **Microfono:** un microfono (abbreviato: mic) è un dispositivo elettronico che converte le onde audio in segnali elettronici, che vengono poi presi dal computer come ingresso. Nei desktop, il microfono è come qualsiasi altra periferica e di solito viene collegato separatamente.
- **Altoparlanti audio**: gli altoparlanti sono trasduttori che convertono le onde elettromagnetiche in onde sonore. Gli altoparlanti ricevono l'input audio da un dispositivo come un computer o un ricevitore audio. Il suono prodotto dagli altoparlanti è definito dalla frequenza e dall'estensione. La frequenza determina quanto l'altezza del suono sia alta o bassa.
- **Fotocamera smartphone**: gli smartphone con fotocamera possono eseguire applicazioni mobili per aggiungere funzionalità come la geolocalizzazione e lo *stitching* di immagine. A partire dalla metà del 2010, alcuni telefoni con fotocamera avanzata dispongono della stabilizzazione ottica (OIS), sensori più grandi, lenti luminose, video 4K e anche zoom ottico.
- **Porte e connessioni**: nell'hardware del computer, una porta è interfaccia tra il computer e altri computer o dispositivi periferici. In termini informatici, una porta si riferisce generalmente alla parte di un dispositivo informatico disponibile per la connessione a periferiche come i dispositivi di input e output.
- **Tecnologia wireless**: la tecnologia wireless fornisce la capacità di comunicare tra due o più entità a distanza senza l'uso di fili o cavi di qualsiasi genere. Alcuni di questi termini potrebbero esservi familiari: trasmissioni radiotelevisive, comunicazione radar, comunicazione cellulare, sistemi GPS, Wi-Fi, Bluetooth e identificazione a radiofrequenza sono tutti esempi di "wireless", con usi ampiamente diversi in alcuni casi.

Esempi delle esigenze del software:

- **Estensioni dei file**: le estensioni dei file costituiscono una maniera di etichettare i file in modo che tu e il tuo computer possiate tenere traccia di ciò che contengono. L'ultima parte del nome del file è usata per indicare il tipo di file in modo che il computer possa aprire il programma corretto quando vuoi usare il file.

  Windows usa le estensioni per determinare come aprire i diversi tipi di file. Quando un utente fa doppio clic su un file per aprirlo, Windows lo aprirà con l'applicazione associata all'estensione di quel file. La configurazione di sistema di Windows mantiene una lista di applicazioni e le relative estensioni associate. Questi sono chiamati "programmi predefiniti". Se una particolare estensione è registrata con un programma, Windows avvierà quel programma ogni volta che l'utente sceglie di aprire un file con quell'estensione. Tuttavia, per ogni estensione, una sola applicazione può essere registrata come

programma predefinito. Per usare un programma diverso da quello predefinito per aprire un file, clicca con il tasto destro sul file e scegli "Apri con".

- **Aggiornamento software**: gli aggiornamenti del software sono importanti perché spesso includono patch critiche per le falle di sicurezza. Possono anche migliorare la stabilità del tuo software e rimuovere funzioni obsolete. Tutti questi aggiornamenti hanno lo scopo di rendere migliore l'esperienza dell'utente
- **Installazione dell'antivirus**: il software antivirus aiuta a proteggere il tuo computer da malware e hacker informatici. Il software antivirus esamina i dati (pagine web, file, software, applicazioni) che viaggiano in rete verso i tuoi dispositivi. Cerca di bloccare o rimuovere il malware il più rapidamente possibile.
- **Impostazioni di visualizzazione**: il tuo computer ha una serie di impostazioni di visualizzazione che ti permettono di personalizzare la tua esperienza visiva in base alla tua attività. Le impostazioni di visualizzazione sono regolabili in base all'uso del computer e al tipo di monitor che si possiede.

5.2.2 Attività pratiche

Step 1: Riavvia il tuo telefono

1. Sulla maggior parte dei telefoni, premi il pulsante di accensione del telefono per circa 30 secondi, o fino a quando il telefono si riavvia
2. Sullo schermo, potrebbe essere necessario selezionare *Riavvia* .

Step 2: Controlla gli aggiornamenti di Android

Importante: le impostazioni possono variare a seconda del telefono.

1. All'interno del telefono, apri *Impostazioni*.
2. Nella parte inferiore, premi *Sistema* › *Avanzate* › *Aggiornamento di sistema*. Se necessario, premi su *Informazioni del telefono* o del *tablet*.
3. Apparirà il tuo stato di aggiornamento. Segui tutti i passaggi sullo schermo.

Step 3: Controlla lo spazio di archiviazione e libera lo spazio

Il tuo telefono può iniziare ad avere problemi quando meno del 10% dello spazio è libero. Se sei a corto di spazio qui sotto puoi trovare informazioni su come liberarlo.

Elimina foto e video

1. Apri l'app di *Google Photos* sul tuo Android o tablet.

2. Effettua il login sul tuo account Google.
3. Tocca e tieni premuto una foto o un video che vuoi spostare nel cestino. Puoi selezionare più elementi.
4. In alto, premere sull'icona del *Cestino* .

Sulla maggior parte dei telefoni, puoi controllare quanto spazio di archiviazione hai a disposizione nell'app *Impostazioni*. Le impostazioni possono variare a seconda del telefono.

Svuota il cestino

Se vedi il messaggio "Elimina definitivamente" quando cerchi di spostare un elemento nel cestino, il tuo cestino è pieno. Il tuo cestino può contenere 1,5 GB.

Importante: se svuoti il cestino, cancelli definitivamente tutti gli elementi nel cestino.

1. Apri l'app di *Google Photos* sul tuo Android o tablet.
2. Effettua il login sul tuo account Google.
3. In basso, premi *Libreria* › *Cestino* › *Ulteriori informazioni* › *Svuota cestino* › *Cancella*.

Rimuovere film, musica e altri media scaricati

Per eliminare contenuti da Google Play:

1. Aprire l'applicazione Google Play con il contenuto, come Play Musica or Play Film e TV.
2. Premi l'icona del *Menu* › *Impostazioni* › *Gestione download*.
3. Premi su *Scaricati* › *Rimuovi*.

Per eliminare i contenuti da altre fonti, cancellali dall'app che hai usato per scaricarli.

Step 4: Chiudi le applicazioni che non rispondono

Android gestisce la memoria utilizzata dalle app. Di solito non è necessario chiudere le app, ma se un'app non risponde, prova a chiuderla.

Step 5: Aggiorna le app

1. Sul tuo telefono, apri l'applicazione *Google Play Store* .
2. Premi l'icona del *Menu* › *Le mie app e i miei giochi*.
3. Le applicazioni con aggiornamenti disponibili hanno la scritta "*Aggiorna*."
    - Se un aggiornamento è disponibile premi su *aggiorna*.
    - Se sono disponibili più aggiornamenti premi su *aggiorna tutto*.

Step 6: Disinstalla le applicazioni che non usi

Attenzione: Tutti i dati salvati in questa applicazione saranno cancellati.

1. Tocca e tieni premuto l'app che vuoi disinstallare.
2. Per vedere le opzioni, inizia a trascinare l'app.
3. Trascina l'app su *Disinstalla* nella parte superiore dello schermo. Se non vedi "Disinstalla", non puoi disinstallare l'app.
4. Solleva il dito.

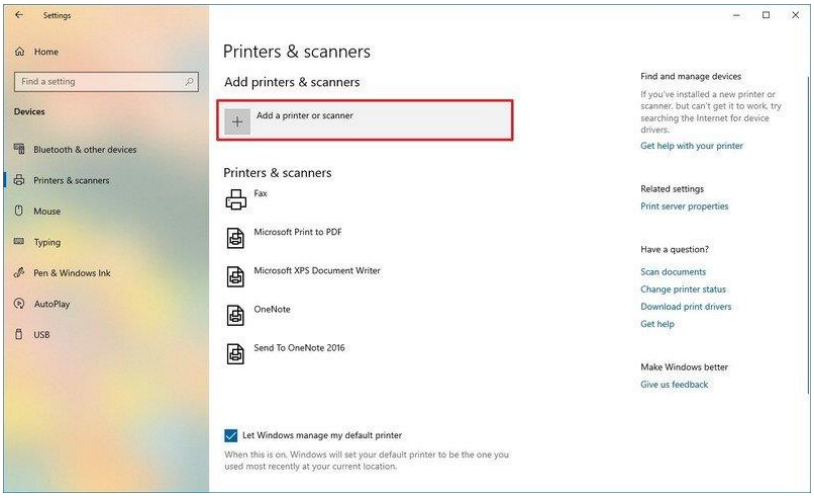
Suggerimento: se vuoi usare di nuovo l'app, puoi provare a reinstallarla.

Installare manualmente una stampante locale

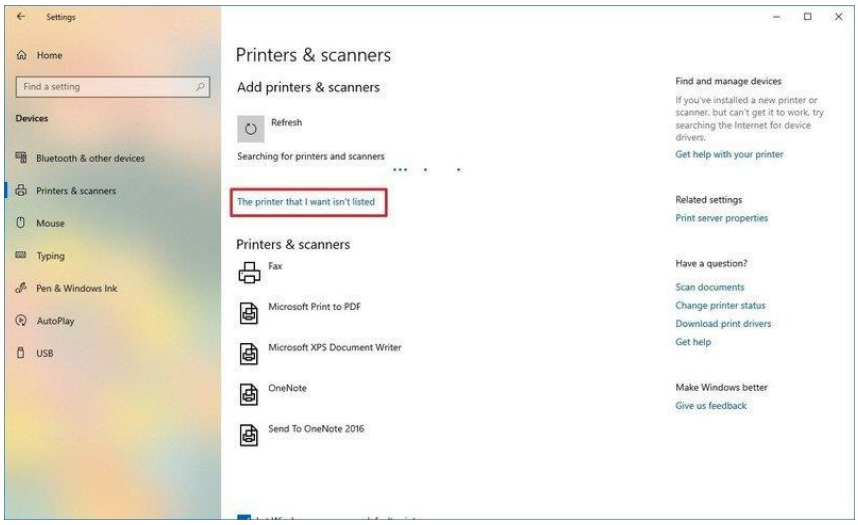
Quando il sistema non rileva automaticamente la tua stampante, puoi aggiungere il dispositivo manualmente a seconda del tipo di connessione e dell'età della stampante.

Importante: prima di procedere, assicurati che il tuo computer sia collegato a Internet per permettere a Windows Update di scaricare i driver aggiuntivi.

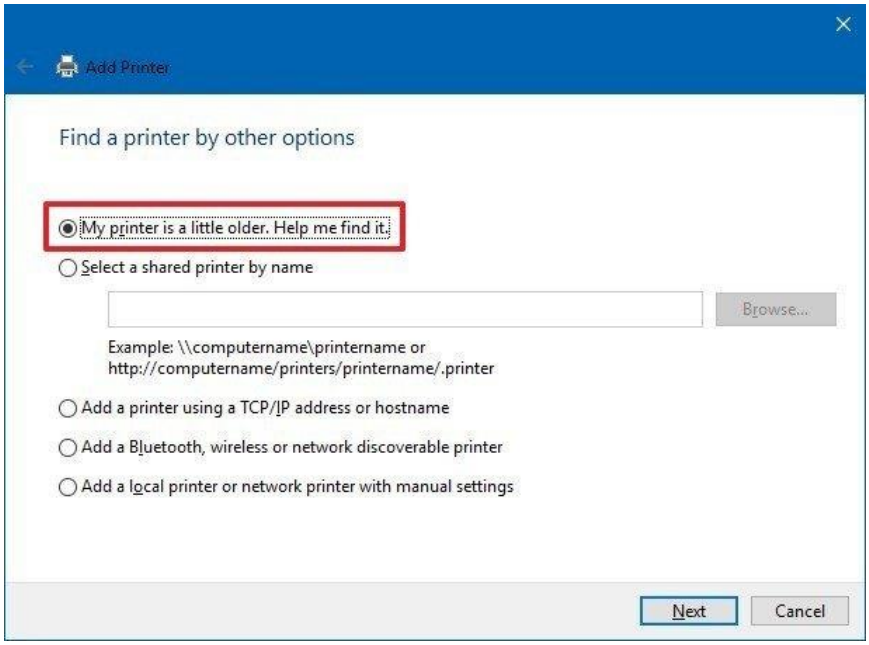
1. Apri ***Impostazioni***.
2. Clicca su ***Dispositivi***.
3. Clicca su ***Stampanti e Scanner***.
4. Clicca sul bottone ***Aggiungi una stampante o uno scanner***.



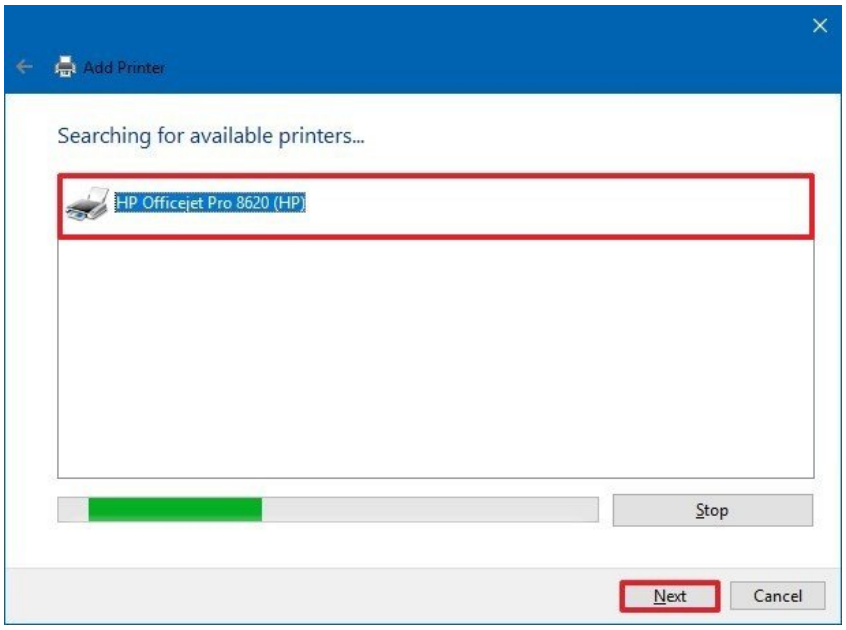
5. Aspetta qualche istante.
6. Clicca l'opzione ***La stampante desiderata non è nell'elenco***.



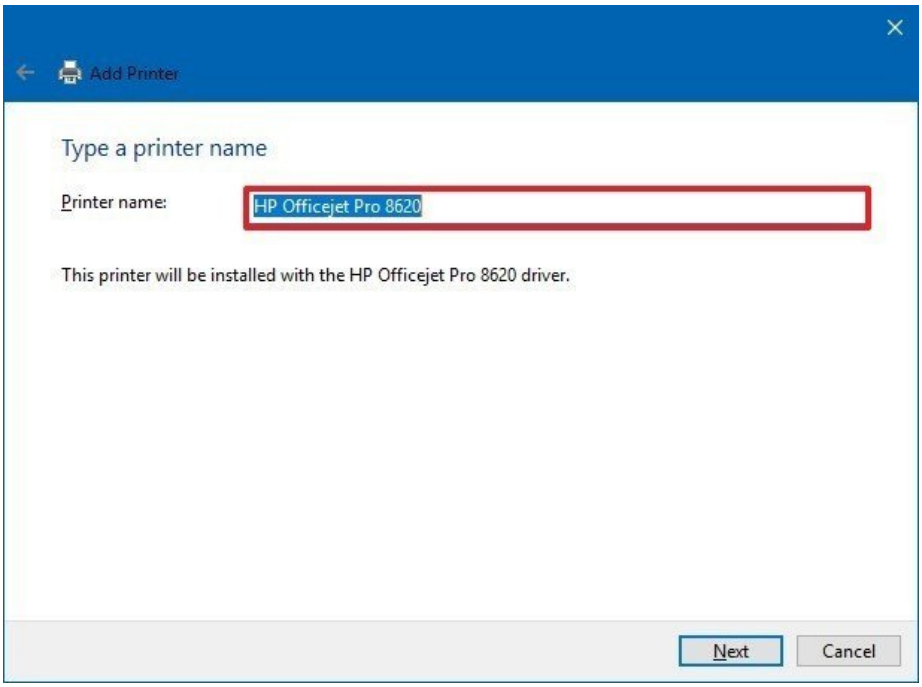
7. Seleziona l'opzione ***La stampante non è recente. Serve assistenza per trovarla***.



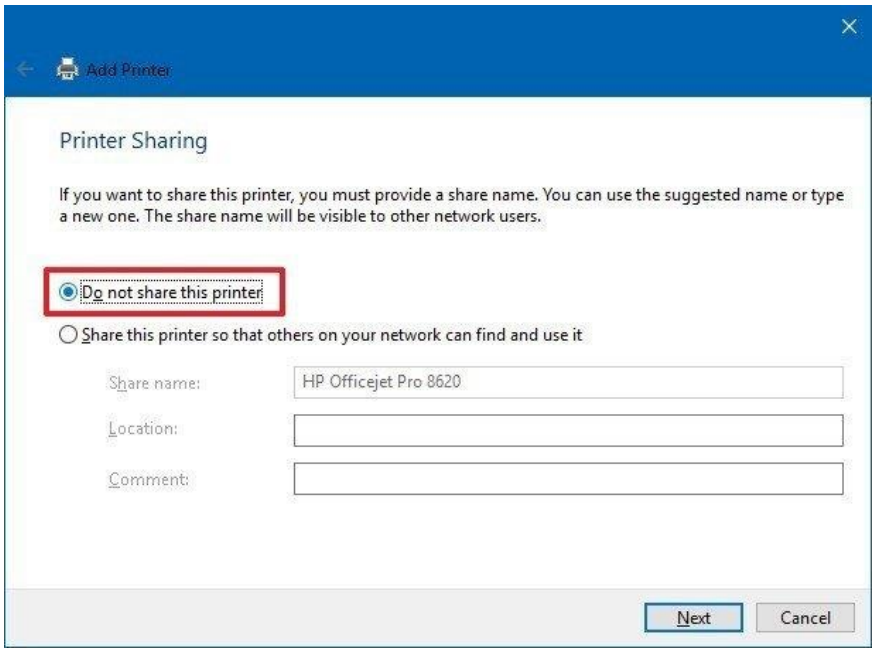
8. Seleziona la tua stampante dalla lista.
9. Clicca ***Avanti***.



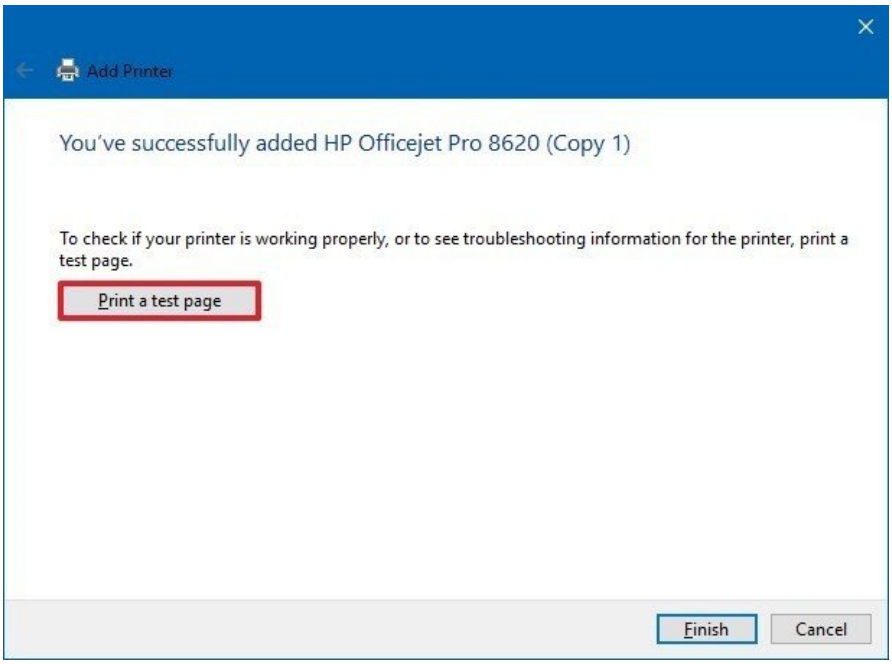
10. Scrivi il nome della stampante.
11. Clicca ***Avanti***.



12. Seleziona l'opzione ***Non condividere questa stampante***.
13. Clicca ***Avanti***.



14. Seleziona l'opzione ***Stampa una pagina di prova*** per confermare che il dispositivo funzioni.



15. Clicca ***fine***.

Una volta completati questi passaggi, dovresti riuscire ad avviare la stampa sul dispositivo.

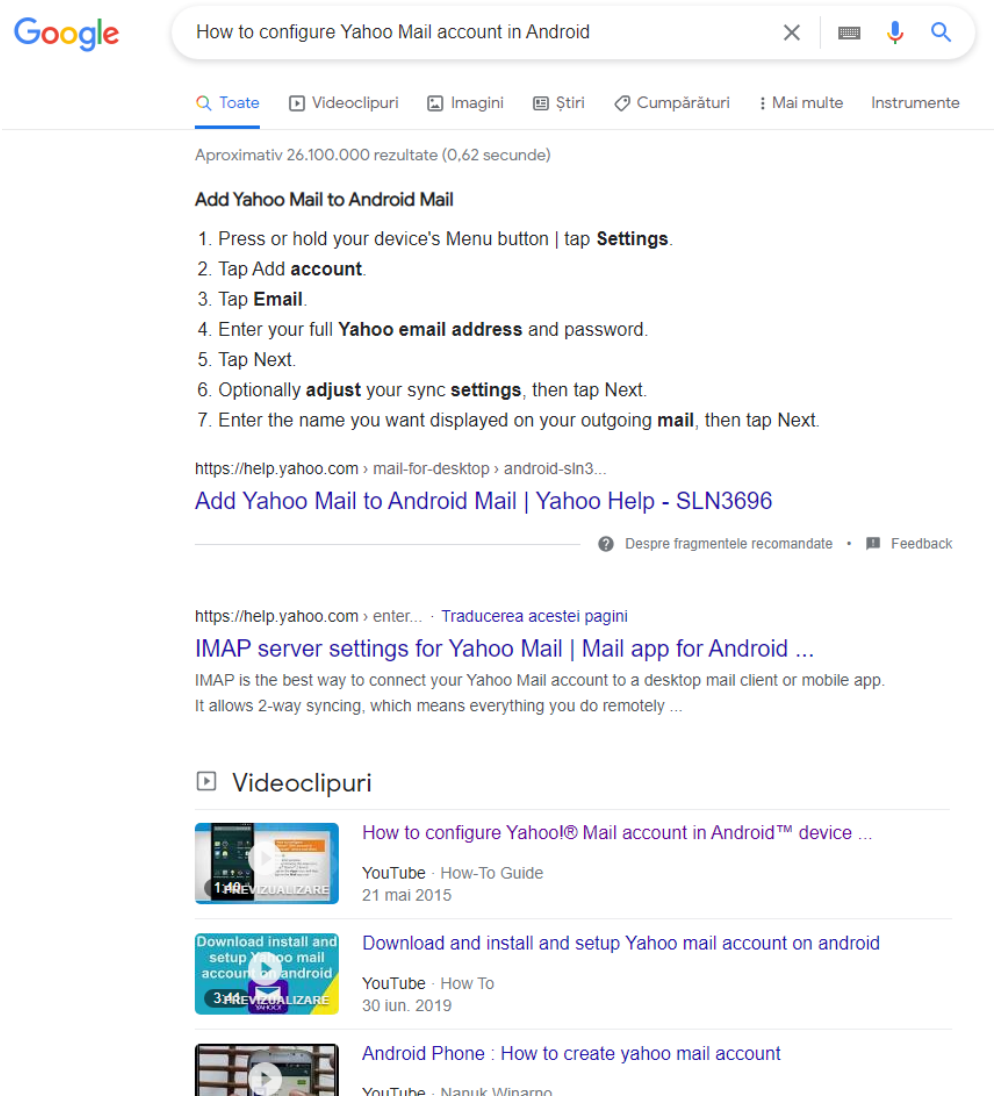
Come configurare l'account mail Yahoo!® sul tuo dispositivo Android

Vuoi controllare le e-mail del tuo account Yahoo!® Mail sul tuo dispositivo Android™? Se vuoi configurare l'account Yahoo!® Mail nel client di posta del tuo dispositivo smartphone, puoi utilizzare un video tutorial per aiutarti a risolvere questa situazione.

1. Apri una pagina del browser e digita il nome di un motore di ricerca, ad esempio Google.

2. Sulla barra del motore di ricerca Google digita "Come configurare l'account Yahoo Mail in Android".

3. Molti risultati appariranno sullo schermo. Scegli uno dei risultati video dei criteri de ricerca e fai doppio clic. Ad es. primo video: (https://www.youtube.com/watch?v=C0KxJ-T7rRw)



4. Guarda questo video e segui i passaggi.

Chiedi alle persone di fare esempi dei bisogni e ripetere la ricerca di tutorial in base alle loro risposte.

5.3 Utilizzare in modo creativo le tecnologie digitali

Unità 5.3	Utilizzare in modo creativo le tecnologie digitali
Durata	6h
Obiettivi	Comprendere ed esplorare le tecnologie digitali creative
Contenuti	5.3.1 Creatività digitale 5.3.2 Attività pratiche
Risorse	Manuale di formazione Computer con accesso a Internet
Metodo di formazione	Presentazione da parte dell'educatore Discussione/dibattito di gruppo Lavoro in coppie/piccoli gruppi

Tabella 29: Struttura dell'unità di competenza 5.3. – Utilizzare in modo creativo le tecnologie digitali del Modulo 5 (Problem Solving).

5.3.1 Creatività digitale

La creatività sta rapidamente diventando una delle caratteristiche più apprezzate del XXI secolo, e secondo un rapporto del 2016 del *World Economic Forum*, è una delle tre principali competenze che i datori di lavoro cercheranno entro il 2020. Un sondaggio di IBM ha anche scoperto che il 60% dei CEO ritiene che la creatività sia la qualità di leadership più importante oggi.

La creatività digitale è un campo nuovo, dinamico, interdisciplinare e in rapida crescita. Mentre c'è una crescente chiarezza su cosa sia la creatività, il significato di digitale si espande quotidianamente. Non sorprende che la creatività digitale possa significare molte cose diverse nel business, nel terzo settore, nell'educazione e nell'apprendimento informale.

Nuovi hardware/software stanno indubbiamente permettendo ai giovani di impegnarsi con il mondo, spesso in modo giocoso e sperimentale, in modi che non avrebbero potuto fare neanche dieci anni fa. Certamente la creatività digitale è sorprendentemente veloce e, con ogni probabilità, è più della somma di digitale + creatività.

Esempi di creatività digitale:

- **Elaborazione del testo:** in informatica, il termine **elaborazione del testo** si riferisce alla teoria e alla pratica di automatizzare la creazione o la manipolazione del **testo** elettronico. Il termine **elaborazione** si riferisce all'**elaborazione** automatizzata (o meccanizzata), in opposizione alla stessa manipolazione fatta manualmente.
- **Editing dei media**: l'editing è il processo di selezione e preparazione di materiale scritto, fotografico, visivo, audio o cinematografico usato da una persona o da un ente per trasmettere un messaggio o un'informazione.
- **Progettazione di presentazioni**: cos'è il **design delle presentazioni? I designer di presentazioni** progettano una serie di idee, storie, parole e immagini in diapositive che sono organizzate per raccontare una storia e persuadere un pubblico.
- **E-mail**: L'**e-mail** è un sistema elettronico per inviare messaggi scritti da un computer a un altro. **E-mail** è l'abbreviazione di ***electronic mail*** (posta elettronica).
- **Social media**: i social media sono una tecnologia *computer-based* che facilita la condivisione di idee, pensieri e informazioni attraverso la costruzione di reti e comunità virtuali. Per progettazione, i social media sono basati su Internet e danno agli utenti una rapida comunicazione digitale dei contenuti.
- **Visualizzazione dei dati**: la visualizzazione dei dati è la rappresentazione grafica di informazioni e **dati**. Usando elementi visivi come diagrammi, grafici e mappe, gli strumenti di **visualizzazione dei dati** forniscono un modo accessibile per vedere e capire tendenze, anomalie e modelli nei **dati**.

Strumenti di creatività digitale

- **Calendari**: un **calendario digitale** ti permette di uscire quando vuoi, vedere gli eventi ricorrenti che avrai, e programmare qualcosa per il 2031 come se fosse la prossima settimana. Lo hai sempre con te. Sicuramente. Per quanto sia meravigliosa un'agenda di carta, è una cosa in più da portare con sé.

- **App per l'editing delle foto**: un'applicazione di **editing delle immagini** per le foto digitali. Si usa per ritagliare e ritoccare le foto, così come per organizzarle in album e presentazioni. Gli editor di **foto** in genere non hanno la miriade di filtri e funzioni di un **editor di immagini** completo come Photoshop di Adobe o Paint Shop Pro di Corel.

- **App di editing del testo**: un **editor di testo** è un tipo di programma per computer che modifica il **testo** semplice. Gli editor di **testo** sono forniti con sistemi operativi e pacchetti di sviluppo software, e possono essere utilizzati per modificare file come i file di configurazione, i file di documentazione e il codice sorgente del linguaggio di programmazione.

- **App per i social media**: le app per i social media sono applicazioni che possono essere scaricate e memorizzate sul tuo telefono o tablet, oppure trasmesse attraverso il tuo browser Internet. Le app dei social media generalmente coinvolgono la messaggistica, la condivisione di foto e i contenuti interattivi. Facebook, Instagram, Twitter.

5.3.2 Attività pratiche

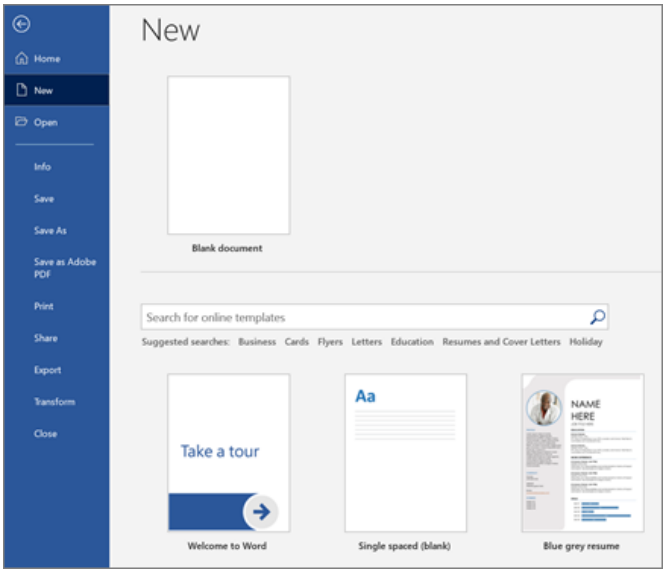
Step 1: Crea un documento

1. Apri un'app di testo come Ms Word.

2. Nella scheda file, clicca *nuovo*.

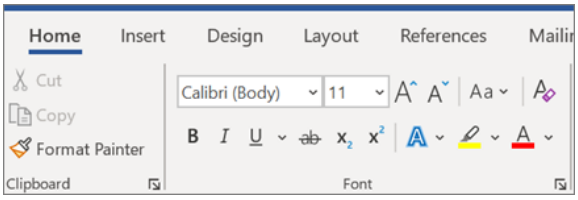
3. Nella casella *Cerca modelli online*, inserisci il tipo di documento che vuoi creare e premi INVIO.

Suggerimento: per iniziare da zero, seleziona il documento vuoto o per fare pratica con le funzioni di Word, prova con una guida all'uso corretto di Microsoft come *Benvenuto in Word*, *Inserisci il tuo primo indice* e *altro*.



4. Aggiungi e formatta il testo

    1. Posiziona il cursore e scrivi il testo.
    2. Per formattare, seleziona il testo e poi un'opzione: grassetto, corsivo, elenco puntato, numerazione...



5. Aggiungi immagini, forme, SmartArt, grafici e altro…

    1. Seleziona l'opzione *Inserisci*.
    2. Seleziona ciò che vuoi aggiungere:

- Tabelle: seleziona *Tabelle*, scorri per ottenere la forma desiderata con il mouse e selezionala.
- Immagini: seleziona *Immagini*, cerca l'immagine desiderata e seleziona *Inserisci*.
- Immagini online: seleziona *Immagini online*, cerca e scegli l'immagine che vuoi, e seleziona *Inserisci*.
- Forme: seleziona *Forme*, e poi scegli una forma dal menu a tendina.
- Icone: seleziona *Icone*, scegli quella che vuoi e clicca *Inserisci*.
- Modelli 3D: seleziona *Modelli 3D*, scegli da un file o da una fonte online, vai all'immagine che vuoi e seleziona *Inserisci*.
- SmartArt: seleziona SmartArt, scegli una grafica SmartArt e clicca *OK*.
- Grafici: seleziona *Grafico*, scegli il grafico che vuoi e clicca *OK*.
- Schermata: seleziona *Schermata* e scegline una dal menu a tendina.

6. Stampa un documento in Word

1. Clicca *File* > *Stampa*.
2. Per vedere in anteprima ogni pagina, clicca sulle frecce avanti e indietro in fondo alla pagina. Se il testo è troppo piccolo da leggere, usa il cursore dello zoom in fondo alla pagina per ingrandirlo.
3. Scegli il numero di copie e tutte le altre opzioni che vuoi e clicca sul pulsante *Stampa*.

Step 2: Crea un post sui social media

Segui i prossimi passi per creare un post su Facebook, sia con l'app mobile che sul sito web di Facebook. I post possono contenere testo, foto, video e dati sulla posizione. Puoi pubblicare sulla tua pagina, su quella di un amico o sulla pagina di un gruppo di cui fai parte.

1. Apri Facebook. L'icona dell'applicazione Facebook assomiglia a una "f" bianca su uno sfondo blu scuro. Facebook si aprirà sul *News Feed* di notizie se sei già loggato.

Se non hai ancora effettuato l'accesso, inserisci il tuo indirizzo e-mail (o numero di telefono) e la password, quindi clicca *Accedi*.

2. Vai alla pagina dove vuoi postare. A seconda di dove vuoi creare il tuo post, questo varierà:

- La tua pagina: puoi creare un post per la tua pagina dalla parte superiore del *News Feed*.
- La pagina di un amico: clicca la barra di ricerca nella parte superiore dello schermo, digita il nome di un amico, seleziona il suo nome, poi tocca la sua immagine del profilo.
- Un gruppo: premi ☰, premi *Gruppi*, premi la scheda *Gruppi* e premi il tuo gruppo.

3. Premi la casella postale. Questa casella si trova nella parte superiore del *News Feed*. Se stai postando sulla pagina di un amico, la casella si trova sotto la sezione delle foto, vicino alla parte superiore della sua pagina. Se stai postando su un gruppo, troverai la casella appena sotto la foto di copertina.

- Di norma, ci sarà una frase come "Scrivi qualcosa" o "A cosa stai pensando? all'interno del riquadro.

4. Carica una foto o un video. Premi *Foto/Video* al centro della schermata del post, quindi seleziona una foto o un video da caricare e premi *Fatto*. Così facendo, la foto o il video vengono aggiunti al tuo post.

- Puoi selezionare più foto o video per caricarli tutti insieme.
- Salta questo passaggio se vuoi caricare un post di solo testo.

5. Aggiungi del testo al tuo post. Premi il campo di testo, quindi digita il testo per il tuo post.

- Puoi anche selezionare un cerchio colorato al centro dello schermo per impostare uno sfondo per il tuo post. Puoi aggiungere colore solo ai post con 130 caratteri o meno.

6. Seleziona Aggiungi al tuo post. Si trova al centro dello schermo. Questo farà apparire le seguenti opzioni di post:

- *Foto/Video*: aggiungi altre foto o video.
- *Registrati*: ti permette di aggiungere un indirizzo o una posizione al tuo post.
- *Stato d'animo, attività*: ti permette di aggiungere uno stato d'animo, un'attività o un'emoji.
- *Tagga persone*: ti permette di aggiungere una persona a questo post. In questo modo il post viene pubblicato anche sulla loro pagina.

7. Seleziona un'opzione post per aggiungere altro al post. Questo passaggio è del tutto opzionale. Se non vuoi aggiungere altro al post, passa allo step successivo.

8. Seleziona *Post*. Si trova nell'angolo in alto a destra dello schermo. Facendo questo creerai il tuo post e lo aggiungerai alla pagina su cui ti trovi.

5.4 Individuare i divari delle competenze digitali

Unità 5.4	Individuare i divari delle competenze digitali
Durata	5h
Obiettivi	Essere in grado di usare le tecnologie per interagire con gli altri
Contenuti	5.4.1 Il divario di competenze digitali in Europa 5.4.2 Attività pratiche
Risorse	Manuale di formazione Computer con accesso a Internet
Metodo di formazione	Presentazione da parte dell'educatore Lavoro in coppie/piccoli gruppi

Tabella 30: Struttura dell'unità di competenza 5.4. – Individuare i divari delle competenze digitali del Modulo 5 (Problem Solving).

5.4.1 Il divario di competenze digitali in Europa

Le tecnologie digitali sono utilizzate in molti settori come l'agricoltura, la sanità, i trasporti, l'istruzione, la vendita al dettaglio, l'automazione, l'energia, la spedizione, la logistica, l'insegnamento e l'industria delle tecnologie dell'informazione e della comunicazione. La domanda di specialisti in tecnologie dell'informazione e della comunicazione sta crescendo rapidamente. In futuro, 9 posti di lavoro su 10 richiederanno competenze digitali. Allo stesso tempo, 169 milioni di europei tra i 16 e i 74 anni (il 44%) non hanno competenze digitali di base.

Come ogni campo, se vuoi crescere in questo campo, devi continuare a imparare.

Gli studenti saranno in grado di scoprire quali miglioramenti dovranno fare per acquisire o migliorare le abilità e le competenze necessarie per svolgere al meglio il loro (futuro) ruolo. Alla fine, questo avrà anche un impatto positivo sulla vita quotidiana.

1. **Investi nell'istruzione:** siti come *Udemy* e *Skillshare* hanno alcuni brillanti corsi su una serie di argomenti digitali. Da SEO e Google Analytics a Social Media e Content Marketing, sarai sicuro di trovare qualcosa nell'area che stai cercando di approfondire. Assicurati sempre di controllare le recensioni prima di acquistare un corso e guarda quanto tempo ci vorrà per completarlo. Alcuni corsi possono essere completati in un giorno, mentre altri richiedono più tempo.
2. **Abbonati:** quando ti imbatti in un articolo veramente utile, clicca su "iscriviti" sul sito per ricevere le future newsletter. Ne vale la pena quando il contenuto si distingue davvero, perché è probabile che gli articoli futuri saranno altrettanto utili.

Assicurati di farlo selettivamente però, poiché l'ultima cosa che vuoi è essere bombardato. Filtrando il contenuto superiore, saprai che quando una mail arriva nella tua casella di posta, vale la pena leggerla.

3. **Unisciti ai gruppi**: comunità, forum e gruppi online possono essere una grande risorsa per rimanere aggiornati in questo campo. Impara dagli altri e condividi la tua esperienza nelle conversazioni in corso. Assicurati solo di procedere con cautela perché alcuni gruppi possono contenere molto spam e informazioni irrilevanti.

   Cerca su Facebook e LinkedIn i gruppi del settore che ti interessa, che sia il marketing digitale in generale o qualcosa di più specifico come l'e-commerce o i social media. Ricorda, più specifico sarai, più le conversazioni e i post saranno rilevanti.

4. **Sali a bordo con Google Alerts**: questo simpatico strumento è un ottimo modo per rimanere aggiornati su tendenze e suggerimenti. Basta far sapere a Google le parole chiave di cui vorresti essere avvisato quando appaiono nei risultati di ricerca e sarai avvisato con un'e-mail.

   Per esempio, quando appare 'tendenze SEO 2019', ti verrà inviata un'e-mail con un link al sito corrispondente. Questo è un ottimo modo per rimanere aggiornati su qualsiasi cosa. Inoltre, è possibile limitare il numero di volte che Google invia le e-mail, e avere tutto incluso in un riassunto settimanale per evitare un bombardamento quotidiano.

5. **Vai su YouTube:** al giorno d'oggi, su YouTube c'è un video per ogni cosa. Sì, a volte bisogna passare al setaccio per trovare le gemme, ma può valerne la pena. Può accadere che un problema per il quale cerchi una soluzione possa essere facilmente risolto in pochi minuti se trovi un video informativo.

6. **Usa gli *hashtag*:** questo è un ottimo modo per cercare tendenze recenti, notizie e aggiornamenti in qualsiasi settore. Basta prendersi qualche minuto quando si viaggia in treno o durante il pranzo per andare su Twitter o LinkedIn e cercare alcuni hashtag. Sarai in grado di navigare tra i contenuti principali sotto quell'hashtag e leggere le ultime notizie. Se ti imbatti in qualcuno che condivide aggiornamenti regolari relativi al tuo settore, probabilmente vale la pena seguirlo.

5.4.2 Attività pratiche

Step 1: Iscriviti ad un canale YouTube

1. Vai su https://www.youtube.com con un browser. Apri YouTube.

2. Accedi al tuo account. Devi aver effettuato l'accesso a un account Google per iscriverti ai canali YouTube. Se non hai effettuato l'accesso, clicca sul pulsante blu "**ISCRIVITI**" in alto a destra e poi accedi con il tuo account Google.

- Se hai già effettuato l'accesso e vuoi cambiare account, clicca sulla foto del profilo in alto a destra, seleziona **Cambia account** e poi scegli un altro account dall'elenco. Se non vedi l'account che vuoi usare, clicca su *Aggiungi account* per aggiungere o creare un altro account**.**

3. Cerca un canale: puoi controllare ciò che è **in tendenza** nel pannello di sinistra, cercare un canale specifico, o trovare qualcosa di nuovo cercando le parole chiave.

- Se conosci il nome del canale a cui vuoi iscriverti (o vuoi cercare per parola chiave), digitalo nella barra di ricerca in alto su YouTube e premi **Invio** o **Return**. Per vedere solo i canali, clicca su **Filtri** nell'angolo in alto a sinistra dei risultati della ricerca e seleziona **Canali** sotto "Genere".
- Puoi anche iscriverti a un canale da qualsiasi video dello stesso. Digita il nome di un video nella barra di ricerca e premi **Invio** o **Return**. Poi, clicca su un video per iniziare a guardarlo: il nome del canale apparirà sotto il titolo del video.

4. Clicca su ISCRIVITI per iscriverti ad un canale. È un pulsante rosso e bianco: se sei sulla home page del canale, sarà vicino all'angolo in alto a destra della pagina sotto l'immagine di copertina. Se hai un video aperto, è sotto il video a destra del nome del canale.

- Ora che sei iscritto, il testo del pulsante "ISCRIVITI" diventerà grigio e cambierà in **ISCRITTO**. Facendo clic su quel pulsante in qualsiasi momento si può annullare l'iscrizione al canale.

5. Visualizza le tue sottoscrizioni: clicca le tre linee orizzontali nell'angolo in alto a sinistra di YouTube per aprire il menu e seleziona **Iscrizioni** per vedere tutti i canali a cui sei iscritto.

- Le tue sottoscrizioni appaiono sotto "ISCRIZIONI" nel pannello di sinistra.
- Clicca su uno dei tuoi canali sottoscritti per vedere il suo contenuto più recente.

6. Regola le tue preferenze di notifica: per impostazione predefinita ti verranno notificati gli aggiornamenti di alcuni canali. Per ricevere più o meno aggiornamenti da un canale, clicca sul canale e poi sull'icona della campanella accanto al pulsante "ISCRITTO". Poi, clicca su **Tutti**, **Nessuno** o **Personalizzato**. **Personalizza** le notifiche in base alla tua attività.

- Per specificare come ti vengono notificati gli aggiornamenti, clicca sulla tua foto del profilo in alto a destra, seleziona **Impostazioni** e poi clicca su **Notifiche** nel pannello di sinistra. Usa i cursori per controllare quali notifiche ti vengono inviate.

Step 2: Unisciti a un gruppo di interesse sui social media

1. Apri Facebook. L'icona dell'applicazione mobile di Facebook è una "f" bianca su uno sfondo blu scuro. Facebook si aprirà al tuo *News Feed* se sei già loggato.

- Se non hai già effettuato l'accesso, inserisci il tuo indirizzo e-mail (o numero di telefono) e la password, quindi premi *Accedi*.

2. Fai click sulla barra di ricerca. Si trova nella parte superiore dello schermo. Questo farà apparire la tastiera del tuo dispositivo.

3. Inserisci il nome di un gruppo o una parola chiave. Digita il nome di un gruppo (o una parola o frase a cui sei interessato), poi premi *Cerca*. Questo cercherà su Facebook gli account, le pagine, i luoghi e i gruppi che corrispondono alla tua ricerca.

4. Seleziona **Gruppi**. Si tratta di una sezione vicina alla parte superiore dello schermo, proprio sotto la barra di ricerca. Questo mostrerà tutti i gruppi relativi alla tua ricerca.

- Potresti dover scorrere l'elenco di schede qui a sinistra per visualizzare l'opzione *Gruppi*.

5. Premi Unisciti vicino ad un gruppo. Il pulsante Unisciti si trova sul lato destro del nome di un gruppo. Premendolo, a destra del gruppo apparirà la scritta "Richiesta effettuata". Una volta che sei stato accettato nel gruppo da un amministratore, potrai postare sul gruppo.

- Se il gruppo è pubblico invece che chiuso, potrai vedere (ma non interagire con) i post e i membri del gruppo.

Congratulazioni, hai completato il Modulo 5 e finito il corso!

Non dimenticarti di controllare le Appendici per maggiori risorse e documenti forniti al fine di supportare lo studio da autodidatta! Molto bene!

No One Behind

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

VALUTAZIONE DEL PROGRAMMA FORMATIVO

1. Valutazione dell'apprendimento

All'interno della metodologia del progetto *No One Behind*, il consorzio ha sviluppato il sistema di valutazione che è debitamente introdotto nel documento *Innovative methodology for educating and training adults from rural zone to improve their digital and ICT skills*[21]. Secondo questo sistema, per ogni unità di competenza sono definiti gli indicatori qualitativi per valutare l'ambito della competenza degli studenti adulti (Tabella):

M1 - Informazioni e *data literacy*	
Navigare, ricercare e filtrare dati, informazioni e contenuti digitali	- Essere in grado di identificare diversi browser. - Essere in grado di riconoscere diversi motori di ricerca. - Essere in grado di cercare informazioni e contenuti online. - Essere in grado di navigare tra gli ambienti digitali. - Essere in grado di capire i rischi di riservatezza e privacy della ricerca su Internet. - Essere in grado di conoscere il ruolo di Internet nell'ottenere informazioni nel contesto del mondo di oggi.
Valutare dati, informazioni e contenuti digitali	- Essere in grado di riconoscere i pericoli delle fake news e della disinformazione nell'era digitale. - Essere in grado di identificare la veridicità dei dati e l'accuratezza delle informazioni digitali. - Essere in grado di rilevare la credibilità e l'affidabilità delle fonti comuni di dati, informazioni e il loro contenuto digitale. - Essere in grado di cercare dati e informazioni affidabili e credibili.
Gestire dati, informazioni e contenuti digitali	- Essere in grado di identificare diversi tipi di programmi, strumenti e ambienti per archiviare e gestire dati, informazioni e contenuti digitali. - Essere in grado di usare strumenti e piattaforme digitali per archiviare e gestire i dati. - Essere in grado di organizzare contenuti e dati in una piattaforma digitale in modo strutturato. - Essere in grado di accedere ad ambienti digitali definendo adeguate impostazioni di privacy.
M2 - Comunicazione e collaborazione	
Interagire attraverso le tecnologie digitali	- Essere in grado di identificare diversi strumenti digitali, caratterizzarli e usarli in accordo con il contesto. - Essere in grado di interagire e comunicare con diversi pubblici usando strumenti e dispositivi digitali adeguati. - Essere in grado di riconoscere e caratterizzare diverse piattaforme e dispositivi digitali per la comunicazione. - Essere in grado di cercare informazioni online in modo sicuro ed etico.
Condividere attraverso le tecnologie digitali	- Essere in grado di condividere informazioni con altri usando strumenti e/o piattaforme adeguate. - Essere in grado di riconoscere e caratterizzare diverse piattaforme e dispositivi digitali per condividere informazioni. - Essere in grado di condividere informazioni con gli altri in modo sicuro ed etico. - Essere in grado di cercare informazioni online in modo sicuro ed etico.
Coinvolgere la cittadinanza	- Essere in grado di comunicare online in modo etico e aperto. - Essere in grado di partecipare online alla società come cittadino.

[21] Consultabile qui.

attraverso le tecnologie digitali	- Essere in grado di usare servizi online legali. - Essere in grado di fornire feedback e opinioni con rispetto per gli altri. - Essere in grado di riconoscere le informazioni e i servizi interattivi online. - Essere in grado di configurare le impostazioni per mantenere private le informazioni.
Collaborare attraverso le tecnologie digitali	- Essere in grado di usare diversi strumenti e piattaforme per comunicare online con gli altri. - Essere in grado di condividere informazioni online usando strumenti e piattaforme appropriate. - Essere in grado di identificare le piattaforme online più usate nel loro Paese o regione. - Essere in grado di distinguere tra le piattaforme di messaggistica istantanea o chat, voice-over-IP, piattaforme di social media, forum ed e-mail.
Netiquette	- Essere in grado di dimostrare un'interazione educata con gli altri online. - Essere in grado di identificare quale tipo di comportamento dovrebbe essere usato in diversi ambienti online (come e-mail, social media o chat). - Essere in grado di applicare le "buone maniere" in un ambiente online comunicando con gli altri. - Essere in grado di capire l'importanza delle regole online quando si usano le risorse digitali.
Gestire l'identità digitale	- Essere in grado di descrivere il concetto di identità digitale. - Essere in grado di capire come proteggere l'identità digitale. - Essere in grado di descrivere semplici modi per proteggere la reputazione online. - Essere in grado di gestire l'impronta digitale. - Essere in grado di sapere come essere rispettosi delle identità digitali degli altri e attenti a ciò che si pubblica su altre persone.
M3 - Creazione di contenuti digitali	
Sviluppare contenuti digitali	- Essere in grado di creare e modificare contenuti digitali in diversi formati. - Essere in grado di creare contenuti e conoscenze nuove e originali. - Essere in grado di rappresentare bene ciò che si intende comunicare. - Essere in grado di identificare il valore del contenuto digitale come aiuto visivo. - Essere in grado di adattare l'espressione attraverso la creazione dei mezzi digitali più appropriati.
Integrare e rielaborare i contenuti digitali	- Essere in grado di modificare informazioni e contenuti in un documento o piattaforma esistente. - Essere in grado di integrare nuove informazioni e contenuti in un documento o piattaforma esistente. - Essere in grado di valutare i modi più appropriati per integrare nuovi elementi specifici di contenuto e informazione.
Copyright e licenze	- Essere in grado di applicare il copyright e le licenze in modo accurato. - Essere in grado di identificare quali licenze sono richieste in determinate circostanze. - Essere in grado di sapere come proteggersi dalla violazione del copyright.
Programmazione	- Essere in grado di elencare semplici istruzioni per un sistema informatico per risolvere un semplice problema o eseguire un compito. - Essere in grado di risolvere semplici problemi tecnici. - Essere in grado di applicare istruzioni per eseguire compiti o risolvere problemi.
M4 - Sicurezza	
Proteggere i dispositivi	- Essere in grado di capire l'importanza di proteggere i dispositivi ed evitare i rischi. - Essere in grado di identificare la differenza tra i diversi tipi di malware. - Essere in grado di capire l'importanza delle misure relative all'affidabilità e alla riservatezza.

Proteggere i dati personali e la privacy	- Essere in grado di proteggere i dati personali. - Essere in grado di capire il rischio di furto d'identità. - Essere in grado di applicare la "Privacy Policy" quando si usano servizi digitali. - Essere in grado di capire le regole di base della sicurezza.
Proteggere la salute e il benessere	- Essere in grado di evitare rischi per la salute e minacce al benessere fisico e psicologico mentre si usano le tecnologie digitali. - Essere in grado di controllare i possibili pericoli e minacce negli ambienti digitali. - Essere in grado di identificare i rischi di un uso improprio dei servizi online e digitali.
Proteggere dell'ambiente	- Essere in grado di riconoscere semplici impatti ambientali delle tecnologie digitali e del loro uso. - Essere in grado di usare i servizi digitali senza esserne dipendenti. - Essere in grado di proteggere l'ambiente dall'impatto dello smaltimento dei dispositivi digitali.
M5 - *Problem Solving*	
Risolvere problemi tecnici	- Essere in grado di navigare online in contesti quotidiani. - Essere in grado di identificare quando un dispositivo digitale è abbastanza appropriato per lavorarci. - Essere in grado di identificare quando si è verificato un problema su un dispositivo o servizio digitale.
Risolvere problemi tecnici	- Essere in grado di riconoscere problemi tecnici provenienti da un dispositivo digitale o dall'ambiente. - Essere in grado di riconoscere i metodi di risoluzione. - Essere in grado di capire come utilizzare gli strumenti di aiuto, le guide pratiche.
Utilizzare in modo creativo le tecnologie digitali	- Essere in grado di usare la tecnologia digitale appropriata per uno scopo specifico (raccogliere informazioni, creare contenuti). - Essere in grado di usare componenti di sistemi digitali e informazioni digitali in condizioni reali.
Utilizzare in modo creativo le tecnologie digitali	- Essere in grado di valutare, sé stessi o altri, per verificare che i nuovi ambienti digitali sono mezzi appropriati per migliorare il livello di competenza digitale. - Essere in grado di cercare opportunità di autosviluppo e di tenersi aggiornati con l'evoluzione digitale.

Tabella 31: Identificazione dei criteri di prova di ogni unità di competenza, per la valutazione del dominio della competenza da parte dei discenti adulti.

Questi criteri basati sull'evidenza dovrebbero essere usati per valutare l'ambito della competenza da parte degli studenti e può essere valutato in due modi:

- Da parte degli educatori degli adulti o dei formatori attraverso l'osservazione delle prestazioni degli studenti durante lo sviluppo delle attività proposte e alla fine della formazione compilando una scheda di valutazione.
- Da parte degli studenti adulti che valutano il loro ambito della competenza compilando una scheda di autovalutazione, all'inizio e alla fine di ogni modulo.

In entrambi i casi, si possono usare le schede di valutazione fornite nelle **Appendici da II a V.**

2. Valutazione del corso

Alla fine del corso di formazione, è prevista la valutazione dello stesso da parte degli studenti beneficiari. La valutazione della formazione permetterà di capire:

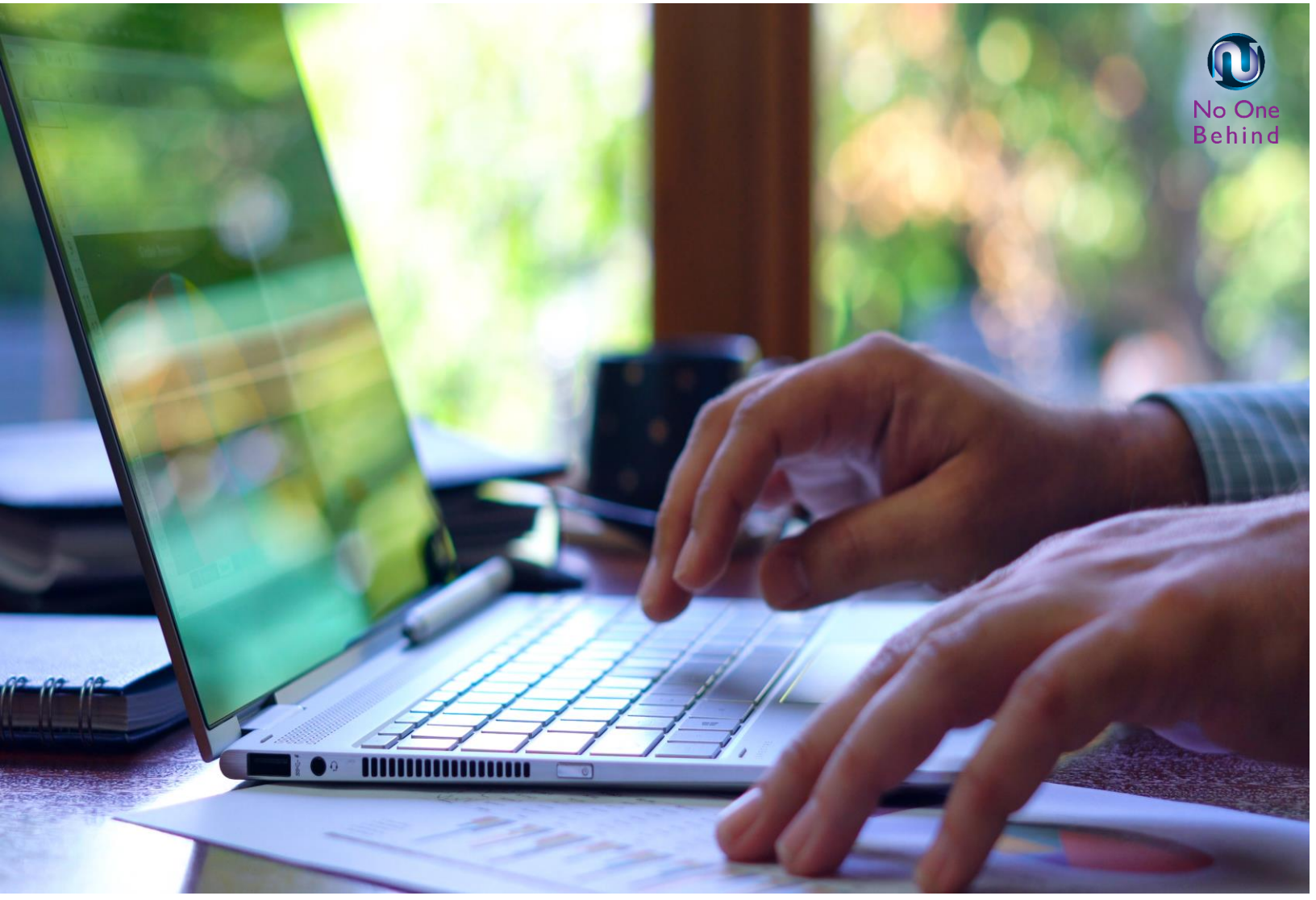
- L'adeguatezza e la pertinenza della formazione ai gruppi target definiti.
- La qualità del curriculum formativo in termini di contenuti e durata.
- Il valore dei supporti e dei materiali forniti.
- Il supporto fornito durante la formazione.

Questo sarà fatto attraverso un questionario (allegato VI) che sarà disponibile online. Raccomandiamo anche un momento di *debriefing*, alla fine di ogni modulo e alla fine del corso dove gli studenti possono trovare lo spazio per parlare della loro esperienza di apprendimento, cosa gli è piaciuto di più e di meno, quali sono state le loro principali difficoltà, come pensano di continuare a praticare ciò che hanno imparato nel corso e così via.

No One Behind

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

APPENDICI



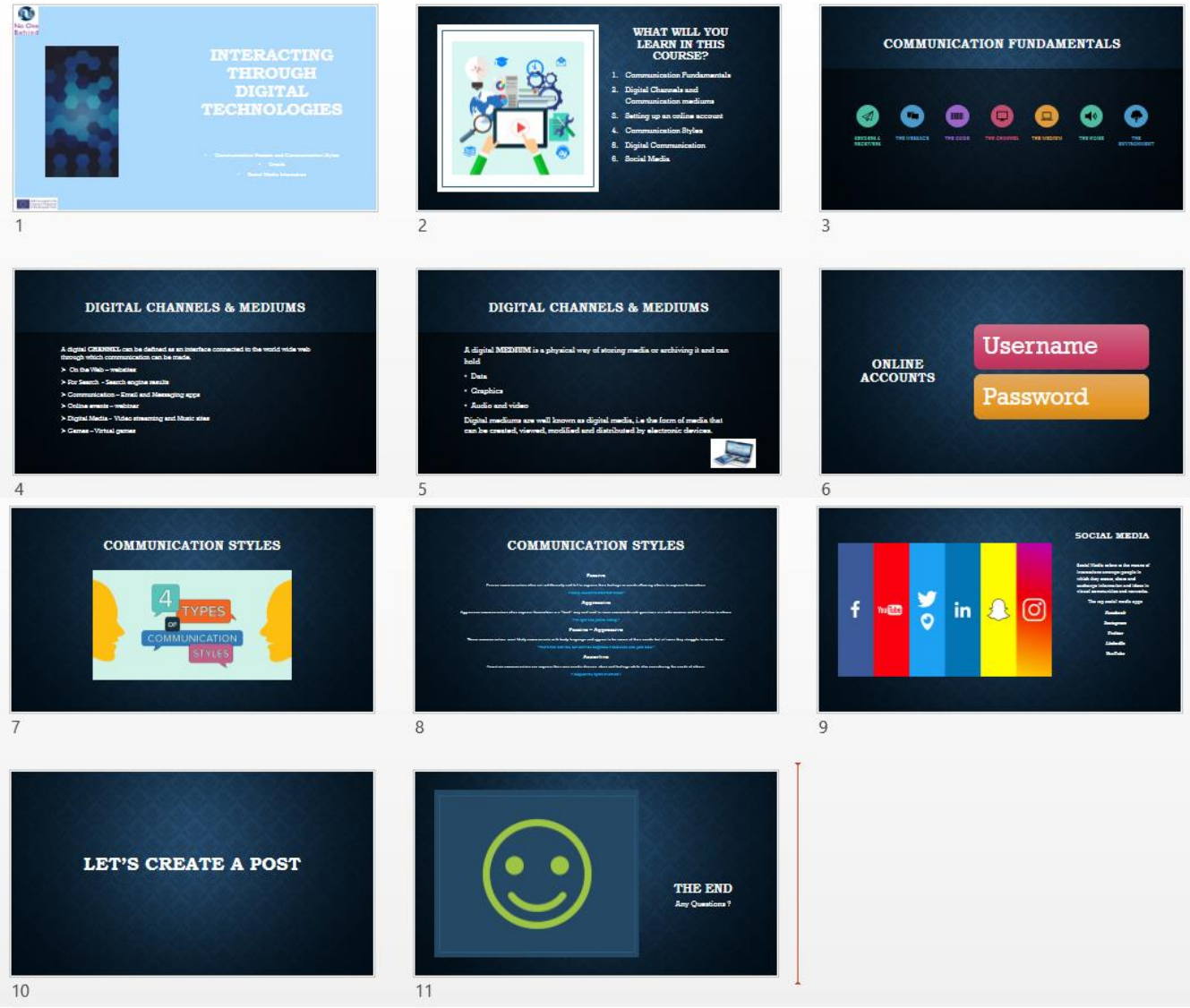
Appendice I – Risorse aggiuntive

Modulo	Unità	Fonti
Modulo 1	1.1	**Formazione online IT**– https://edu.gcfglobal.org/en/subjects/tech/ **Tutorial "Usare i motori di ricerca"** – https://edu.gcfglobal.org/en/Internetbasics/using-search-engines/1/ **Come navigare efficacemente su Internet (1)** – https://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_How_Search_Internet_Effectively.pdf **Come navigare efficacemente su Internet (2)** – https://mediasmarts.ca/sites/default/files/tip-sheet/tipsheet_we_are_broadcasters.pdf
	1.2	**Protezione dei dati** - https://ec.europa.eu/info/sites/default/files/charter-application_en.pdf **Come si diffondono le fake news** - https://www.youtube.com/watch?v=cSKGa_7XJkg
Modulo 2	2.1	**Tutorial base – e-mail**: https: //www.youtube.com/watch?v=cnxsl8h5gj4 **Usare strumenti digitali per trasformare la classe**: https://www.youtube.com/watch?v=B99FXVamqMM **Cosa il tuo stile di comunicazione digitale dice su di te**: https://www.webroot.com/us/en/resources/tips-articles/what-your-digital-communication-style-says-about-you
	2.2	**Nozioni per la condivisione digitale di appunti:** http://blog.whooosreading.org/digital-notes/ **Commenti e condivisioni digitali:** https://applieddigitalskills.withgoogle.com/c/middle-and-high-school/en/create-a-presentation-all-about-a-topic/create-a-presentation-all-about-a-topic/digitally-share-and-comment.html
	2.3	**Cittadinanza digitale:** 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 **Cosa sono le informazioni personali:** https://www.commonsensemedia.org/educators/lesson/keep-it-private-k-2 **La Cittadinanza digitale e i suoi insegnamenti:** https://files.eric.ed.gov/fulltext/EJ1286737.pdf
	2.4	**30 dei migliori strumenti di collaborazione digitale per gli studenti** - https://www.teachthought.com/technology/12-tech-tools-for-student-to-student-digital-collaboration/ **L'importanza del lavoro in gruppo e della collaborazione in un mondo digitale** - https://blog.bit.ai/importance-of-teamwork-and-collaboration/ **Strumenti di collaborazione digitale**: 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=en https://kissflow.com/project/best-project-management-tools/

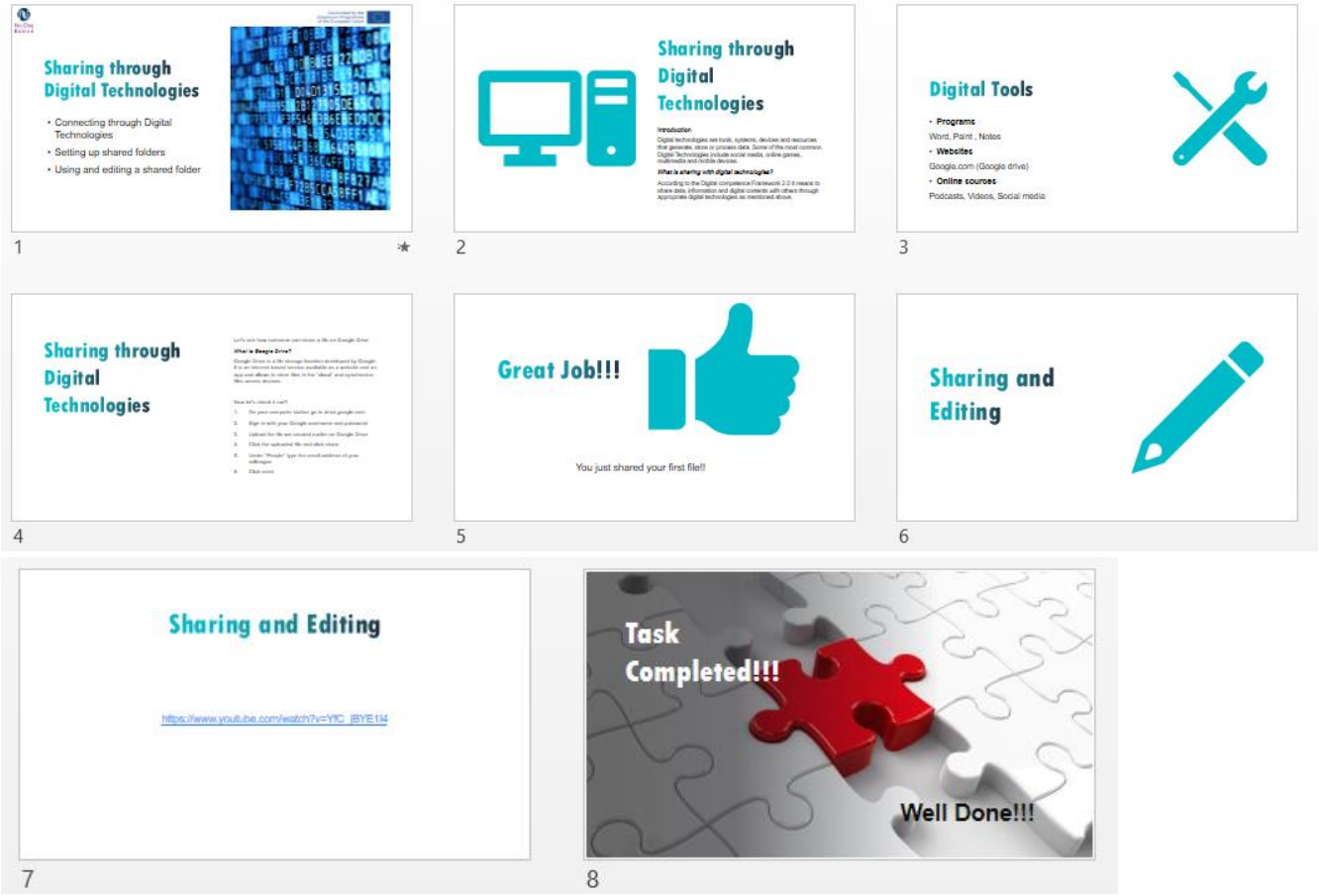
	2.5	***Netiquette*: significato, definizione e spiegazione -** https://www.youtube.com/watch?v=7-HopTAFUm0 **Esempi di cattiva *netiquette* -** https://www.cybersmile.org/what-we-do/advice-help/netiquette/examples-of-bad-netiquette **Esempi di buona *netiquette* -** https://www.cybersmile.org/advice-help/category/examples-of-good-netiquette 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	**Password: come proteggere le tue attività digitali -** https://www.funeralwise.com/learn/digitallegacy/how-to-manage-passwords/ **L'identità digitale: cos'è + perché è importante -** https://learn.g2.com/digital-identity **Cos'è l'identità digitale e come funziona -** 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
Modulo 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_are_they_What_does_progression_look_like_How_are_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/

Risorse aggiuntive – Presentazioni Power Point

Modulo 2, Unità 2.1 – Interagire attraverso le tecnologie digitali



Modulo 2, Unità 2.2 – Condividere informazioni attraverso le tecnologie digitali



Modulo 2, Unità 2.3 – Coinvolgere la cittadinanza attraverso le tecnologie digitali

Appendice II – Scheda di valutazione del Modulo 1: Informazioni e *data literacy*

Informazioni e *Data Literacy*

1.1. Navigare, ricercare e filtrare dati			
Unità di competenza	**Scarso**	**Buono**	**Ottimo**
Essere in grado di identificare diversi browser.	☐	☐	☐
Essere in grado di riconoscere diversi motori di ricerca.	☐	☐	☐
Essere in grado di cercare informazioni e contenuti online.	☐	☐	☐
Essere in grado di navigare tra gli ambienti digitali.	☐	☐	☐
Essere in grado di capire i rischi di riservatezza e privacy della ricerca su Internet.	☐	☐	☐
Essere in grado di conoscere il ruolo di Internet nell'ottenere informazioni nel contesto del mondo di oggi.	☐	☐	☐
1.2. Valutare dati, informazioni e contenuti digitali			
Unità di competenza	**Scarso**	**Buono**	**Ottimo**
Essere in grado di riconoscere i pericoli delle fake news e della disinformazione nell'era digitale.	☐	☐	☐
Essere in grado di identificare la veridicità dei dati e l'accuratezza delle informazioni digitali.	☐	☐	☐
Essere in grado di rilevare la credibilità e l'affidabilità delle fonti comuni di dati, informazioni e il loro contenuto digitale.	☐	☐	☐
Essere in grado di cercare dati e informazioni affidabili e credibili.	☐	☐	☐
1.3. Gestire dati, informazioni e contenuti digitali			
Unità di competenza	**Scarso**	**Buono**	**Ottimo**
Essere in grado di identificare diversi tipi di programmi, strumenti e ambienti per archiviare e gestire dati, informazioni e contenuti digitali.	☐	☐	☐
Essere in grado di usare strumenti e piattaforme digitali per archiviare e gestire i dati.	☐	☐	☐
Essere in grado di organizzare contenuti e dati in una piattaforma digitale in modo strutturato.	☐	☐	☐
Essere in grado di accedere ad ambienti digitali definendo adeguate impostazioni di privacy.	☐	☐	☐

Appendice III – Scheda di valutazione del Modulo 2: Comunicazione e collaborazione

Comunicazione e collaborazione

2.1. Interagire attraverso le tecnologie digitali

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di identificare diversi strumenti digitali, caratterizzarli e usarli in accordo con il contesto.	☐	☐	☐
Essere in grado di interagire e comunicare con diversi pubblici usando strumenti e dispositivi digitali adeguati.	☐	☐	☐
Essere in grado di riconoscere e caratterizzare diverse piattaforme e dispositivi digitali per la comunicazione.	☐	☐	☐
Essere in grado di cercare informazioni online in modo sicuro ed etico.	☐	☐	☐

2.2. Condividere informazioni attraverso le tecnologie digitali

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di condividere informazioni con altri usando strumenti e/o piattaforme adeguate.	☐	☐	☐
Essere in grado di riconoscere e caratterizzare diverse piattaforme e dispositivi digitali per condividere informazioni.	☐	☐	☐
Essere in grado di condividere informazioni con gli altri in modo sicuro ed etico.	☐	☐	☐
Essere in grado di cercare informazioni online in modo sicuro ed etico.	☐	☐	☐

2.3. Coinvolgere la cittadinanza attraverso le tecnologie digitali

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di comunicare online in modo etico e aperto.	☐	☐	☐
Essere in grado di partecipare online alla società come cittadino.	☐	☐	☐
Essere in grado di usare servizi online legali.	☐	☐	☐
Essere in grado di fornire feedback e opinioni con rispetto per gli altri,	☐	☐	☐
Essere in grado di riconoscere le informazioni e i servizi interattivi online.	☐	☐	☐
Essere in grado di riconoscere le informazioni e i servizi interattivi online.	☐	☐	☐

2.4. Collaborare attraverso le tecnologie digitali

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di usare diversi strumenti e piattaforme per comunicare online con gli altri.	☐	☐	☐
Essere in grado di condividere informazioni online usando strumenti e piattaforme appropriate.	☐	☐	☐
Essere in grado di identificare le piattaforme online più usate nel loro Paese o regione	☐	☐	☐
sere in grado di distinguere tra le piattaforme di messaggistica istantanea o chat, voice-over-IP, piattaforme di social media, forum ed e-mail.	☐	☐	☐

	2.5. *Netiquette*			
	Unità di competenza	**Scarso**	**Buono**	**Ottimo**
	Essere in grado di dimostrare un'interazione educata con gli altri online.	☐	☐	☐
	Essere in grado di identificare quale tipo di comportamento dovrebbe essere usato in diversi ambienti online (come e-mail, social media o chat).	☐	☐	☐
	Essere in grado di applicare le "buone maniere" in un ambiente online comunicando con gli altri.	☐	☐	☐
	Essere in grado di capire l'importanza delle regole online quando si usano le risorse digitali.	☐	☐	☐
	2.6. Gestire l'identità digitale			
	Unità di competenza	**Scarso**	**Buono**	**Ottimo**
	Essere in grado di descrivere il concetto di identità digitale.	☐	☐	☐
	Essere in grado di capire come proteggere l'identità digitale.	☐	☐	☐
	Essere in grado di descrivere semplici modi per proteggere la reputazione online.	☐	☐	☐
	Essere in grado di gestire l'impronta digitale.	☐	☐	☐
	Essere in grado di sapere come essere rispettosi delle identità digitali degli altri e attenti a ciò che si pubblica su altre persone.	☐	☐	☐

Appendice IV – Scheda di valutazione del Modulo 3: Creazione di contenuti digitali

Creazione di contenuti digitali

3.1. Sviluppare contenuti digitali

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di creare e modificare contenuti digitali in diversi formati.	☐	☐	☐
Essere in grado di creare contenuti e conoscenze nuove e originali.	☐	☐	☐
Essere in grado di rappresentare bene ciò che si intende comunicare.	☐	☐	☐
Essere in grado di identificare il valore del contenuto digitale come aiuto visivo.	☐	☐	☐
Essere in grado di adattare l'espressione attraverso la creazione dei mezzi digitali più appropriati.	☐	☐	☐

3.2. Integrare e rielaborare i contenuti digitali

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di modificare informazioni e contenuti in un documento o piattaforma esistente.	☐	☐	☐
Essere in grado di integrare nuove informazioni e contenuti in un documento o piattaforma esistente.	☐	☐	☐
Essere in grado di valutare i modi più appropriati per integrare nuovi elementi specifici di contenuto e informazione.	☐	☐	☐

3.3. Copyright e licenze

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di applicare il copyright e le licenze in modo accurato.	☐	☐	☐
Essere in grado di identificare quali licenze sono richieste in determinate circostanze.	☐	☐	☐
Essere in grado di sapere come proteggersi dalla violazione del copyright.	☐	☐	☐

3.4. Programmazione

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di elencare semplici istruzioni per un sistema informatico per risolvere un semplice problema o eseguire un compito.	☐	☐	☐
Essere in grado di risolvere semplici problemi tecnici.	☐	☐	☐
Essere in grado di applicare istruzioni per eseguire compiti o risolvere problemi.	☐	☐	☐

Appendice IV – Scheda di valutazione del Modulo 4: Sicurezza

Sicurezza

4.1. Proteggere i dispositivi

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di capire l'importanza di proteggere i dispositivi ed evitare i rischi.	☐	☐	☐
Essere in grado di identificare la differenza tra i diversi tipi di malware.	☐	☐	☐
Essere in grado di capire l'importanza delle misure relative all'affidabilità e alla riservatezza.	☐	☐	☐

4.2. Proteggere i dati personali

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di capire l'importanza delle misure relative all'affidabilità e alla riservatezza	☐	☐	☐
Essere in grado di capire il rischio di furto d'identità.	☐	☐	☐
Essere in grado di applicare la "Privacy Policy" quando si usano servizi digitali.	☐	☐	☐
Essere in grado di capire le regole di base della sicurezza.	☐	☐	☐

4.3. Proteggere la salute

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di evitare rischi per la salute e minacce al benessere fisico e psicologico mentre si usano le tecnologie digitali.	☐	☐	☐
Essere in grado di controllare i possibili pericoli e minacce negli ambienti digitali.	☐	☐	☐
Essere in grado di identificare i rischi di un uso improprio dei servizi online e digitali.	☐	☐	☐

4.4 Proteggere l'ambiente

Unità di competenza	Scarso	Buono	Ottimo
Essere in grado di identificare i rischi di un uso improprio dei servizi online e digitali.	☐	☐	☐
Essere in grado di usare i servizi digitali senza esserne dipendenti.	☐	☐	☐
Essere in grado di proteggere l'ambiente dall'impatto dello smaltimento dei dispositivi digitali.	☐	☐	☐

Appendice V – Scheda di valutazione del Modulo 5: *Problem solving*

Problem-solving				
	5.1. Risolvere problemi tecnici			
	Unità di competenza	**Scarso**	**Buono**	**Ottimo**
	Essere in grado di navigare online in contesti quotidiani.	☐	☐	☐
	Essere in grado di identificare quando un dispositivo digitale è abbastanza appropriato per lavorarci.	☐	☐	☐
	Essere in grado di identificare quando si è verificato un problema su un dispositivo o servizio digitale.	☐	☐	☐
	5.2. Individuare i fabbisogni e le risposte tecnologiche			
	Unità di competenza	**Scarso**	**Buono**	**Ottimo**
	Essere in grado di riconoscere problemi tecnici provenienti da un dispositivo digitale o dall'ambiente.	☐	☐	☐
	Essere in grado di riconoscere i metodi di risoluzione.	☐	☐	☐
	Essere in grado di capire come utilizzare gli strumenti di aiuto, le guide pratiche.	☐	☐	☐
	5.3. Utilizzare in modo creativo le tecnologie digitali			
	Unità di competenza	**Scarso**	**Buono**	**Ottimo**
	Essere in grado di usare la tecnologia digitale appropriata per uno scopo specifico (raccogliere informazioni, creare contenuti).	☐	☐	☐
	Essere in grado di usare componenti di sistemi digitali e informazioni digitali in condizioni reali.	☐	☐	☐
	5.4. Individuare i divari delle competenze digitali			
	Unità di competenza	**Scarso**	**Buono**	**Ottimo**
	Essere in grado di valutare, sé stessi o altri, per verificare che i nuovi ambienti digitali sono mezzi appropriati per migliorare il livello di competenza digitale.	☐	☐	☐
	Essere in grado di cercare opportunità di autosviluppo e di tenersi aggiornati con l'evoluzione digitale.	☐	☐	☐

Appendice VI – Valutazione della formazione

Questa scheda di valutazione ha come obiettivo principale la raccolta di dati e il tuo feedback relativi alla qualità del programma di formazione del cittadino "digitalmente competente". Il presente questionario deve essere compilato individualmente e alla fine della formazione. Il questionario è confidenziale e la tua opinione è fondamentale per il miglioramento del programma di formazione.
Il questionario è strutturato in **tre parti**: la **parte A - Statistica** ha due domande che permettono ai partner di fare un'analisi statistica dei workshop realizzati. La **parte B - Valutazione quantitativa**, è composta da 13 affermazioni, a cui rispondere utilizzando scala di gradimento da 1 a 5: 1 (fortemente in disaccordo), 2 (disaccordo), 3 (né d'accordo né in disaccordo), 4 (d'accordo) e 5 (completamente d'accordo) [22]. La **parte B - Valutazione qualitativa** è composta da due **domande aperte**: una prima in cui si dovrebbe fornire **ulteriori commenti/suggerimenti** circa le **affermazioni valutate con 1, 2 o 3** e una seconda domanda in cui è possibile aggiungere qualsiasi ulteriore commento al programma di formazione e al workshop.

Parte A: dati personali

Paese di residenza

Romania ☐ Portogallo ☐ Grecia ☐ Italia ☐ Danimarca☐

Professione

Part B: valutazione quantitativa

	1	2	3	4	5	A
Il programma di formazione è importante per la mia vita personale e/o professionale.						
La formazione corrispondeva alle mie aspettative iniziali.						
Gli obiettivi della formazione sono stati raggiunti.						
Le unità e i contenuti affrontati erano interessanti e pertinenti.						
La durata della formazione è conforme ai suoi obiettivi, contenuti e attività/progetti.						
La formazione ha permesso l'acquisizione di competenze digitali.						
I contenuti, le pratiche e/o gli strumenti presentati nella formazione erano adatti per essere migliorati nelle mie attività quotidiane.						
I materiali di supporto utilizzati durante la formazione erano adeguati (in termini di progettazione, linguaggio, utilità, informazioni fornite).						
Le attività, i compiti e gli esercizi proposti durante la formazione sono adeguati all'acquisizione e allo sviluppo/consolidamento delle competenze digitali.						
Gli educatori hanno fornito il supporto necessario durante la formazione.						
Gli educatori sono stati chiari ed efficienti durante la formazione.						
Gli educatori hanno promosso la partecipazione e il coinvolgimento dei partecipanti alla formazione.						

[22] Se una delle affermazioni non è pertinente alla tua esperienza, ti preghiamo di rispondere con “A” (*altro*).

Part C: valutazione qualitativa

1. Per favore, fornisci **ulteriori commenti/suggerimenti** circa le **affermazioni valutate con 1, 2 o 3**:

2. Hai qualche commento addizionale relativo al curriculum formative? Ti preghiamo di condividerlo qui di seguito.

Data: ___ / ____ / _____

Grazie per la collaborazione!

No One Behind

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

BIBLIOGRAFIA

No One Behind

European Commission: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en

Celebic, G. & Rendulic, D. (2011). ***Basic Concepts of Information and Communication Technology Handbook***. Open Society for Idea Exchange (ODRAZI), Zagreb. Source: http://www.itdesk.info/handbook_basic_ict_concepts.pdf

Encyclopaedia Britannica: https://www.britannica.com/technology/browser

Australian Cyber Security Centre: https://www.cyber.gov.au/acsc/view-all-content/guidance/proactive-measures-protect-your-information

Georgetown University Library: https://www.library.georgetown.edu/tutorials/research-guides/evaluating-Internet-content

Smithsonian Magazine: https://www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/?no-ist

Washington State University Vancouver: https://webliteracy.pressbooks.com/chapter/building-a-habit-by-checking-your-emotions/#footnote-51-1

The balance small business: https://www.thebalancesmb.com/copyright-definition-2948254

University, Spring Arbor. Fundamentals of Communication: 8 Basic Concepts and Definitions. *Spring Arbor University.* [Online] June 2021. https://online.arbor.edu/news/fundamentals-communication-eight-basic-concepts-and-definitions.

7 Examples of Digital Channels. **Spacey, John.** 2017, Simplicable .

The 10 new paradigms of communication in the digital age. **Orihuela, Jose Luis.** 2017, Jlori.

4 *Types of Communication Styles.* **Alvernia University.** Pennsylvania : s.n., 2018, Alvernia University, p. 2.

LEADGENERA. LEADGENERA. *Content Marketing.* [Online] June 2021. https://leadgenera.com/knowledge-hub/marketing/the-10-best-social-media-and-content-apps-for-2020/.

Commision, European. The Digital Competence Framework 2.0. *EU SCIENCE HUB.* [Online] January 9th, 2019. https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework.

Care, Department of Health and Social. Engage. *Digital passport.* [Online] https://engage.dhsc.gov.uk/digitalpassport/tools/.

Google. Google. *Google Drive.* [Online] Google. https://support.google.com/drive/answer/2424384?hl=en&co=GENIE.Platform%3DDesktop.

European Commission. Europa. *Digital Citizenship Transformation.* [Online] European Commision. https://epale.ec.europa.eu/en/blog/digital-citizenship-transformation.

Common Sense. *Everything You Need to Teach Digital Citizenship.* [website] s.l. : Common Sense, 2021.

Australian Government. eSafety Commisioner . *Digital Citizens Guide.* [Online] https://www.esafety.gov.au/media/2563.

Liveworkstudio. live|work. *Digital Relationships.* [Online] https://www.liveworkstudio.com/themes/organisational-change/digital-relationships/.

Eferin, Kate Gromova and Yaroslav. World Bank Blogs. *Ethics in the digital world: Where we are now and what's next.* [Online] April 9th, 2021. https://blogs.worldbank.org/opendata/ethics-digital-world-where-we-are-now-and-whats-next.

Zwerdling, Daniel. npr. *Your Digital Trail, And How It Can Be Used Against You.* [Online] 2013. https://www.npr.org/sections/alltechconsidered/2013/09/30/226835934/your-digital-trail-and-how-it-can-be-used-against-you.

The University of Alabama at Birmingham. UAB Institute for Human Rights Blog. *Digital Citizenship: The Good, The Bad, & The Role of the Internet.* [Online] January 2019. https://sites.uab.edu/humanrights/2019/01/18/digital-citizenship-the-good-the-bad-the-role-of-the-

BYU Library:

- https://guides.lib.byu.edu/c.php?g=216340&p=1428402
- https://www.techwalla.com/articles/why-is-a-file-extension-important
- https://slidetodoc.com/solving-technical-problems-identifying-needs-and-technological-responses/
- https://www.mcafee.com/blogs/consumer/consumer-threat-reports/software-updates-important/
- https://www.opencolleges.edu.au/informed/features/8-ways-boost-creativity-technology/

No One Behind

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

Il presente progetto è finanziato con il sostegno della Commissione Europea. L'autore è il solo responsabile di questa pubblicazione e la Commissione declina ogni responsabilità sull'uso che potrà essere fatto delle informazioni in essa contenute.

Progetto n. º 2020-1-RO01-KA204-079988