

iAware

GUIDA METODOLOGICA CON ISTRUZIONI DEL TRAINER



Erasmus+



UNIVERSIDADE
LUSÓFONA





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

Questa pubblicazione è stata finanziata con il sostegno del
Commissione Europea. Riflette solo le opinioni degli autori, e la
Commissione non può essere ritenuta responsabile per qualsiasi
utilizzo che può essere fatto delle informazioni in esso contenute.

Numero convenzione di sovvenzione: 2019-1-PL01-KA204-065601

Autori:

Piotr Celiński

Euro-Forum

Paulo Ferreira

Universidade Lusófona

Zbigniew Husak

Euro-Forum

Simone Indovina

PRISM Impresa Sociale s.r.l.

Katarzyna Kopec

Euro-Forum

Beniamino Torregrossa

PRISM Impresa Sociale s.r.l.

Lublin, Poland, 2022

Euro-Forum Agnieszka Gudków, Marek Gudków Spółka Jawna



[This publication is licenced under a
Creative Commons Attribution 4.0
International Licence.](https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUZIONE.....1

CAPITOLO 1 - PROBLEMI DERIVANTI DALL'INSEGNAMENTO DELLE TIC AD ADULTI CON SCARSE COMPETENZE E MODI PER AFFRONTARLI.....4

Problemi legati alla mancanza di conoscenze e di motivazione
nell'utilizzo delle risorse TIC 6

Problemi legati alla mancanza di accesso e di utilizzo delle TIC 8

Problemi derivanti dalla mancanza di competenze di base per
utilizzare efficacemente gli strumenti TIC 10

CAPITOLO 2 - BUONE PRATICHE NELL'INSEGNAMENTO DELLE TIC AGLI ADULTI.....11

Educazione digitale degli adulti: formale o informale? 13

Finanziamento dell'educazione degli adulti 15

Gli adulti sono pronti a migliorare le loro competenze? 16

Le iniziative di apprendimento digitale più diffuse e di successo nei
Paesi partner del progetto 'iAware' 18

CAPITOLO 3 - METODI E STRUMENTI SVILUPPATI NELL'AMBITO DEL PROGETTO IAWARE 23

Metodi di insegnamento 25

Metodi di attivazione a sostegno dell'educazione degli adulti nel
progetto 'iAware' 27

Strumenti didattici: materiali multimediali e piattaforma 'iAware' .. 30

CAPITOLO 4 - PROGRAMMA 'IAWARE' 32

Presupposti, obiettivi e risultati del programma	33
Struttura del programma	35
Modulo 1 - Tipi e identificazione delle minacce online.....	37
Lezione 1 - Spam e truffe	38
Lezione 2 - Phishing	48
Lezione 3 - Privacy online.....	64
Lezione 4 - Impronta digitale	74
Modulo 2 - Contrastare e minimizzare i rischi e garantire la sicurezza della rete.....	83
Lezione 1 - Come proteggersi efficacemente da messaggi di spam e truffa e da siti web falsi	84
Lezione 2 - come riconoscere efficacemente i messaggi di phishing? Come proteggersi dal phishing.....	95
Lezione 3 - Come prendersi cura in modo efficace della propria privacy e dei propri dati quando si utilizza internet	104
Lezione 4 - Come proteggersi efficacemente quando si usa internet ..	113
Modulo 3 - Partecipazione attiva alla società dell'informazione.....	122
Lezione 1 - Identità digitale e media mobili	123
Lezione 2 - Remix - il multimediale libero nella vita quotidiana.....	133
Lezione 3 - Impegnarsi nella cittadinanza attraverso le tecnologie digitali.....	140
Lezione 4 - Giornalismo Civico. Condividere storie nel mondo digitale	145
Modulo 4 - Uso consapevole delle tecnologie dell'informazione e della comunicazione.....	151
Lezione 1 - Fake news	152
Lezione 2 - Alfabetizzazione mediatica: come riconoscere le fake news?	158
Lezione 3 - Disinformazione e cattiva informazione	163
Lezione 4 - Uso consapevole delle TIC.....	167

Modulo 5 - Direzioni per lo sviluppo di Internet, costruzione attiva di una comunità globale di e-cittadini	174
Lezione 1 - Passato, presente e futuro di Internet	175
Lezione 2 - IoT - Internet of Things	182
Lezione 3 - AI, Big Data e Cloud	191
Lezione 4 - Cittadinanza elettronica	198

CAPITOLO 5 - STRUMENTI PER LA VALUTAZIONE DEI LIVELLI DI COMPETENZA ICT 205

ICT	206
DigComp	207
Panoramica delle certificazioni ICT	210
Strumenti di valutazione e autovalutazione	213

LA BIBLIOGRAFIA216

The background features a light blue and white color scheme. It is decorated with a pattern of binary code (0s and 1s) scattered across the surface. In the top-left corner, there are concentric circular patterns in shades of purple and pink, some solid and some dashed. In the bottom-right corner, there are similar concentric circular patterns in shades of blue and teal, also with solid and dashed lines. Hexagonal shapes are visible in the corners, some filled with color and others as outlines.

INTRODUZIONE

La vita nella società moderna, lo sviluppo personale, così come l'intraprendere un'attività professionale, richiedono che un individuo possieda alcune competenze di base che gli permettano di agire efficacemente in condizioni specifiche. L'analisi di queste competenze ritenute necessarie ha portato allo sviluppo di un elenco di competenze chiave acquisite attraverso percorsi di apprendimento permanente. Nelle Raccomandazioni del Consiglio del 22 maggio 2018, il Parlamento Europeo elenca le competenze digitali tra le otto competenze chiave la cui importanza sta aumentando non solo a causa dello sviluppo molto dinamico della tecnologia, ma anche per l'esperienza acquisita durante la pandemia COVID-19.

La competenza digitale, che implica l'uso critico e responsabile delle nuove tecnologie, è stata riconosciuta dal Parlamento europeo come una delle competenze chiave per l'apprendimento permanente e implica l'uso critico e responsabile delle nuove tecnologie. La definizione del termine "competenza digitale" non è semplice e non può essere dettagliata perché il mondo digitale è in continua evoluzione. Le competenze digitali non sono un insieme di abilità per l'uso efficace di computer, dispositivi mobili o Internet, né si riferiscono a soluzioni o strumenti specifici, poiché la velocità del cambiamento nella sfera tecnologica li renderebbe obsoleti molto rapidamente. Inoltre, le competenze digitali non si limitano alle sole competenze hardware, ma comprendono anche le competenze informative, la capacità di accedere alle informazioni, di utilizzarle e di sviluppare le proprie conoscenze con l'aiuto delle TIC. Queste competenze facilitano un ulteriore sviluppo continuo e, in questo modo, anche l'adattamento ai requisiti propri delle società moderne.

Si può affermare che nel XXI secolo le competenze digitali sono importanti quanto l'alfabetizzazione, le competenze matematiche e quelle linguistiche. Sono collegate a molte delle competenze che i cittadini dell'Europa moderna dovrebbero possedere e influenzano direttamente l'acquisizione di altre competenze chiave, come la comunicazione nella lingua madre e nelle lingue straniere, la capacità di apprendere e le competenze sociali e civiche. L'alfabetizzazione digitale ha un impatto in settori quali la qualità della vita, l'economia, l'assistenza sanitaria, l'istruzione, la scienza, la sicurezza, l'agricoltura, la cultura, l'intrattenimento e la partecipazione alla società.

In questo e-book vogliamo includere un programma di formazione completo sviluppato nell'ambito del progetto Erasmus+ "iAware - Programma innovativo per l'educazione digitale degli adulti". Il progetto è stato realizzato da tre organizzazioni partner di tre diversi Paesi europei. "EURO-FORUM" dalla Polonia era il leader del progetto e "Prism" dall'Italia e l'Università Lusofona dal Portogallo erano le organizzazioni partner. Il progetto è una risposta al problema delle

insufficienza delle competenze digitali degli adulti, rilevato congiuntamente da queste organizzazioni. Gli obiettivi del progetto comprendono:

- *la creazione di un programma moderno di TIC e di formazione degli adulti che tenga conto delle sfide attuali in termini di sicurezza di Internet e di uso consapevole delle risorse online*
- *fornire gli strumenti, le risorse di conoscenza e le competenze giuste ai formatori TIC e agli educatori per adulti, al fine di formare gli atteggiamenti degli adulti verso l'uso consapevole delle moderne tecnologie*
- *il miglioramento delle competenze digitali chiave degli adulti nell'Unione Europea e lo sviluppo della società dell'informazione*

Il programma presentato nei capitoli seguenti è creato nell'ambito del progetto "iAware" è suddiviso in cinque moduli tematici:

1. *Tipi e identificazione delle minacce in Internet.*
2. *Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete.*
3. *Partecipazione attiva alla società dell'informazione.*
4. *Uso consapevole delle tecnologie dell'informazione e della comunicazione.*
5. *Indicazioni per lo sviluppo di Internet, costruzione attiva di una comunità globale di e-cittadini.*

L'e-book è destinato ai formatori e agli educatori che lavorano con gli adulti come risorsa di supporto e compendio per l'uso del metodo innovativo sviluppato nell'ambito del progetto. I capitoli seguenti aiuteranno i formatori a prepararsi in modo completo per il loro lavoro sulla base dei piani di lezione sviluppati nel progetto "iAware".



CAPITOLO 1

**PROBLEMI DERIVANTI DALL'INSEGNAMENTO
DELLE TIC AD ADULTI CON SCARSE
COMPETENZE E MODI PER AFFRONTARLI**

Il livello di competenza digitale e la qualità dell'uso di strumenti digitali è un aspetto fondamentale della vita nella società del XXI secolo, che ha implicazioni sia a livello generale, con effetti sul mercato del lavoro o sullo sviluppo economico, influenzando l'azione civica e il funzionamento delle istituzioni pubbliche, sia a livello molto specifico, con effetti sulla qualità della vita dei singoli cittadini dell'UE. Tuttavia, gli indubbi vantaggi dello sviluppo tecnologico sono accompagnati da nuove criticità. L'uso diffuso delle tecnologie, le crescenti possibilità e, spesso, anche la loro indispensabilità nella vita di tutti i giorni fanno sì che le persone che non riescono a usarle, o che hanno un basso livello di competenze, siano sempre più escluse socialmente. Diventa importante avere le giuste competenze per utilizzare la tecnologia a proprio vantaggio.

Aumentare il livello di competenza digitale tra gli adulti è stata una sfida posta ai formatori che lavorano con il metodo del progetto "iAware". Le barriere legate all'uso del computer e di Internet possono essere molto diverse; tra queste, i fattori tecnologici legati alla mancanza di possibilità tecniche per connettersi a Internet, o finanziari, e fattori psicologici legati alla mancanza di conoscenza, motivazione e competenze adeguate all'uso.

I problemi che possono influire sull'insegnamento a soggetti scarsamente qualificati possono essere suddivisi in tre aree:

1. *Problemi legati alla mancanza di conoscenza e di motivazione all'uso delle risorse TIC.*
2. *Problemi legati alla mancanza di accesso e di opportunità di utilizzo delle TIC.*
3. *Problemi derivanti dalla mancanza di competenze di base per un uso efficace degli strumenti TIC.*

Le barriere all'uso delle TIC sopra individuate sono interconnesse e molto spesso si presentano contemporaneamente.

PROBLEMI LEGATI ALLA MANCANZA DI CONOSCENZE E DI MOTIVAZIONE NELL'UTILIZZO DELLE RISORSE TIC

Avere la giusta motivazione per utilizzare le nuove tecnologie è fondamentale. La motivazione è ciò che determina la decisione di acquistare un computer o uno smartphone, di connettersi a Internet e di acquisire le competenze necessarie per utilizzare le applicazioni. La motivazione è fondamentale anche per l'utilizzo delle soluzioni TIC. Avere accesso a computer e reti a casa, al lavoro, a scuola, ma anche usarli, è un'altra questione, perché l'accesso non sottintende necessariamente l'utilizzo.

Questo fenomeno è legato alla mancanza di motivazione all'uso delle soluzioni TIC. Una certa percentuale della popolazione non usa Internet, i computer o i dispositivi mobili perché non ne sente assolutamente la necessità. Ci sono categorie di persone, inclusi coloro che sono alfabetizzati digitalmente, che tuttavia ne rifiutano l'utilizzo. Ciò è legato a una mancanza di motivazione in seguito ad una scarsa conoscenza di ciò per cui Internet può essere utilizzato, nonché alla capacità di utilizzarlo e alla possibilità di utilizzarlo da parte, ad esempio, dei familiari che possono cercare informazioni su Internet per il non-utente. Sebbene il problema riguardi persone di tutte le età, sono più spesso gli anziani ad esserne colpiti, il che è spesso legato alla percezione che le nuove tecnologie siano solo per i giovani e che l'idea dell'apprendimento permanente sia vista come innaturale. È stato riscontrato che le persone più anziane fanno un uso minore delle tecnologie digitali, in particolare di Internet. Ciò è dovuto al fatto che le tecnologie digitali sono in circolazione da poco tempo e, in quanto novità, sono poco familiari a questo gruppo di persone e quindi meno accessibili. Per le generazioni che hanno frequentato corsi di informatica a scuola fin dalla più tenera età, utilizzare i vantaggi di Internet è naturale e ulteriori funzionalità come lo shopping online o la messaggistica istantanea sono accolte con entusiasmo. Questo non è altrettanto evidente per i cittadini più anziani.

L'accesso a Internet da solo non garantisce che le persone lo utilizzino. L'aspetto fondamentale, tuttavia, non è la mancanza di volontà di utilizzo in sé, ma piuttosto le ragioni di tale riluttanza. Sono queste le vere barriere all'adozione del digitale. Alla base c'è il problema della mancanza di conoscenza, che è all'origine di altre barriere e porta alla mancanza di necessità di usare Internet, nonché a barriere psicologiche, tra cui la paura e l'autoesclusione per mancanza di motivazione all'apprendimento. Il problema della mancanza di conoscenze non riguarda solo l'ignoranza delle possibilità offerte da computer, smartphone e Internet. Si tratta anche di una mancanza di informazioni affidabili, che porta a una mancanza di fiducia, ad esempio, nell'online banking o nelle informazioni fornite via Internet. La mancanza di conoscenze è anche legata alla difficoltà di trovare argomenti e attività di interesse per una persona che fa una ricerca online, la cui acquisizione sarebbe una motivazione per apprendere nuove competenze. Di conseguenza, la mancata percezione di Internet e del computer come strumenti per soddisfare i propri bisogni diventa un problema fondamentale. Una forma di lotta alla barriera principale - l'esclusione motivazionale - consiste nel costruire la necessità di utilizzare Internet intorno a motivazioni di vita, lavorative, sociali o di società più ampie. Un modo per contrastarla è la partecipazione di queste persone a corsi o workshop organizzati da varie organizzazioni e rivolti a un pubblico specifico.

Una barriera significativa legata all'inizio dell'utilizzo delle tecnologie digitali è la percezione di queste nuove tecnologie come un mondo a cui non si appartiene. Ciò è spesso dovuto a un atteggiamento passivo e alla mancanza di volontà di imparare cose nuove. Esistono anche barriere legate alla paura, all'apprensione e a varie idee sbagliate associate all'uso del computer, come ad esempio la dipendenza da computer, da truffatori o malware, o la mancanza di fiducia nella capacità di mantenere contatti sociali su Internet. Un altro problema che si traduce in una mancanza di motivazione si manifesta nella mancanza di contenuti e di servizi diversi che possano essere di interesse per gruppi specifici. Il superamento di queste barriere è legato alle azioni dei fornitori di contenuti. Non si tratta solo di azioni di aziende commerciali, ma anche di enti governativi, ad esempio per adattare i contenuti e i moduli alle persone con disabilità. Tanto più che oggi l'accesso a Internet non è solo una comodità, ma a volte persino una necessità per partecipare pienamente alla vita sociale o professionale.

PROBLEMI LEGATI ALLA MANCANZA DI ACCESSO E DI UTILIZZO DELLE TIC

I problemi legati alla mancanza di accesso includono barriere finanziarie, di connessione alla rete e hardware. Le barriere finanziarie sono principalmente legate alla mancanza di attrezzature adeguate in casa e alla mancanza di una connessione a Internet a causa dei prezzi eccessivi. Un'altra barriera legata alla mancanza di accesso è la mancanza di fattibilità tecnica della fornitura di Internet. Questo vale soprattutto per i residenti delle città più piccole, dove a volte non ci sono fondi sufficienti per l'acquisto di attrezzature informatiche ed è vano trovare soluzioni tecniche moderne che permettano di utilizzare tutte le possibilità di Internet.

Tuttavia, negli ultimi tempi, questi problemi stanno perdendo importanza. Ciò è dovuto principalmente allo sviluppo delle infrastrutture e all'introduzione di tecnologie sempre più moderne, come Internet mobile. La qualità dell'accesso a Internet - larghezza di banda e affidabilità della connessione - sta diventando sempre più importante. L'attivazione digitale non può limitarsi a ridurre i costi di accesso e a creare infrastrutture; i Paesi devono assicurarsi che tutti gli utenti abbiano pari accesso. È essenziale sensibilizzare continuamente il pubblico sui vantaggi dell'uso delle TIC e sugli sforzi di attivazione delle comunità locali. Per molte persone, il semplice fatto di avere accesso alle TIC non significa che saranno utenti attivi. È necessario promuovere la giusta motivazione in questi individui e aiutarli ad aumentare il loro livello di competenza.

Un altro problema nell'utilizzo di Internet è legato alle limitazioni hardware, che possono essere intese come la mancata corrispondenza tra hardware, software e le capacità degli utenti. Questo è particolarmente vero per gli anziani e le persone con disabilità. Con lo sviluppo del mercato, si osserva un aumento della disponibilità di tecnologie più intuitive, adattate a gruppi di utenti specifici, ad esempio una spaziatura appropriata tra i tasti della tastiera, l'adattamento della

risoluzione dello schermo, la dimensione dei caratteri, il design e la complessità delle interfacce utente o la scelta di uno smartphone appropriato. L'adattamento dei contenuti web, ad esempio dei siti web per consentire l'accesso agli utenti più anziani o con diverse disabilità, sta contrastando questo problema. I contenuti resi disponibili sul web devono essere appropriati, utili e accessibili a gruppi specifici.

PROBLEMI DERIVANTI DALLA MANCANZA DI COMPETENZE DI BASE PER UTILIZZARE EFFICACEMENTE GLI STRUMENTI TIC

Per alcune persone che non sono in grado di utilizzare le moderne tecnologie digitali, la mancanza di competenze adeguate, ma anche la difficoltà di acquisire nuove abilità, è un fattore limitante per iniziare a utilizzare Internet. Anche le attività di base legate al computer, come l'accensione, la digitazione, l'uso del mouse, la navigazione di siti web o l'utilizzo di un motore di ricerca, possono risultare chiaramente difficili. Allo stesso tempo, spesso non sono sufficientemente motivati ad acquisire nuove competenze. Anche una curva di apprendimento più lenta o la necessità di un supporto da parte di una persona più esperta e competente per svolgere varie attività, ad esempio installare applicazioni, effettuare registrazioni, imparare a usare il software, possono costituire una barriera.

Quando si presentano esigenze legate all'uso di Internet o del computer, queste vengono ridotte (ad esempio, l'abbandono di eventi per i quali è necessario iscriversi online) o soddisfatte da altri. Le barriere di competenza sono spesso legate alla mancanza di fiducia nelle proprie capacità, alla paura e, soprattutto, alla difficoltà di identificare i bisogni che possono essere soddisfatti utilizzando Internet. È fondamentale incoraggiare le persone con scarse competenze a partecipare a corsi di formazione e workshop organizzati da diverse istituzioni o ad acquisire autonomamente le conoscenze.



CAPITOLO 2

BUONE PRATICHE NELL'INSEGNAMENTO DELLE TIC AGLI ADULTI

Oggigiorno, la dinamica del cambiamento può essere valutata, non solo riguardo la dimensione tecnologica ed economica, ma anche relativamente a quella Sociale. L'apprendimento permanente sta assumendo una dimensione speciale, che ci permette di operare più facilmente nella realtà circostante, in continua evoluzione. L'apprendimento non è più solo un'attività volontaria intrapresa da pochi individui per soddisfare le proprie ambizioni, i propri interessi e le proprie esigenze di sviluppo personale, ma una necessità per il corretto funzionamento della vita sociale e del mercato del lavoro.

I benefici più evidenti dell'istruzione comprendono le conoscenze e le abilità che un individuo acquisisce nel corso del processo di apprendimento, soprattutto quando derivano dalla motivazione e dalle esigenze dell'individuo stesso. Il gap di competenze è un motivo altrettanto determinante nell'acquisizione di nuove competenze. Si riferisce a uno stato in cui una persona sente chiaramente la mancanza di una determinata abilità. Attraverso varie attività di sviluppo, il gap viene colmato e le nuove competenze aprono nuove possibilità. Lo sviluppo continuo delle competenze ha un impatto anche sulla sfera mentale. L'impegno volontario nel processo di apprendimento, in particolare la regolarità e la costanza nell'azione, rafforzano il senso di autorevolezza e di influenza di una persona. Approfondire un argomento interessante e stimolante contribuisce a creare un senso di soddisfazione e ad aumentare la motivazione all'apprendimento. Si rafforza, così, anche l'autostima e aumenta la fiducia in se stessi.

EDUCAZIONE DIGITALE DEGLI ADULTI: FORMALE O INFORMALE?

Quando si parla di "educazione degli adulti", è possibile fare riferimento a due macro significati. Da un lato, è l'insieme dei processi di apprendimento - formali e informali - che integrano o ampliano l'istruzione acquisita a scuola. Dall'altro, è l'educazione pratica in senso lato, che consente agli adulti di sviluppare le proprie competenze, acquisire conoscenze, migliorare le proprie qualifiche professionali o arricchire la propria vita personale.

In ciascuno dei tre Paesi partner, con "educazione degli adulti" si fa riferimento ad una serie di attività finalizzate all'arricchimento culturale, alla mobilità professionale e all'ampliamento delle qualifiche professionali. Queste attività possono essere organizzate dalla scuola in collaborazione con le comunità locali, coinvolgendo anche il mercato del lavoro e le parti sociali a livello territoriale; possono essere utilizzate per estendere o integrare l'istruzione impartita durante la scuola dell'obbligo o per sostituire l'istruzione obbligatoria per chi ha abbandonato la scuola. Queste attività possono semplicemente mirare ad arricchire la cultura personale per fornire o portare a un titolo accademico.

Per istruzione formale si intende l'istruzione nel sistema scolastico, fornita da varie scuole pubbliche e non pubbliche e da istituzioni educative autorizzate all'insegnamento. Tale istruzione segue curricula approvati e si basa sugli standard adottati nel sistema educativo approvato dalle normative nazionali applicabili. Porta a una qualifica confermata da un certificato, un attestato o un diploma. L'educazione informale è un apprendimento autogestito con l'obiettivo di acquisire conoscenze o migliorare le competenze, che si svolge al di fuori delle forme organizzate di istruzione scolastica ed extrascolastica e dovrebbe poter avvenire senza la partecipazione di un insegnante. Un altro tipo di educazione che si può distinguere è l'educazione non formale. Si tratta di attività di apprendimento organizzate che non corrispondono alla definizione di educazione scolastica. Una

caratteristica dell'educazione non formale è che non porta a un cambiamento del livello di istruzione, ma porta all'acquisizione e all'ampliamento di competenze in vari ambiti della vita professionale, sociale o culturale. A differenza dell'educazione informale, l'educazione non formale deve svolgersi con un docente, un istruttore o un insegnante.

La grande maggioranza degli adulti sceglie istituzioni e forme di apprendimento non formali se desidera ampliare le proprie conoscenze, acquisire nuove abilità o competenze. Partecipano a vari tipi di corsi e formazioni di propria iniziativa o costretti dai cambiamenti del mercato del lavoro, e questa forma di istruzione li aiuta a riqualificarsi, svilupparsi o adattarsi in una determinata professione.

In diversi Paesi, le istituzioni statali hanno riconosciuto il problema del livello di competenze digitali degli adulti e stanno producendo documenti per aiutare a gestire l'alta percentuale di persone poco qualificate. Un esempio è l'Italia, dove è stato annunciato un piano strategico nazionale sulle competenze ICT degli adulti per il 2020. Il piano mira a migliorare il coordinamento tra i diversi enti e processi legati all'apprendimento permanente, al fine di stabilire congiuntamente strategie di formazione nazionale per il periodo 2020-2022, per garantire l'integrazione e il reinserimento nel mercato del lavoro. L'Italia si colloca al 25° posto su 28 Stati membri dell'UE nell'Indice dell'economia e della società digitali 2020 della Commissione europea. Il livello di competenze digitali varia notevolmente tra gli occupati nelle diverse attività economiche. Le competenze digitali sono più diffuse nel settore dei servizi, seguito dalla pubblica amministrazione, e meno diffuse nei settori industriale e primario. Ciò può inibire l'innovazione e l'inclusione nella società e nel mercato del lavoro.

FINANZIAMENTO DELL'EDUCAZIONE DEGLI ADULTI

Si possono distinguere tre fonti di finanziamento per tutte le forme di educazione degli adulti: la prima è costituita dai fondi provenienti dal bilancio statale e distribuiti da varie istituzioni statali. In Polonia, ad esempio, tra le istituzioni coinvolte nell'educazione non formale c'è il Fondo nazionale per la formazione, che consente di cofinanziare la formazione dei lavoratori e dei datori di lavoro in diverse organizzazioni di formazione, sia statali che private. L'obiettivo di questo fondo è evitare che i dipendenti perdano il lavoro a causa di competenze inadeguate ai requisiti di un'economia in continua evoluzione.

Un'altra fonte di finanziamento è rappresentata dal sostegno finanziario della Commissione europea, che mette a disposizione fondi per vari progetti e attività dell'organizzazione. Il sostegno finanziario nel campo dell'istruzione e della formazione può essere ottenuto, tra l'altro, dal programma ERASMUS+. Si tratta di un programma di finanziamento che sostiene attività nei settori dell'istruzione, della formazione, della gioventù e dello sport. La Commissione europea è responsabile delle strategie del programma e della supervisione della sua attuazione. È dal programma ERASMUS+ che viene attuato il progetto "iAware". Il Fondo Sociale Europeo costituisce un altro esempio di programma di questo tipo, attraverso il quale l'Unione Europea sostiene lo sviluppo socio-economico di tutti gli Stati membri e le sue risorse vengono investite nelle persone, in particolare in quelle che faticano a trovare lavoro.

Una terza fonte di finanziamento per la formazione è costituita dalle risorse finanziarie dei tirocinanti o dei datori di lavoro.

GLI ADULTI SONO PRONTI A MIGLIORARE LE LORO COMPETENZE?

Come mostrano i risultati dell'Indagine sull'istruzione degli adulti (Eurostat, 2016), in media nell'Unione europea il 47,2% degli adulti di età compresa tra i 25 e i 64 anni nell'anno precedente l'indagine era impegnato nell'apprendimento formale e non formale legato al lavoro. Paesi come l'Austria, i Paesi Bassi e la Svezia, dove almeno il 60% degli adulti era impegnato nell'apprendimento, si collocano al di sopra della media. Alcune caratteristiche dell'educazione degli adulti sono comuni a tutti i Paesi dell'Unione Europea. I giovani sono più disposti a ricevere un'istruzione, mentre con l'avanzare dell'età diminuisce la loro partecipazione a varie forme di istruzione. Si può anche trovare una relazione tra il livello di istruzione iniziale e la disponibilità a sviluppare le proprie competenze. Chi ha un livello di istruzione più elevato è più propenso a partecipare a vari corsi e formazioni.

L'aumento delle competenze ICT consiste nell'imparare a conoscere e a trarre vantaggio dalle nuove opportunità tecnologiche. Le qualifiche digitali significano acquisire esperienza diretta con strumenti, macchine o software. Si tratta anche di una comprensione teorica di come le nuove tecnologie possono essere utilizzate nella vita personale e professionale. I benefici del miglioramento delle competenze sono sia per le singole persone che per l'ambiente socio-economico in cui operano. Dal punto di vista individuale, il miglioramento delle competenze è un investimento nello sviluppo personale, ma anche nell'aumento del proprio valore sul mercato del lavoro.

Gli adulti imparano in modo diverso dai giovani. Spesso prendono decisioni educative basate su esperienze precedenti, quindi le conoscenze e le competenze che cercano di acquisire devono essere tradotte in una successiva applicazione pratica. I fattori che motivano gli adulti a partecipare a corsi di formazione e formazione includono il desiderio di migliorare le proprie competenze professionali,

che può essere finalizzato a ottenere una promozione o a migliorare i propri guadagni, il desiderio di migliorare le proprie abilità, la non volontà di rimanere indietro rispetto alle tecnologie in via di sviluppo e la necessità di utilizzare vari strumenti digitali per partecipare alla vita sociale e culturale. Le ragioni che scoraggiano le persone dal cogliere le opportunità di sviluppo comprendono la mancanza di tempo, l'insufficienza di risorse finanziarie e la mancanza di fiducia nella partecipazione a corsi e formazioni, nonché la scarsa conoscenza dell'offerta sul mercato dell'apprendimento, che rende impossibile pianificare attività adeguate.

LE INIZIATIVE DI APPRENDIMENTO DIGITALE PIÙ DIFFUSE E DI SUCCESSO NEI PAESI PARTNER DEL PROGETTO 'IAWARE'

IL PROGETTO DIGINV - Italia

Il progetto sviluppa la metodologia Digital Invasion, ideata in Italia. La metodologia migliora le competenze digitali e comunicative degli operatori culturali, aiutandoli a diventare promotori e a coinvolgere i cittadini nella valorizzazione del patrimonio culturale. Inoltre, lavora per migliorare le competenze digitali dei cittadini coinvolti (dai più giovani agli anziani) utilizzando le nuove tecnologie per promuovere i siti di interesse culturale. Si prevedono due diversi risultati. Da un lato, le invasioni digitali stesse consentiranno ai partecipanti di apprendere i concetti di base della comunicazione digitale, riducendo il divario di alfabetizzazione digitale tra i partecipanti. Le Digital Invasion applicheranno i principi della digitalizzazione dei sistemi produttivi, della narrazione digitale e del marketing online per promuovere il patrimonio culturale e renderlo più accessibile e competitivo a livello locale e internazionale, valorizzando il patrimonio culturale materiale e immateriale e lo sviluppo dei partecipanti in un modo completamente nuovo. Le invasioni digitali sono titolari di buone pratiche e del know-how strategico necessario per il loro trasferimento agli operatori e all'estero. D'altro canto, gli operatori e le organizzazioni partner otterranno nuovi strumenti per coinvolgere le comunità nell'arricchimento del patrimonio culturale e per consolidare il dialogo con le autorità locali. Questo dialogo rafforzerà la linea d'azione comune a livello europeo che sarà definita per coinvolgere i cittadini nella promozione del patrimonio culturale.

https://www.digitalinvasions.eu/?fbclid=IwAR1qEjgEMGxhuQ0_eFXWJORG855kmlATQL6DycyJo7WkorF_lizPvTW2KRQ

LA SCUOLA CON ME - Italia

Il progetto inizia a La Spezia (Italia) presso il locale Centro per l'Istruzione degli Adulti (CPIA). Il risultato finale è presentato su un sito web in continuo sviluppo, che contiene materiali disponibili gratuitamente per chiunque voglia

insegnare o imparare l'italiano come lingua straniera o seconda. Il blog raccoglie letture, video, canzoni, link a numerosi strumenti e attività: esercizi divisi per livello, dizionari online, un coniugatore di verbi e molto altro. Dal punto di vista educativo, grazie al metodo audiovisivo possiamo ottenere una maggiore attenzione e un maggiore coinvolgimento degli studenti, che possono lavorare insieme alla stessa attività. Dal punto di vista economico ed ecologico, possiamo risparmiare sulle fotocopie e sulla carta in generale. Inoltre, dopo le lezioni, gli studenti possono esercitarsi quando e dove vogliono, seguendo i suggerimenti dell'insegnante o semplicemente i propri interessi e lavorando su qualsiasi dispositivo, compreso lo smartphone. Inoltre, c'è la possibilità di lasciare un commento sul blog o di seguire le loro attività attraverso la pagina Facebook recentemente creata.

<http://lascuolaconme.altervista.org>

<https://epale.ec.europa.eu/en/content/la-scuola-con-me-site-teaching-and-learning-italian>

IDEAL - Integrazione della formazione digitale nell'alfabetizzazione degli adulti - Italia

Il principale obiettivo generale del progetto IDEAL è stato quello di fornire orientamento e formazione agli insegnanti di adulti in tutta Europa sull'uso degli strumenti TIC e dei metodi digitali per migliorare l'insegnamento delle competenze di base. Ciò è stato fatto attraverso un approccio integrato alla raccolta, alla condivisione e alla diffusione di pratiche di insegnamento e apprendimento innovative e inclusive che utilizzano strumenti TIC e metodi digitali. Il progetto prevedeva tre tipi di attività principali: lo sviluppo di quattro prodotti intellettuali per fornire orientamento e formazione agli educatori per adulti e per condividere il know-how educativo esistente delle organizzazioni partner; l'organizzazione di due workshop educativi di 5 giorni in Finlandia e in Italia; e l'organizzazione di due eventi di divulgazione in Finlandia e in Italia. Durante e dopo il progetto, l'équipe del progetto e tutti i partner individualmente hanno svolto attività di comunicazione e divulgazione. Hanno inoltre istituito un efficace sistema di valutazione per garantire un adeguato monitoraggio e una valutazione della gestione e dei risultati del progetto. I risultati intellettuali sviluppati nell'ambito del progetto comprendono un kit di strumenti online con analisi del contesto e dei bisogni, linee guida sulle buone pratiche e video tutorial. Tutti i risultati intellettuali sono disponibili online sul sito www.erasmusideal.com e saranno integrati nei programmi di studio delle organizzazioni partner.

<https://www.erasmusideal.com>

POOL INTERATTIVO DI STRUMENTI per il potenziamento delle abilità di base e delle competenze chiave degli adulti - Italia

L'idea del progetto è nata da un'analisi della situazione delle competenze di base degli adulti. L'indagine OCSE sulle competenze degli adulti (2013/14), sostenuta dalla DG Istruzione e cultura della Commissione, ha evidenziato che il 20% della popolazione europea in età lavorativa ha scarse competenze in materia di alfabetizzazione e calcolo, e che il 25% degli adulti non è in grado di utilizzare efficacemente le TIC. Questi dati hanno avuto implicazioni dirette per la strategia Europa 2020, sia a livello globale che di Paese, e hanno dimostrato la necessità di rafforzare la dimensione delle competenze della strategia Europa 2020. In questo contesto, l'obiettivo principale del progetto è stato quello di aumentare il livello di competenza nelle competenze di base tra gli adulti con un basso livello di istruzione di Romania, Polonia, Germania, Spagna e Italia attraverso i seguenti obiettivi operativi: raccogliere, analizzare e classificare gli strumenti OER esistenti e le buone pratiche a sostegno dell'istruzione degli adulti scarsamente qualificati, sviluppare un Pool interattivo (database online) di strumenti che consenta la categorizzazione e la valutazione degli strumenti esistenti e l'aggiunta di nuovi, sviluppare una Guida all'IPool che fornisca istruzioni passo-passo per l'utilizzo del pool e diffondere i risultati per garantirne l'uso anche in altri Paesi dell'UE e in altri settori educativi.

<http://www.i-pool.eu>

UPSKILL - Portogallo

Si tratta di un programma di riqualificazione professionale nel settore delle tecnologie digitali rivolto a disoccupati o lavoratori part-time. Il programma prevede una formazione intensiva in istituti universitari seguita dall'integrazione nel mercato del lavoro. Il programma è il risultato dell'unione di diverse istituzioni per organizzare un progetto nazionale in risposta alla crescente domanda di lavoratori qualificati nel settore delle TIC. Dall'inizio del programma, nel marzo 2020, si è registrato un aumento delle aziende che hanno aderito all'iniziativa. L'aumento del numero di aziende è un fattore necessario per incrementare le attività di formazione. Il programma prevede un approccio globale al mercato del lavoro. Si inizia con la registrazione delle aziende e l'identificazione del numero di professionisti che intendono assumere in base alla tecnologia e all'ubicazione. Il passo successivo consiste nell'identificare le aree tecnologiche, strutturare i corsi di formazione e determinare i relativi contenuti formativi coinvolgendo gli istituti di istruzione superiore in stretta collaborazione con le aziende. I corsi durano circa

sei mesi, seguiti da tre mesi di formazione sul lavoro nelle aziende partecipanti. Il progetto mira a garantire l'occupazione ad almeno l'80% dei partecipanti.

<https://upskill.pt>

PUNTI DI ACCESSO PER I CITTADINI PORTOGHESI - Portogallo

Il progetto ha creato più di mezzo migliaio di punti di accesso a una serie di servizi digitali di varie istituzioni pubbliche sparse in tutto il Portogallo (anche all'estero) con l'aiuto di una persona formata. I servizi offerti comprendono, ad esempio, documenti di stato civile, questioni fiscali ed erariali, sicurezza sociale e altri servizi pubblici. Tutti i punti sono dotati di un sistema a due schermi - uno per il cittadino e uno per l'impiegato - in modo che i cittadini possano seguire costantemente i passi compiuti dall'impiegato, consentendo loro di imparare per poter poi utilizzare essi stessi i servizi pubblici digitali. Aiutando coloro che hanno scarse competenze digitali, il progetto consente ai cittadini portoghesi di trarre il massimo vantaggio dai servizi pubblici online, rafforzando la fiducia nell'uso delle TIC e incoraggiando tutti i cittadini a utilizzarle.

E-MOCNI (E-EMPOWERED) - Competenze digitali, vantaggi reali - Polonia

Il progetto è stato finanziato dal Fondo europeo di sviluppo regionale nell'ambito del Programma operativo Polonia digitale. Il progetto è stato attuato da diverse istituzioni del settore delle ONG nel periodo 2016-2019. L'obiettivo del progetto era fornire formazione sulle TIC alle persone che non avevano ancora sfruttato le opportunità offerte dalle moderne tecnologie, comprese le persone con disabilità. Il progetto prevedeva una formazione in loco e online e offriva ai partecipanti al progetto l'opportunità di imparare a usare la tecnologia su base quotidiana e di utilizzarla per prendersi cura della propria salute, delle finanze o dell'istruzione, dello sviluppo professionale, delle relazioni con i propri cari o degli hobby. Nell'ambito di questo progetto, quasi 18.000 persone provenienti da 125 comuni di tutta la Polonia hanno preso parte ai corsi di formazione. Ai partecipanti sono stati offerti più di 100 argomenti di formazione raggruppati in diverse aree tematiche, ad esempio la gestione di un conto elettronico nell'area delle Finanze, le attività culturali su Internet nell'area degli Hobby, il social networking sulla base di Facebook nell'area delle Relazioni con i familiari.

<https://e-mocni.org.pl>

E-OBYWATEL (E-CITIZEN) NUOVE COMPETENZE DIGITALI - Polonia

Il progetto ha coinvolto quasi 9.000 persone provenienti da tutta la Polonia e comprendeva tre tipi di formazione legati all'acquisizione o allo sviluppo di competenze digitali. Si trattava di corsi di formazione tradizionali finalizzati all'acquisizione e al miglioramento delle competenze digitali nell'area del funzionamento del computer e dell'uso del computer nella vita quotidiana e professionale, integrati da lezioni individuali rivolte a gruppi con esigenze educative specifiche (ad esempio, persone con disabilità). Il secondo tipo riguardava la formazione online, che integrava o sviluppava le competenze digitali in aree specifiche della vita quotidiana, mentre il terzo tipo era dedicato alla formazione blended learning, che mirava a migliorare le competenze digitali specifiche.

<https://eobywatel.kig.pl>

JA W INTERNECIE (ME IN INTERNET) - Polonia

Si tratta di un programma di finanziamento per la formazione gratuita volta a migliorare le competenze digitali degli adulti, in modo che utilizzino maggiormente i servizi elettronici. Nell'ambito di questo programma, quasi 15.000 partecipanti hanno preso parte a corsi di formazione in diverse aree tematiche: Genitori online, Le mie finanze e transazioni online, Agricoltore online, Cultura online, La mia attività online. L'accento è stato posto sulla capacità dei partecipanti di ottenere e verificare informazioni, comunicare utilizzando vari strumenti, risolvere problemi, utilizzare software, utilizzare servizi pubblici e servizi elettronici. Il programma ha fornito ai partecipanti conoscenze e strumenti che hanno sviluppato le loro competenze per operare in modo efficiente e sicuro nel mondo digitale.

<https://jawinternecie.edu.pl>

The background features a complex, abstract design. In the top-left corner, there are concentric circles in shades of purple and pink, some with dashed lines and small dots. In the top-right corner, there are hexagonal shapes in shades of purple and pink. The bottom half of the image is dominated by large, concentric circles in shades of blue and teal, also with dashed lines and dots. The entire background is covered with a faint, repeating pattern of binary code (0s and 1s) in a light blue color.

CAPITOLO 3

**METODI E STRUMENTI SVILUPPATI
NELL'AMBITO DEL PROGETTO IAWARE**

Il progetto "iAware" ha prodotto venti piani didattici da 90 minuti suddivisi in cinque moduli tematici. Gli esperti hanno cercato di preparare lezioni efficaci tenendo conto dei fattori che determinano la specificità dell'educazione degli adulti, che è decisamente diversa dall'educazione dei bambini o dei giovani. Il formatore impegnato in questo tipo di formazione deve conoscere i principi dell'educazione degli adulti e saperli applicare nella pratica, cosa che sicuramente faciliterà il raggiungimento degli effetti previsti e l'effettiva realizzazione degli obiettivi formativi.

Nel processo di educazione degli adulti, è essenziale garantire le giuste condizioni per promuovere l'efficacia del processo di apprendimento. Devono essere confortevoli e sicure per il discente, poiché questo è uno dei fattori che lo motivano a intraprendere l'istruzione. Gli adulti spesso prendono decisioni basate su esperienze precedenti, quindi le conoscenze e le competenze che vogliono acquisire devono essere tradotte in applicazioni pratiche successive.

Il principio fondamentale dell'apprendimento degli adulti è che essi imparano attraverso l'esperienza. Ogni partecipante arriva alla formazione con il proprio bagaglio di conoscenze, modi di fare, opinioni e convinzioni a cui fare riferimento in situazioni specifiche. Per questo motivo, nel pianificare le lezioni dei moduli "iAware", gli esperti si sono allontanati dai modi di insegnamento "tradizionali", in cui il processo educativo da parte del formatore consisteva nel fornire ampie conoscenze teoriche e il compito del pubblico era quello di ascoltare pazientemente. Tutti i piani di lezione si basano su metodi e strumenti che enfatizzano fortemente l'attività e il coinvolgimento del discente, combinando teoria e pratica e insegnando l'uso delle conoscenze teoriche per risolvere problemi pratici specifici. L'attenzione è rivolta al discente e al suo processo di acquisizione di conoscenze e competenze. In questo approccio il formatore cerca di creare opportunità per nuove esperienze e sperimentazioni.

METODI DI INSEGNAMENTO

Un metodo di insegnamento può essere inteso come un modo deliberatamente e sistematicamente applicato di cooperazione tra l'insegnante e gli studenti, che consente a questi ultimi di padroneggiare la conoscenza insieme alla capacità di utilizzarla nella pratica. È il modo in cui l'insegnante-formatore lavora con gli studenti. La classificazione dei metodi di insegnamento non è standardizzata. Esistono molte divisioni diverse dei metodi di insegnamento, che dipendono dai criteri di divisione adottati. Se consideriamo l'attività del partecipante come criterio di divisione, possiamo distinguere tra metodi di somministrazione e metodi di attivazione.

I metodi espositivi comprendono quelli in cui il formatore-docente è la fonte della conoscenza. Assicurano che la persona che insegna sia attiva, mentre i discenti sono i destinatari dei contenuti trasmessi. Servono principalmente a presentare argomenti nuovi che possono essere appresi principalmente attraverso la trasmissione verbale dei contenuti. L'attività del discente è orientata a ricevere il messaggio, comprenderlo e ricordarlo. L'efficacia di questi metodi dipende principalmente dalle conoscenze, dalle competenze pedagogiche e dalla personalità dell'insegnante, nonché dalle condizioni organizzative e tecniche in cui si svolge l'insegnamento. Tra i metodi espositivi troviamo, ad esempio, la lezione, il racconto, la descrizione, la dimostrazione e l'istruzione.

I metodi di attivazione sono un gruppo di metodi di insegnamento caratterizzati dal fatto che nel processo di apprendimento l'attività dei partecipanti alle attività di insegnamento-apprendimento supera l'attività del formatore. Il gruppo dei metodi di attivazione comprende quelli in cui il processo di insegnamento-apprendimento crea le condizioni per la partecipazione attiva dei discenti alle attività educative. Questi metodi includono la lezione problematica, il metodo della discussione, il metodo del brainstorming, il metodo situazionale, la chat, la messa in scena o il metodo del progetto.

I metodi di attivazione, in cui sono coinvolti più sensi, consentono di formare pienamente le abilità. Le conoscenze e le abilità acquisite in azione sono durature e facilmente adottabili in altri ambiti dell'attività umana. L'attività mentale e l'attività cognitiva sono due tipi di attività legate al processo cognitivo. L'attività mentale può essere stimolata innescando le operazioni mentali desiderate, ad esempio creando una situazione problematica. L'attività cognitiva, invece, può essere indotta da soluzioni pratiche a situazioni legate alla vita quotidiana o alla pratica lavorativa.

Nell'educazione degli adulti, la selezione di un metodo appropriato è essenziale, poiché i discenti hanno già fatto molte esperienze e possono valutare criticamente i metodi scelti male.

METODI DI ATTIVAZIONE A SOSTEGNO DELL'EDUCAZIONE DEGLI ADULTI NEL PROGETTO 'IAWARE'

I metodi di attivazione utilizzati nel programma "iAware" consentono il massimo coinvolgimento dei partecipanti al corso nel processo di apprendimento. Inoltre, aiutano a raggiungere gli obiettivi di apprendimento. Tuttavia, il compito principale dei metodi di attivazione è quello di mettere i discenti in una situazione in cui sentano il bisogno di compiere l'azione che il formatore si aspetta da loro.

La lezione frontale è uno dei metodi di insegnamento più tradizionali. Tuttavia, affidarsi esclusivamente a questo metodo può causare noia e mancanza di impegno da parte del pubblico. È un mezzo per aiutare gli studenti a familiarizzare con le informazioni e ad ampliare le loro conoscenze, ma senza elementi di attivazione da parte loro può avere un effetto negativo sui risultati dell'apprendimento. Per questo motivo, invece di una lezione tradizionale, in molti casi è stata utilizzata una tecnica di guida, che consiste nel preparare una serie di domande per determinare ciò che i discenti già sanno sull'argomento in discussione.

Inoltre, è stato previsto l'utilizzo del metodo della "chat", ovvero una conversazione guidata dal formatore con i partecipanti, durante la quale il formatore aiuta i discenti a trovare la giusta soluzione a un determinato problema attraverso domande preparatorie, di guida o di raccolta. La chat è spesso introduttiva, utilizzata dal formatore per introdurre il pubblico all'argomento della lezione e per prepararlo al lavoro. Lo scopo di questa chiacchierata è organizzare il gruppo per il nuovo lavoro, cioè stabilire l'argomento e l'obiettivo della lezione e porre la domanda su cui il gruppo di formazione dovrà lavorare. Un altro obiettivo è quello di far scaturire un'attività mentale in tutti gli ascoltatori e di sviluppare la necessità di cercare le risposte da soli. Tale strumento permette di acquisire nuove conoscenze, di stabilire relazioni fino ad allora sconosciute tra cose e fenomeni e di trarre conclusioni.

Il metodo del "brainstorming" è un altro metodo didattico utilizzato durante le lezioni. Offre l'opportunità di proporre spontaneamente tutte le idee, anche le più avventurose, per la soluzione di un problema, senza una verifica preliminare. Le idee vengono proposte da tutti i partecipanti al gruppo di apprendimento. Il brainstorming si svolge in due fasi. La prima prevede la raccolta di idee, la formulazione di problemi e la loro registrazione (ad esempio scrivendole sulla lavagna), mentre la seconda fase si concentra sulla valutazione delle idee e delle proposte. Tuttavia, il metodo del brainstorming deve seguire alcune regole. La più importante è quella di garantire agli studenti la piena libertà di espressione. Ognuno di loro ha il diritto di proporre un'idea e altri possono aggiungerla, ma tutte le idee non devono essere commentate, criticate o giustificate.

La discussione costituisce un altro metodo di insegnamento che si può trovare nei piani didattici del progetto iAware. Si tratta di un metodo di insegnamento che prevede uno scambio di idee tra gli studenti, sia che le questioni espresse siano i loro punti di vista sia che si riferiscano alle opinioni degli altri. In una discussione, l'argomento deve essere ben formulato: né troppo difficile né troppo facile. Alla fine della discussione, dovrebbe esserci un riassunto, che fornisca una breve panoramica dei risultati e di come è stata condotta la discussione.

Il metodo dello caso di studio può essere utilizzato anche nei piani didattici. Il vantaggio principale di questo metodo è che permette al formatore di tradurre la teoria in un caso concreto. Si tratta di un'analisi dettagliata che presenta un problema specifico. Il metodo prevede l'analisi di un caso reale o ipotetico in cui il formatore presenta ai discenti un compito da svolgere e fornisce consigli utili per l'azione. I discenti si scambiano le proprie proposte per risolvere il problema. I casi di studio possono essere complessi e includere molte fasi di azione, ma nel caso del progetto "iAware" sono stati utilizzati casi di studio relativamente semplici che non richiedono molto tempo in classe e non sono molto complicati da eseguire.

Anche il metodo del progetto utilizza il principio dell'autoapprendimento. Si basa su un'azione pratica relativa alla realizzazione di un determinato evento. L'obiettivo di questo metodo è ricercare, organizzare e sistematizzare le informazioni provenienti da varie fonti e poi presentare i risultati del lavoro.

Inoltre, l'insegnamento attraverso i giochi didattici è un metodo didattico interessante che è stato sviluppato nel progetto. Il gioco didattico è un metodo di insegnamento che utilizza i giochi come forma per facilitare l'acquisizione di conoscenze e competenze. I giochi sono allegati ai programmi delle lezioni come supporto didattico e comprendono giochi sotto forma di vari quiz interattivi. Possono essere utilizzati per riassumere o rivedere le conoscenze acquisite durante le lezioni.

I vantaggi dei metodi di attivazione nell'apprendimento degli adulti includono:

- *Rendere le attività di apprendimento più attraenti,*
- *Consentire ai discenti di parlare, condividere le loro esperienze, trarre conclusioni in modo autonomo.*
- *Garantire la durata delle conoscenze acquisite in modo attivo.*
- *Integrare i discenti nel gruppo di formazione*
- *Favorire il coinvolgimento e l'interesse del discente per l'argomento*
- *Integrare le conoscenze provenienti da diverse aree della vita*

STRUMENTI DIDATTICI: MATERIALI MULTIMEDIALI E PIATTAFORMA 'IAWARE'

Il compito più importante del progetto che abbiamo realizzato consisteva nella creazione del programma di formazione modulare sulle competenze digitali "iAware". L'obiettivo principale di questo programma era quello di sviluppare la consapevolezza nell'uso delle moderne tecnologie e, per tecnologie moderne, intendiamo l'introduzione di nuove soluzioni di vita e di soluzioni tecnologiche che richiedono l'uso di Internet o di apparecchiature elettroniche - computer, tablet o smartphone.

Oltre ai piani di lezione, il progetto ha sviluppato anche un ambiente di apprendimento interattivo. Per ogni programma di lezione sono stati sviluppati almeno due materiali multimediali sotto forma di quiz, presentazioni o giochi interattivi per aumentare l'attrattiva della formazione e migliorare il coinvolgimento dei discenti. Questi materiali costituiscono anche un elemento di autovalutazione che aiuta a riassumere e verificare le conoscenze dei discenti. Dato il gruppo target, ovvero persone con scarse competenze in materia di TIC, i quiz sono stati preparati in forma semplice, in modo che il loro utilizzo fosse facile e intuitivo per l'utente.

Gli autori del progetto hanno deciso di sfruttare le possibilità di Internet, considerandolo uno strumento eccellente per integrare e supportare l'istruzione tradizionale. Oltre al programma "iAware" e al suo ambiente di apprendimento complementare, il progetto ha portato alla creazione di una piattaforma di apprendimento. L'intero corso, suddiviso in cinque moduli secondo il programma di formazione, è stato caricato su questa piattaforma:

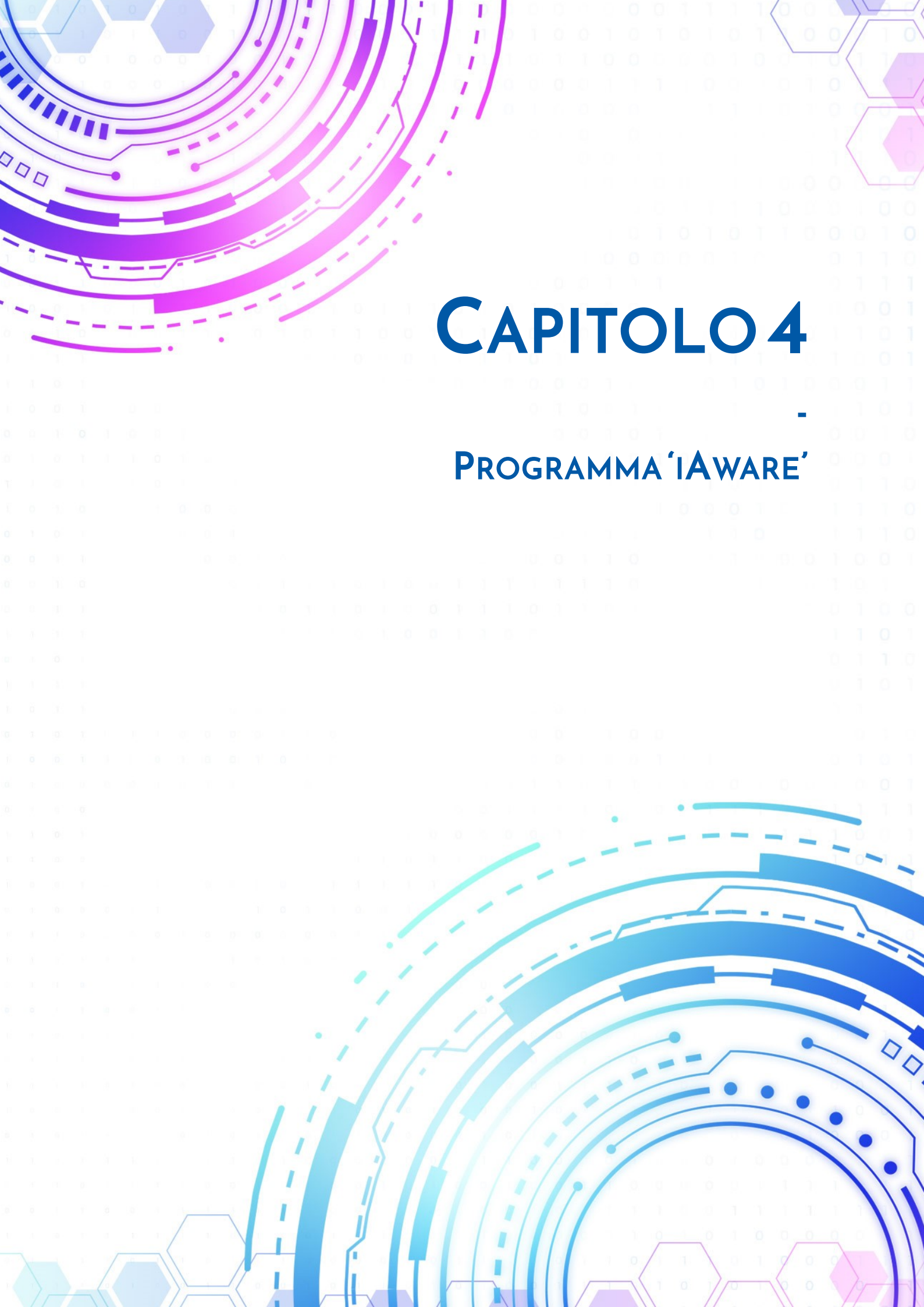
1. *Tipi e identificazione delle minacce in Internet.*
2. *Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete.*
3. *Partecipazione attiva alla società dell'informazione.*

4. *Uso consapevole delle tecnologie dell'informazione e della comunicazione.*
5. *Indicazioni per lo sviluppo di Internet, costruzione attiva di una comunità globale di e-cittadini.*

L'obiettivo della creazione della piattaforma era, da un lato, aumentare l'attrattiva della formazione erogata secondo il programma sviluppato nel progetto e, dall'altro, fornire un accesso più ampio ai prodotti del progetto e raggiungere un gruppo target più ampio, coinvolgendo anche i discenti che hanno difficoltà a frequentare la formazione tradizionale, spesso a causa di barriere geografiche, temporali o disabilità. La condivisione dei materiali didattici online può anche incoraggiare l'autoapprendimento e l'individualizzazione del processo di apprendimento: ogni discente può tornare a consultare questi materiali in qualsiasi momento, in qualsiasi luogo e al proprio ritmo di apprendimento.

La piattaforma è stata sviluppata dal partner italiano del progetto PRISM ed è disponibile all'indirizzo <https://www.iaware-education.eu>. Nella sezione materiali si possono trovare tutti i risultati sviluppati nell'ambito del progetto, suddivisi in due categorie: per il discente e per il formatore. È disponibile in quattro versioni linguistiche: inglese, polacco, portoghese e italiano. Per i discenti interessati è disponibile un modulo relativo alla registrazione degli utenti sulla piattaforma. Il sito web è stato appositamente progettato per essere di facile lettura, in modo che tutti i discenti, anche quelli con il più basso livello di conoscenza di Internet, possano trovare le informazioni giuste.

Il presupposto che ha accompagnato gli esperti nella preparazione del programma è stato quello di concentrarsi sulla realizzazione di esercizi pratici. Gli esempi preparati erano basati su standard funzionanti nella vita quotidiana, sociale o professionale e dovevano far riferimento all'esperienza dei discenti. Gli esperti hanno preparato una serie di materiali per i discenti che coprono tutti e cinque i moduli. Oltre ai materiali interattivi da loro sviluppati, il corso include collegamenti ad altri siti web, video con contenuti simili e altri esempi. In questo modo, dopo il corso, i discenti potranno affinare da soli le conoscenze e le competenze acquisite nel corso. Una discussione dettagliata dei piani di lezione e dei materiali di accompagnamento si trova nella sezione successiva relativa al programma, che comprende il programma stesso, i materiali e le linee guida per i formatori che desiderano lavorare con il metodo "iAware".

The background features a light blue and white binary code pattern. In the top-left corner, there are concentric circles and arcs in shades of purple and pink. In the bottom-right corner, there are concentric circles and arcs in shades of blue and teal. Hexagonal shapes are scattered throughout, some in purple/pink and others in blue/teal.

CAPITOLO 4

PROGRAMMA 'IAWARE'

PRESUPPOSTI, OBIETTIVI E RISULTATI DEL PROGRAMMA

Il progetto "iAware - Programma innovativo per l'educazione degli adulti" è realizzato da un partenariato di tre organizzazioni di Polonia, Italia e Portogallo. L'organizzazione polacca EURO-FORUM ne è il leader, mentre la portoghese COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL e l'italiana PRISM IMPRESA SOCIALE SRL sono le organizzazioni partner. Il progetto è una risposta al problema, rilevato congiuntamente, delle insufficienti competenze digitali degli adulti. Il problema deriva dalla mancanza di programmi educativi moderni che includano contenuti che vadano oltre l'apprendimento delle abilità di funzionamento standard dei dispositivi moderni e dell'uso delle risorse di rete. Il progetto affronta quindi le sfide contemporanee legate allo sviluppo della tecnologia e di Internet e risponde all'esigenza di un miglioramento continuo delle competenze TIC degli adulti nell'attuale realtà di Internet.

Gli obiettivi principali del progetto comprendono:

- *creazione di un programma di educazione all'avanguardia alle TIC per gli adulti che tenga conto delle sfide contemporanee nel campo della sicurezza di Internet e dell'uso consapevole delle risorse online;*
- *fornire i giusti contenuti educativi, gli strumenti, le conoscenze e le competenze per sviluppare negli adulti atteggiamenti di uso consapevole delle moderne tecnologie ai formatori e agli educatori di adulti nel campo delle TIC;*
- *miglioramento delle competenze chiave in materia di TIC tra gli adulti dell'Unione Europea e costruzione di una società dell'informazione responsabile.*

Nell'ambito del progetto sono stati prodotti i seguenti risultati:

1. *Il programma di formazione modulare per le competenze digitali "iAware".*

Si tratta di un programma di formazione innovativo per sviluppare le competenze digitali degli adulti. Sviluppato in modo pratico e funzionale, è stato suddiviso in cinque moduli tematici che affrontano questioni relative alle minacce online, alla loro identificazione, alla prevenzione, alla partecipazione attiva nella società dell'informazione o all'uso consapevole delle moderne tecnologie dell'informazione e della comunicazione. Il programma di formazione è accompagnato da un elaborato supplemento didattico che contiene i contenuti del programma sotto forma di materiale multimediale - quiz e video.

2. *La piattaforma di apprendimento "iAware" è disponibile all'indirizzo <https://www.iaware-education.eu>.*

Si tratta di un'applicazione basata sul web in cui tutti i materiali sviluppati nell'ambito del progetto - il programma, il supplemento didattico e questo e-book - sono resi disponibili in forma digitalizzata. Ciò consentirà ai formatori di erogare la formazione in modo più accattivante, utilizzando contenuti multimediali dedicati ai singoli moduli. La piattaforma sarà a disposizione di tutti gli adulti che desiderano migliorare le proprie competenze nell'uso consapevole delle moderne tecnologie digitali.

3. *Una guida metodologica con istruzioni per i formatori, ovvero il presente e-book.*

Si tratta di un manuale di istruzioni sull'uso degli strumenti per i formatori e gli educatori delle TIC che lavorano con gli adulti, pubblicato sotto forma di e-book, che si concentra sul supporto sostanziale allo sviluppo dei formatori nelle aree di competenza più bisognose di intervento, in relazione ai bisogni diagnosticati nel progetto. Tutti i contenuti inclusi nell'e-book sono il più possibile universali, cioè possono essere implementati sia nel partenariato che in altri Paesi europei.

STRUTTURA DEL PROGRAMMA

Tutte le attività del progetto sono concepite per contribuire all'obiettivo finale, in linea con la politica della Commissione Europea, di migliorare le competenze chiave delle TIC negli adulti dell'Unione Europea e di costruire la società dell'informazione. Questo obiettivo sarà raggiunto attraverso la creazione di un moderno programma di educazione alle competenze digitali per gli adulti, che terrà conto delle sfide contemporanee di Internet, compresa la comprensione dei rischi e delle opportunità dello sviluppo del web.

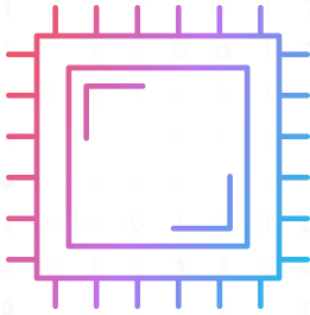
L'intero programma è stato suddiviso in cinque moduli. Ogni modulo è composto da quattro lezioni di 90 minuti, come mostrato nel diagramma:

Modulo 1	Modulo 2	Modulo 3	Modulo 4	Modulo 5
Lezione 1	Lezione 1	Lezione 1	Lezione 1	Lezione 1
Lezione 2	Lezione 2	Lezione 2	Lezione 2	Lezione 2
Lezione 3	Lezione 3	Lezione 3	Lezione 3	Lezione 3
Lezione 4	Lezione 4	Lezione 4	Lezione 4	Lezione 4

In totale, il programma contiene venti schemi di lezione integrati da materiali didattici multimediali. Sia i programmi delle lezioni che i materiali multimediali per i partecipanti al corso si integrano a vicenda. Tutti i materiali sono stati resi disponibili in forma digitale sulla piattaforma iAware all'indirizzo: <https://www.iaware-education.eu>.

I singoli moduli trattano argomenti quali:

- ❖ *Modulo 1 - Tipi e identificazione delle minacce online*
- ❖ *Modulo 2 - Contrastare e minimizzare i rischi e garantire la sicurezza online*
- ❖ *Modulo 3 - Partecipazione attiva alla società dell'informazione*
- ❖ *Modulo 4 - Uso consapevole delle competenze TIC*
- ❖ *Modulo 5 - Tendenze di Internet, costruzione attiva di una comunità globale di e-cittadini*



MODULO 1

-

TIPI E IDENTIFICAZIONE DELLE MINACCE ONLINE

Internet è un mezzo essenziale senza il quale sarebbe difficile immaginare di operare efficacemente nel mondo moderno. Tuttavia, è risaputo che l'uso del web può rappresentare una minaccia per i suoi utenti. Se usato correttamente, Internet può essere utile sia all'utente che alla società. Tuttavia, spetta soprattutto alla razionalità degli utenti fare un uso corretto delle possibilità del web. L'utente è l'anello più debole della catena, ed è per questo che gli esperti hanno deciso di dotare i partecipanti al programma "iAware" di conoscenze su come utilizzare Internet in modo sensato. Il primo modulo del programma "iAware" riguarda i diversi tipi e l'identificazione delle minacce online.

Prevede i seguenti argomenti:

1. *Spam e truffe*
2. *Phishing*
3. *Privacy online*
4. *Impronta digitale*

Argomenti molto simili saranno trattati nel secondo modulo - "Contrastare e minimizzare le minacce e garantire la sicurezza online", che costituirà un ulteriore sviluppo degli argomenti del primo modulo. Le lezioni del primo modulo si concentrano sulla presentazione, la definizione e l'identificazione delle minacce. Le lezioni del secondo modulo mostreranno come difendersi efficacemente dalle minacce in questione.

Lezione 1

Spam e truffe

L'obiettivo principale della prima lezione è quello di identificare le minacce dello spam e della truffa e di capire quali possibili rischi comportano. Sono entrambi fenomeni abbastanza comuni e i discenti potrebbero averli già incontrati. Nell'identificare questi fenomeni, il formatore deve determinare il livello di conoscenza dei discenti e fare riferimento alle loro esperienze precedenti. I discenti dovrebbero essere in grado di identificare le minacce da soli ed eventualmente integrare le loro conoscenze. Lo spam, ad esempio, può essere definito come un messaggio non richiesto inviato per via elettronica tramite e-mail o vari instant messenger, mentre lo spam è solitamente inviato in massa, più frequentemente sotto forma di pubblicità. L'essenza di questo tipo di messaggi consiste nell'inviare una grande quantità di informazioni con lo stesso contenuto a un pubblico molto vasto. In altre parole, lo spam può essere definito come l'invio di messaggi elettronici inaspettati su scala di massa in modo anonimo.

Quando si parla di spam, è importante considerare anche la definizione di e-mail di massa. Fondamentalmente, si possono distinguere due categorie di e-mail di massa. La prima categoria è costituita da offerte commerciali non richieste, altrimenti note come spam commerciale di natura pubblicitaria, vietato dalla legislazione europea. Il secondo gruppo di e-mail di massa comprende le e-mail di massa non richieste. Questa categoria comprende e-mail di natura solitamente non commerciale, ad esempio appelli di organizzazioni sociali, enti di beneficenza, richieste di aiuto o avvisi di massa.

Affinché un messaggio sia considerato spam, devono essere soddisfatte le tre condizioni seguenti:

- *il contenuto del messaggio è indipendente dall'identità del destinatario.*
- *il destinatario del messaggio non ha dato il proprio consenso preventivo alla ricezione del messaggio stesso*
- *il contenuto del messaggio dà adito all'aspettativa che il mittente tragga un beneficio sproporzionato dall'invio del messaggio.*

I formatori devono ricordare ai discenti che, sebbene sembri un fenomeno relativamente innocuo, lo spam genera una serie di problemi ed è una seccatura per i destinatari. Ingombra le caselle di posta degli utenti di Internet, blocca la rete, sovraccarica i server e occupa spazio su disco. Inoltre, rappresenta una minaccia per la sicurezza degli utenti di Internet, in quanto fonte di virus. Nonostante le numerose misure di protezione, le e-mail di spam arrivano in gran numero. I mittenti utilizzano spesso metodi non etici per inviare spam, ad esempio spacciandosi per banche o altre istituzioni affidabili. Possono anche intitolare "abilmente" i messaggi in modo tale che sia molto probabile che vengano letti da utenti Internet incuriositi. Un messaggio di posta elettronica con il titolo "hai ricevuto un'eredità" o "hai vinto un premio" può effettivamente incoraggiare il destinatario a leggere il contenuto di tale messaggio non richiesto.

Gli studenti devono essere consapevoli del fatto che l'invio di messaggi non richiesti è regolamentato a livello europeo e in ogni Stato membro. Uno dei compiti della lezione è scoprire quali leggi nazionali regolano questi fenomeni. I formatori dovrebbero quindi verificare prima della lezione quali leggi o regolamenti disciplinano lo spam e le truffe nel loro Paese.

MODULO	Tipi e identificazione delle minacce in Internet	UNITA'	1	TEMA	Spam e truffa
RISULTATI DI APPRENDIMENTO: - Gli studenti saranno in grado di nominare minacce come spam e truffe. - Gli studenti saranno in grado di identificare spam o truffa. - Gli studenti capiranno i possibili pericoli di queste attività.					
FASI	OBIETTIVO	PROCEDURE			RISORSE
ARGOMENTO DI STUDIO (tempo: 15 minuti)	Far conoscere agli studenti gli obiettivi e i risultati della formazione Familiarizzare gli studenti con esempi di messaggi di truffa e spam	1. Il formatore saluta gli studenti 2. Il formatore definisce e presenta agli studenti gli obiettivi della lezione: • Dopo la lezione di oggi saprai cosa sono spam e truffa • Capirai come funziona lo spam • Saprai perché non vale la pena rispondere alle e-mail che sono spam 3. Il formatore fa conoscere agli studenti il programma della lezione e le sue fasi successive 4. Il formatore chiede agli studenti di aprire la loro e-mail (se ne hanno una). Chiede loro di trovare tra i messaggi nell'e-mail, esempi di messaggi inviati loro a loro insaputa, che non volevano e che ritengono non necessari.			ARGOMENTO DI STUDIO (tempo: 15 minuti)

		5. Gli studenti cercano nella loro posta elettronica, condividono i messaggi "più interessanti" sul forum del gruppo. Il formatore evidenzia i diversi tipi di questi messaggi.	
Compito PROVA A NOMINARE (tempo: 15 minuti)	Per nominare il fenomeno dello spam Per definire la truffa in relazione allo spam	1. Il fenomeno dello SPAM per gli utenti di posta elettronica è abbastanza noto; quindi, a seconda delle conoscenze degli studenti, il formatore può chiedere loro di definire lo spam o fornisce una definizione e mostra esempi in un account di posta elettronica. Definizioni esemplificative di SPAM in termini così generali possono essere trovate nel capitolo di questa lezione nell'e-book. 2. Il formatore fa notare agli studenti che lo spam di solito va di pari passo con un altro fenomeno, cioè la truffa. Il formatore spiega che la truffa può essere tradotta come farsa / truffa perché è una truffa in cui si guadagna prima fiducia e poi si usa, ad esempio, per estorcere denaro. Un'attività tipica è l'invio di corrispondenza di massa (spam) per via elettronica e l'offerta alla vittima, in tale messaggio, di una quota di enormi profitti in cambio di una presunta intermediazione che richiede pochi investimenti.	Compito PROVA A NOMINARE (tempo: 15 minuti)
Compito ATTO	Familiarizzare gli studenti con un tipo di truffa	1. Il formatore introduce gli studenti alle restanti attività della lezione. In base alla fase della lezione precedente, il trainer descrive uno dei più famosi tipi di truffa.	Compito ATTO (tempo: 25 minuti)

**(tempo: 25
minuti)**

2. Forse l'esempio più famoso di spam è la cosiddetta "truffa nigeriana", una truffa che consiste nell'estorsione di fondi e dati personali inviati volontariamente dalle vittime direttamente ai truffatori. Vari tipi di storie (ad esempio sull'acquisizione di un'eredità) vengono inviati come spam agli account di posta elettronica. Il truffatore di solito offre alla vittima di dividere una grande quantità di denaro a condizioni diverse, ma solo dopo aver effettuato un trasferimento di denaro sul suo conto. Infatti, il denaro inviato dalla vittima viene intercettato dal truffatore.

3. Il formatore sottolinea che SPAM e SCAM sono cose molto serie che accadono online, ma a volte possono essere trattate con umorismo.

4. Il formatore invia agli studenti un collegamento al video su YouTube o riproduce il video sullo schermo.

5. Il formatore parla agli studenti dello spam, se hanno mai ricevuto tale e-mail nella loro casella di posta, cosa hanno fatto in tal caso e discute quali potrebbero essere le conseguenze di rispondere allo spam come nel video di esempio.

6. Gli studenti rispondono alle domande del formatore e condividono le loro riflessioni sul video guardato.

Compito

Per capire come funziona lo spam e

1. Il formatore spiega agli studenti che si stima che circa l'80% di tutti i messaggi giornalieri siano posta indesiderata, ovvero spam.

Compito

ATTO **(tempo: 20 minuti)**

quali possono essere le sue conseguenze

Per presentare una panoramica dei diversi tipi di spam

Per definire altri termini relativi allo spam

2. Il formatore chiede agli studenti di pensare alle conseguenze dell'invio di così tanti messaggi. Gli studenti possono essere divisi in gruppi più piccoli in modo da riflettere sulla domanda, quindi presentare i risultati del loro lavoro sul forum e confrontarli con gli effetti del lavoro di altri gruppi. Gli studenti possono controllare le loro caselle di posta elettronica.

Esempi di conseguenze che possono essere menzionate:

- Blocco dello spazio su disco
- Minaccia di infezione da un virus dannoso
- Rallentamento dei server a seguito di un aumento del lavoro di elaborazione dello spam
- Possibilità di perdere i messaggi ricevuti bloccando la posta in arrivo
- Creare un caos nella propria casella di posta, che può portare alla perdita di messaggi importanti
- Problemi durante la lettura della posta normale
- Phishing dei dettagli di contatto
- Ridotta fiducia nella pubblicità su Internet
- Trasmissione di contenuti indesiderati da parte dell'utente (ad es. Contenuti per adulti, offensivi)

ATTO

(tempo: 20 minuti)

3. Il prossimo compito degli studenti sarà quello di classificare e dividere i messaggi di spam in categorie.

- Annunci
- Eredità
- E-mail fittizie - qui il formatore dovrebbe invitare gli studenti alla lezione successiva, interamente dedicata al fenomeno dell'estorsione dei dati e del phishing

4. Il formatore chiede agli studenti di considerare se hanno riscontrato spam da qualche parte al di fuori dell'e-mail. Forse ricevono telefonate indesiderate o lettere tradizionali con messaggi pubblicitari che non hanno ordinato. Questo può anche essere chiamato spam. Gli studenti condividono le loro esperienze con il gruppo. Questa attività, a seconda delle dimensioni del gruppo di formazione, può essere eseguita con l'intero gruppo o suddivisa in squadre di più persone.

5. Il formatore spiega agli studenti che la persona che invia spam, cioè i messaggi non richiesti, è chiamata spammer.

6. D'altra parte, per inviare tali messaggi, viene utilizzato un software speciale, appositamente progettato per diffondere lo spam e chiamato bot o spambots.

CAPITOLO 4

BUONE ABITUDINI (tempo: 10 minuti)	Gli studenti insieme al formatore creano un elenco di buone pratiche per quanto riguarda la posta elettronica non richiesta.	1. Gli studenti valutano come ridurre lo spam e condividono i loro commenti sul forum del gruppo. 2. Su Internet cercano norme legali riguardanti lo spam che siano vincolanti in un determinato paese.	BUONE ABITUDINI (tempo: 10 minuti)
COMPITO DI RISPOSTA / RIFLESSIONE (tempo: 5 minuti)	Revisionare e verificare le conoscenze acquisite. Per ottenere feedback dagli studenti in merito alla lezione.	Il formatore riassume la lezione e controlla la reazione degli studenti alla lezione (positiva / negativa).	COMPITO DI RISPOSTA / RIFLESSIONE (tempo: 5 minuti)
Quiz di autoapprendimento Apprendimento esteso Consolidamento	Riassumere	Il trainer riassume la lezione. Se il formatore desidera continuare la lezione sul fenomeno della truffa, deve passare alla lezione successiva di questo modulo che tratta l'estorsione dei dati e il phishing. Dopo aver ampliato entrambi gli argomenti, è possibile visitare il modulo: "Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete".	

Per la lezione sono previsti due quiz interattivi.



Quiz 1

Questo quiz può essere utilizzato alla fine della lezione come riepilogo di ciò che gli studenti dovrebbero sapere dopo la lezione e può essere svolto insieme, ad esempio su una lavagna interattiva, o da ogni studente individualmente sul proprio computer/tablet. I formatori possono anche chiedere agli studenti di fare il quiz a casa come autovalutazione. Il quiz consiste in dieci domande a cui rispondere VERO o FALSO. Di seguito è riportato il contenuto del quiz con le risposte corrette.

- 1) *Spam significa inviare messaggi elettronici in modo anonimo. VERO*
- 2) *La truffa è l'induzione fraudolenta della fiducia al fine di frodare. VERO*
- 3) *Lo spam può assumere la forma di invio di "catene portafortuna". VERO*
- 4) *Lo spam viene inviato in forma anonima per rendere difficile l'individuazione del mittente effettivo. VERO*
- 5) *I contenuti di spam possono comparire anche sui forum di Internet.*
- 6) *Lo spam è un fenomeno del tutto innocuo. FALSO*
- 7) *I siti di social network come Facebook e Instagram sono sicuri e gli utenti non sono esposti a spam e truffe.*
- 8) *Un messaggio di truffa è un messaggio malevolo progettato per frodare. VERO*
- 9) *Un messaggio truffa può assomigliare in modo confuso a un messaggio di istituzioni pubbliche reali. VERO*
- 10) *È sicuro cliccare su tutti i link forniti nelle e-mail. FALSO*



Quiz 2

Questo quiz è anche un riassunto della lezione - una raccolta di tutte le informazioni chiave da ricordare dalla lezione. Il formatore può visualizzarlo sulla LIM alla fine della lezione o gli studenti possono visualizzarlo sui loro dispositivi. Può anche essere un brevissimo promemoria dell'input della lezione prima della prima lezione del secondo modulo, che tratta della difesa efficace contro lo spam e le truffe. Di seguito viene presentato il contenuto di questo breve riassunto.

Schermata 1

SPAM

- *Per lo più e-mail inviate in massa a molti destinatari*
- *I destinatari non hanno ordinato o accettato di ricevere tali messaggi.*
- *Si verifica anche in altri canali di comunicazione: messaggi di testo, messaggistica istantanea o siti di social network.*

Schermata 2

SPAM

- *Alcuni di questi messaggi possono essere innocui: si limitano a riempire la casella di posta elettronica.*
- *Ci sono messaggi che possono rappresentare una minaccia per l'utente*
- *Lo scopo dei messaggi pericolosi è quello di frodare i dati o il denaro dell'utente.*

Schermata 3

TRUFFA

- *Un fenomeno molto comune su Internet*
- *Una forma di truffa online o telefonica*
- *Basato sull'induzione della fiducia per portare al phishing*

Schermata 4

TRUFFA

- *Nei casi di frode online, i truffatori utilizzano moduli o siti web fraudolenti che si spacciano per siti reali.*
- *I criminali possono anche spacciarsi per istituzioni pubbliche*
- *Tra le truffe più diffuse ci sono offerte di prodotti a prezzi sorprendentemente bassi, premi inaspettati in concorsi, storie di eredità ricevute ma anche sostegno a persone malate o disabili.*

Lezione 2

Phishing

È probabile che la maggior parte degli utenti di telefonia mobile e dei titolari di account di posta elettronica abbia ricevuto almeno una volta nella vita un messaggio sospetto. Se era accompagnato da un link, molto probabilmente si trattava di phishing. Sfortunatamente per l'utente medio del web, i truffatori stanno diventando sempre più bravi a impossessarsi dei dati e a utilizzare le informazioni ottenute per ingannare la vittima. Pertanto, gli obiettivi principali di questa lezione sono: sensibilizzare gli studenti sulla necessità di proteggere i propri dati quando navigano sul web e identificare il fenomeno del phishing.

Esempi di definizioni di phishing che possono essere fornite agli studenti della classe:

- *Il phishing è un metodo di frode che consiste nell'impersonare un'istituzione o una persona nota alla vittima per indurla a fornire informazioni preziose o a infettare i suoi dispositivi con malware o a convincerla a compiere determinate azioni.*
- *Il phishing è un metodo di frode che consiste, nella maggior parte dei casi, nell'invio di e-mail o SMS che affermano di provenire da aziende o istituzioni pubbliche affidabili per indurre le persone a rivelare informazioni personali come password o numeri di carte di credito.*
- *Il phishing è un attacco di ingegneria sociale che mira a indurre la vittima a rivelare volontariamente informazioni riservate.*
- *Il phishing è una truffa online in cui una terza parte si spaccia per un'azienda o un'istituzione al fine di ingannare una persona e indurla ad accedere al sistema bancario elettronico, a ordinare e ad autorizzare una transazione di pagamento.*

Il termine "ingegneria sociale" è anche legato al concetto di phishing e cerca di sfruttare gli anelli più deboli della catena della sicurezza, ossia le persone, facendo appello alla vanità, all'avidità, alla curiosità e all'altruismo o al rispetto o alla paura dell'autorità per convincerle a rivelare determinate informazioni o ad accedere a un sistema informatico. In altre parole, l'ingegneria sociale consiste nell'ingannare le persone convincendole a rivelare i loro dati privati, come password o conti bancari, o a concedere l'accesso a un computer per installare discretamente un malware.

MODULO	Tipi e identificazione delle minacce in Internet	UNITA'	2	TEMA	estorsione di dati - phishing
RISULTATI DI APPRENDIMENTO: - Gli studenti sanno che devono proteggere i propri dati durante la navigazione sul web. - Gli studenti impareranno il significato dei termini estorsione di dati, phishing. - Gli studenti sono consapevoli che i truffatori di Internet potrebbero essere interessati ai loro dati. - Gli studenti capiranno che divulgando le proprie informazioni possono diventare vittime di frodi su Internet.					
FASI	OBIETTIVO	PROCEDURE			RISORSE
ARGOMENTO DI STUDIO (tempo: 25 minuti)	Far conoscere agli studenti gli obiettivi e i risultati della lezione Introdurre gli studenti all'argomento della lezione Determinare dagli studenti il tipo di dati che possono essere oggetto di phishing in Internet	1. Il formatore saluta gli studenti. 2. Il formatore definisce gli obiettivi della lezione e li presenta agli studenti: • Dopo la lezione di oggi saprai cos'è l'estorsione dei dati • Nella lezione di oggi imparerai il significato della parola PHISHING • Acquisirete familiarità con i diversi tipi di metodi di phishing 3. Il formatore fa conoscere agli studenti il programma della lezione e le sue fasi successive 4. Il formatore chiede agli studenti di pensare per un momento quali dati possono essere richiesti dal punto di vista della persona che vorrebbe utilizzarli in modo inappropriato. Per aiutare a guidare gli studenti			- una serie di messaggi sospetti stampati - una serie di messaggi sospetti in una versione elettronica - un proiettore e un computer con accesso a Internet per il formatore

		sull'argomento, il formatore può utilizzare esempi di messaggi di phishing in formato cartaceo o elettronico. Quindi il formatore pone la domanda "Quali dati vogliono ottenere da noi i mittenti di tali messaggi?" 5. Brainstorming con gli studenti: tutte le idee relative ai dati vengono scritte alla lavagna. I dati che possono interessare i truffatori includono: nome e cognome, data di nascita, numero di identificazione PESEL, numero di carta d'identità, luogo di residenza, numero di telefono, dati di accesso al servizio bancario elettronico, numero di conto bancario, dettagli di accesso a negozi online o piattaforme di aste, dettagli di accesso e-mail, nomi utente e password per vari siti Web e social network, foto. 6. Il formatore riassume brevemente le idee raccolte e coinvolge gli studenti nella fase successiva, considerando per cosa possono essere utilizzati tali dati (ad es. Estorsione di un credito, prestito, creazione di un conto bancario falso, acquisto di vari, creazione di conti falsi o un profilo su un sito di social networking, impersonare una determinata persona e scrivere opinioni o commenti offensivi, stipulare contratti falsi, condurre attività commerciali, falsificare documenti, furto di identità).	
Compito PROVA A NOMINARE (tempo: 10 minuti)	Per definire i termini "estorsione di dati" e "phishing"	1. Il formatore chiede agli studenti di cercare di abbozzare la definizione del termine "estorsione di dati" da soli 2. Il formatore combina il concetto di estorsione dei dati con il concetto di PHISHING e ne dà la definizione. Definizioni	- un proiettore e un computer con accesso a Internet per il trainer - lavorare con i computer - gli studenti hanno accesso

CAPITOLO 4

esemplari del fenomeno PHISHING possono essere trovate nel libro nel capitolo assegnato a questa lezione.

a un computer con connessione Internet

- Per facilitare una memorizzazione migliore e più rapida, il formatore può fare riferimento a un video di YouTube che spiega il concetto di phishing. Esempi:
- Cos'è il phishing?
- <https://www.youtube.com/watch?v=BnmneAjVrM4>
- <https://www.youtube.com/watch?v=hG6XJROw8HY>
- <https://www.youtube.com/watch?v=BzNh-gxosE8>

Compito ATTO (tempo: 20 minuti)

Comprendere i meccanismi di phishing

Per trovare "" l'anello più debole "

Conoscere il concetto di "ingegneria sociale"

Presentare una panoramica dei

1. Il formatore può dividere gli studenti in gruppi e inviare a ciascun gruppo un collegamento o fornire un esempio di e-mail stampata su un pezzo di carta che costituisce un esempio di phishing. Con un numero limitato di studenti, il lavoro di gruppo può essere sostituito con il lavoro individuale.
2. Il formatore chiede agli studenti di esaminare e-mail di esempio che erano attacchi di phishing e di considerare il motivo per cui questi attacchi hanno successo.

- un proiettore e un computer con accesso a Internet per il trainer
- lavorare con i computer - gli studenti hanno accesso a un computer con connessione Internet
- Esempi di messaggi di posta elettronica che illustrano il fenomeno

diversi tipi di phishing

3. Dopo una breve riflessione, ogni gruppo presenta le proprie conclusioni.
4. Il formatore sottolinea che, a differenza di altre minacce online, il phishing non richiede conoscenze tecniche particolarmente avanzate, perché i criminali non sfruttano la vulnerabilità tecnica del software del dispositivo, ma utilizzano tecniche di manipolazione chiamate ingegneria sociale. Si scopre che l'anello più debole è una persona che non controlla esattamente l'origine dell'email.
5. Il formatore sottolinea che gli attacchi di phishing consistono nell'innescare determinate emozioni - paura, rabbia, curiosità, in modo da provocare una reazione automatica e rapida.
6. Il formatore introduce gli studenti al concetto di "ingegneria sociale". Definizione di esempio da trovare nell'e-book.
7. Una panoramica dei diversi tipi di phishing: il formatore sottolinea che la procedura di phishing non riguarda solo la posta elettronica.
 - Spear phishing: questo è un tipo di attacco che prende di mira un'istituzione o una persona. Un attacco di questo tipo viene profilato, ovvero l'attaccante raccoglie in anticipo informazioni sulla sua vittima e solo allora costruisce un messaggio che è per convincere la vittima a visitare un sito web fasullo o scaricare un file predisposto

PHISHING possono essere trovati su:

- <https://its.lehigh.edu/phishing/examples>
- <https://www.phishing.org/phishing-examples>
- <https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive>

		- Clonazione di posta elettronica: un attacco in cui il criminale utilizza un messaggio reale precedentemente inviato all'utente. L'autore dell'attacco copia il modello di messaggio autentico e vi inserisce un collegamento a un sito Web dannoso - Reindirizzamento a un'altra pagina: reindirizzamento deliberato degli utenti che visitano una determinata pagina Web a un'altra, il più delle volte fabbricato dallo stacker - Messaggi di testo e phishing telefonico: questo attacco utilizza messaggi di testo e vocali, in cui i criminali utilizzano strumenti speciali per impersonare il numero di telefono di un'azienda specifica o inviare messaggi di testo falsi	
BUONE PRATICHE (tempo: 30 minuti)	Scambiare le proprie esperienze degli studenti. Riassumere e organizzare le conoscenze acquisite	1. Il formatore chiede agli studenti se hanno avuto esperienze di phishing, se ne sono stati vittime o se hanno riscontrato questo fenomeno nel loro ambiente circostante. 2. Il formatore, insieme agli studenti, svolge un esercizio che raccoglie le conoscenze e riassume il lavoro. 3. Gli studenti lavorano in gruppo (con un piccolo numero di studenti può essere fatto individualmente) 4. Il formatore chiede agli studenti di creare il proprio esempio di e-mail di phishing. Possono utilizzare esempi di tali messaggi dalle fasi precedenti. Gli studenti lavorano in editor di testo o nel proprio account di posta elettronica. Per organizzare il lavoro, gli studenti	- un computer, un proiettore, accesso a Internet - un editor di testo o un account di posta elettronica

		dovrebbero considerare di affrontare le seguenti domande: • Quale potrebbe essere lo scopo dei dati di phishing? • Quali dati vorrebbero estorcere? • Dove e come potrebbero utilizzare questi dati? • Come formulare un'e-mail per renderla credibile? 5. Gli studenti creano le loro e-mail, presentano i risultati del loro lavoro, rispondono alle domande poste sopra e scambiano commenti con altri studenti.	
COMPITO DI RISPOSTA / RIFLESSIONE (tempo: 5 minuti)	Revisionare e verificare le conoscenze acquisite.	Il formatore riassume la lezione, incoraggia gli studenti ad approfondire da soli le proprie conoscenze ea partecipare alle lezioni del modulo successivo: "Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete", in cui saranno in grado di espandere le conoscenze acquisite durante questa lezione.	
Quiz di autoapprendimento Apprendimento esteso Consolidamento	- Utilizza un altro modulo in cui imparerai come prevenire il phishing e come rilevare tali frodi - "Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete"	Utilizza un altro modulo in cui imparerai come prevenire il phishing e come rilevare tali frodi: "Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete"	Puoi controllare i link: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf

e quello che raccoglie
l'UNITÀ1 e l'UNITÀ 2 da
questo modulo:

[https://www.youtube.com/
watch?v=NI37JI7KnSc](https://www.youtube.com/watch?v=NI37JI7KnSc)

CASE STUDY
(time: 25
mins)

To acquaint the
learners with the
lesson aims and
results

To introduce the
learners to the topic
of the lesson

To determine by the
learners the type of
data that may be
phished in the
Internet

1. The trainer greets the learners.
2. The trainer defines the lesson aims and presents them to the learners:
 - After today's lesson you will know what data extortion is
 - In today's lesson you will learn the meaning of the word PHISHING
 - You will familiarise yourselves with the different types of phishing methods
3. The trainer acquaints the learners with the lesson plan and its successive stages
4. The trainer asks the learners to think for a moment what data can be requested from the point of view of the person who would like to use them inappropriately. In order to help guide the learners to the topic, trainer can use examples of phishing messages in a printed or electronic form. Then the trainer asks the question "What data do the senders of such messages want to obtain from us?"
5. Brainstorming with the learners- all ideas connected with data are written on the board. Data that may be of

- a set of printed suspicious messages
- a set of suspicious messages in an electronic version
- a projector and a computer with internet access for the trainer

		interest to fraudsters include: name and surname, date of birth, PESEL identification number, ID card number, place of residence, telephone number, electronic banking login details, bank account number, login details for online stores or auction platforms, email login details, usernames and passwords for various websites and social networks, photos. 6. The trainer briefly summarises the collected ideas and engages the learners in the next stage - considering what such data can be used for (e.g. extorting a credit, loan, setting up a fake bank account, making various purchases, setting up fake accounts or a profile on a social networking site, impersonating a given person and writing offensive opinions or comments, entering into false contracts, conducting business activities, forging documents, identity theft).	
Task TRY TO NAME (time: 10 mins)	To define the terms 'data extortion' and 'phishing'	1. The trainer asks the learners to try to sketch the definition of the term 'data extortion' on their own 2. The trainer combines the concept of data extortion with the concept of PHISHING and gives its definition. Exemplary definitions of the PHISHING phenomenon can be found in the book in the chapter assigned to this lesson.	• a projector and computer with internet access for the trainer • work with computers - learners have access to a computer with the Internet connection • To facilitate better and quicker memorisation, the trainer may refer to a YouTube video explaining

			the concept of phishing. Examples: - <i>What is phishing?</i> - https://www.youtube.com/watch?v=BnmneAjVrM4 - https://www.youtube.com/watch?v=hG6XJROw8HY - https://www.youtube.com/watch?v=BzNh-gxosE8
Task ACT (time: 20 mins)	To understand the mechanisms of phishing To find the "'weakest link' To get to know the concept of 'social engineering' To present an overview of the different types of phishing	1. The trainer can divide the learners into groups and send each group a link or give an example of an e-mail printed on a piece of paper that constitutes an example of phishing. With a small number of learners, group work can be replaced with individual work. 2. The trainer asks the learners to look at sample e-mails that were phishing attacks and consider why these attacks are successful. 3. After a short reflection, each group presents their conclusions. 4. The trainer points out that, unlike other online threats, phishing does not require particularly advanced technical knowledge, because criminals do not exploit the technical vulnerability of the device software, but use manipulation techniques called social engineering. It turns out that the	• a projector and computer with internet access for the trainer • work with computers- learners have access to a computer with the Internet connection • Examples of e-mail messages illustrating the PHISHING phenomenon can be found at: - https://its.lehigh.edu/phishing/examples - https://www.phishing.org/phishing-examples

weakest link is a person who doesn't exactly check the origin of the email.

5. The trainer emphasises that phishing attacks consist in triggering certain emotions- fear, anger, curiosity, so as to cause an automatic, quick reaction.
6. The trainer introduces the learners to the concept of 'social engineering'. Sample definition to be found in the e-book.
7. An overview of different types of phishing: the trainer points out that the phishing procedure does not only concern e-mail.
 - Spear phishing - this is a type of attack that targets one institution or person. An attack of this type is profiled, i.e. the attacker collects information about his victim beforehand and only then constructs a message that is to convince the victim to visit a fake website or download a crafted file
 - E-mail cloning- an attack in which the criminal uses a previously sent real message to the user. The attacker copies the genuine message template and places a link to a malicious website in it
 - Redirection to another page- deliberate redirection of users visiting a certain webpage to another, most often fabricated by the stacker
 - Text message and phone phishing- this attack uses text and voice messages, where criminals use special tools

- <https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive>

		to impersonate the phone number of a specific company or send fake text messages	
GOOD PRACTICES (time: 30 mins)	To exchange the learners' own experiences. To summarise and organise the acquired knowledge	1. The trainer asks the learners if they have had any experiences with phishing, if they were a victim of it, or if they encountered this phenomenon in their immediate environment. 2. The trainer, together with the learners, carries out an exercise that gathers knowledge and summarises the work. 3. The learners work in groups (with a small number of learners it can be done individually) 4. The trainer asks the learners to create their own example of a phishing e-mail. They can use examples of such messages from the previous stages. Learners work in text editors or in their e-mail account. In order to organise the work, the learners should consider addressing the following questions: • What could the purpose of phishing data be? • What data would they like to extort? • Where and how could they use this data? • How to formulate an e-mail to make it credible? 5. The learners create their e-mails, present the results of their work, answer the questions posed above and exchange comments with other learners.	• a computer, a projector, access to the Internet • a text editor or an email account

FEEDBACK/ REFLECTION TASK (time: 5 mins)	To revise and verify the acquired knowledge.	The trainer summarises the lesson, encourages the learners to deepen their knowledge on their own and to participate in the lessons of the next module: 'Counteracting and minimising threats and ensuring network safety', in which they will be able to expand the knowledge acquired during this lesson.	
Self-study quizzes Extended learning Consolidation	Use another module where you will learn how to prevent phishing and how to detect such fraud - 'Counteracting and minimising threats and ensuring network safety'	Use another module where you will learn how to prevent phishing and how to detect such fraud - 'Counteracting and minimising threats and ensuring network safety'	• You can check the links: - https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing - https://www2.deloitte.com/content/dam/Deloitte/s/g/Documents/risk/sea-risk-cyber-101-part10.pdf • and the one collecting UNIT1 and UNIT 2 from this module: - https://www.youtube.com/watch?v=NI37JI7KnSc

Il phishing può assumere forme diverse in ogni Paese. I formatori dovrebbero preparare esempi di truffe su Internet a cui gli utenti dei Paesi interessati sono più facilmente esposti.

Per la lezione sono previsti due quiz multimediali.



Quiz 1

Questo quiz può essere utilizzato alla fine della lezione come riassunto di ciò che gli studenti dovrebbero sapere dopo la lezione e può essere svolto insieme, ad esempio su una lavagna interattiva, o individualmente sui loro computer/tablet. Il formatore può anche chiedere agli studenti di fare il quiz a casa come autovalutazione. Il quiz consiste in dieci domande a cui rispondere VERO o FALSO. Il contenuto del quiz con le risposte corrette è riportato di seguito.

- 1) *Il phishing è un attacco mirato a frodare i dati.VERO*
- 2) *Un attacco di phishing può basarsi su messaggi di testo.VERO*
- 3) *Anche la messaggistica istantanea può essere utilizzata per il phishing.VERO*
- 4) *Solo le istituzioni pubbliche sono vittime di attacchi di phishing.FALSO*
- 5) *Gli attacchi di phishing si basano in gran parte su metodi di ingegneria sociale.VERO*
- 6) *I software antivirus proteggono dal phishing.FALSO*
- 7) *Le persone possono fornire liberamente i propri dati su Internet.FALSO*
- 8) *Installare applicazioni da un link contenuto in un SMS è rischioso.VERO*
- 9) *Lo spear-phishing è un attacco mirato a un destinatario specifico.VERO*
- 10) *Solo i computer Windows sono vulnerabili al phishing. FALSO*



QUIZ 2

Questo quiz è anche un riassunto della lezione, che riunisce tutte le informazioni chiave che gli studenti dovrebbero ricordare dalla lezione. Il formatore può visualizzarlo sulla LIM alla fine della lezione o, in alternativa, gli studenti possono visualizzarlo sui loro dispositivi. Può anche essere un breve riepilogo prima della seconda lezione del secondo modulo, in cui i partecipanti impareranno a difendersi efficacemente dagli attacchi di phishing. Di seguito viene presentato il contenuto di questo breve riassunto.

Schermata 1

L'uso di un software antivirus non protegge dai tentativi di phishing.

L'utilizzo di un software antivirus riduce il rischio che il computer venga infettato da virus, ma non protegge dagli attacchi di phishing.

Schermata 2

I tentativi di phishing non avvengono solo tramite e-mail.

Il phishing può avvenire anche per telefono, quando si installano applicazioni da fonti non verificate, attraverso messaggi di testo o chiamate vocali.

Schermata 3

Nel campo del mittente dell'e-mail è possibile inserire un'azienda affidabile.

Ricordate che è facile modificare le informazioni sul mittente nel profilo del client e-mail.

Schermata 4

Le banche e le altre aziende affidabili non chiedono informazioni personali nelle e-mail.

Se si riceve una richiesta di questo tipo, è meglio cancellare immediatamente l'e-mail.

Schermata 5

Tutti i tipi di file contenuti negli allegati possono costituire una minaccia.

Non sono solo i file con estensione .exe a rappresentare una minaccia e non aprite gli allegati delle e-mail se non ne conoscete l'origine.

Schermata 6

Fate attenzione quando fate acquisti online.

Acquistate sempre da aziende, piattaforme commerciali o siti affidabili.

Schermata 7

Le e-mail che contengono link ad altri siti web possono essere più pericolose.

Non cliccate sui link se non siete sicuri del mittente dell'e-mail.

Schermata 8

Ricordate che i vostri dati sono un bene prezioso.

Non inserite i vostri dati, come nome, indirizzo, numero di carta di pagamento o di conto corrente, su siti web casuali.

Lezione 3

-

Privacy online

Il tema della privacy online è una questione essenziale e sempre più affrontata e discussa nell'educazione digitale contemporanea. La privacy è la moneta corrente di Internet e la privacy online di un utente dipende dalla capacità di controllare sia la quantità di informazioni fornite che l'accesso ad esse. Collegandosi a Internet gli utenti entrano a far parte di un enorme database, spostandosi sul web lasciano le loro impronte e utilizzando i social media rivelano essi stessi informazioni della loro vita privata.

Su Internet è difficile proteggere la propria privacy e le informazioni personali. Molti siti incoraggiano gli utenti a condividere informazioni su di sé, non solo il nome, ma anche foto, video, informazioni sul lavoro, interessi, ecc. L'obiettivo principale di questa attività è rendere gli studenti consapevoli del fatto che, pubblicando tali informazioni, le condividono con il mondo intero e che ciò che va su Internet rimane per sempre.

Il modo migliore per proteggere la privacy degli utenti di Internet è quello di educarli. Un ulteriore obiettivo di questi corsi è quello di rendere gli utenti di Internet sempre più consapevoli del fatto che Internet è un luogo pubblico e che devono prendersi cura della loro privacy.

Quando si tiene una lezione sulla privacy, i formatori devono adattarsi al gruppo di studenti con cui lavorano. Di solito, più gli studenti sono giovani, più usano frequentemente siti web, social network o piattaforme di shopping online e più facilmente forniscono i loro dati online. I formatori devono anche tenere presente che ognuno traccia una linea di demarcazione diversa tra ciò che è personale e ciò a cui gli altri possono accedere. I membri del gruppo possono vedere la privacy in modo diverso. Alcuni allievi possono sentirsi a proprio agio nel postare foto di momenti personali sui social network, mentre altri potrebbero considerarlo inappropriato. Per alcuni, condividere informazioni su momenti di vita come un matrimonio non è inusuale, mentre altri non vogliono nemmeno dire il proprio nome. I diversi approcci dei discenti possono essere il punto di partenza ideale per una discussione nel gruppo di formazione. Il formatore può includere questo punto nel programma della lezione.

Anche il diritto alla privacy viene affrontato nel programma delle lezioni. Esiste una legislazione dell'UE sulla privacy, compresa la protezione dei dati personali. Questa include il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Tuttavia, in ogni Paese il diritto alla privacy è regolato da altri atti. Lo scopo del compito della lezione è quello di trovare la legislazione nazionale che regola la privacy. Prima della lezione, il formatore deve preparare le informazioni sulla protezione della privacy nel paese in cui si svolge la lezione. Il formatore può anche utilizzare varie normative di siti web durante la lezione.

MODULO	Tipi e identificazione delle minacce in Internet	UNITÀ DI LEZIONE	3	ARGOMENTO	Cos'è la privacy online?
RISULTATI DI APPRENDIMENTO: - Gli allievi comprenderanno il concetto di diritto alla privacy - Gli allievi conosceranno i vari aspetti della privacy - Gli allievi sapranno cosa significa informazione sensibile e personale					
FASI	OBIETTIVI	PROCEDURA			RISORSE
CASO DI STUDIO discussione (tempo: 15 minuti)	Per familiarizzare gli allievi con gli obiettivi della formazione, discussione sui limiti della privacy.	1. Il formatore saluta gli allievi. 2. Il formatore definisce gli obiettivi della lezione e li presenta ai partecipanti. Dopo la lezione di oggi: • saprai cos'è la privacy • capire perché la privacy è un bene prezioso • cosa significa dati sensibili e dati personali 3. Il formatore fa conoscere agli allievi il piano della lezione con le sue fasi successive. 4. Il formatore fa delle domande di esempio relative a diversi tipi di privacy e chiede agli allievi di giustificare brevemente le loro risposte. • Come ti senti quando qualcuno ti sta troppo vicino? • Come ti senti a toccare un'altra persona senza il suo consenso? • Cosa pensi quando qualcuno mette in giro voci su di te? • Permetteresti a degli estranei di leggere le tue e-mail o i tuoi SMS?			• Computer, proiettore, accesso a internet • Nastro o gesso/ segnapunti

		• Vorresti che altre persone sapessero quali siti web usi o quali pagine navighi su internet? • Vorresti che le tue foto fossero distribuite senza il tuo consenso? • Ti dispiacerebbe se il tuo indirizzo o numero di telefono fosse noto a tutti, anche a persone di cui non ti fidi? • Pensi che i tuoi dati sanitari dovrebbero essere accessibili ad altre persone? 5. Il formatore riassume la discussione e sottolinea che ognuno ha bisogno di uno spazio intorno a sé che appartiene solo ad una determinata persona. Non solo si riferisce all'aspetto fisico, ma anche a vari dati che non vogliamo condividere con altre persone.	
Attività PROVA A NOMINARE (tempo: 10 minuti)	Per nominare i termini: • Privacy • Diritto alla privacy • Dati personali • Dati sensibili	1. Facendo riferimento alla discussione della fase precedente della lezione, il formatore afferma che lo spazio che consideriamo solo nostro può essere chiamato "privacy". 2. Insieme ai partecipanti, il formatore cerca di distinguere i diversi aspetti della privacy. Questo può essere fatto disegnando il diagramma sulla lavagna. 3. La possibile divisione degli aspetti della privacy include quelli relativi a: • contatto fisico • comunicazione - lettura di e-mail, SMS, intercettazione di conversazioni • informazioni su di noi 4. Il formatore spiega che tutti hanno diritto alla privacy nella vita quotidiana. La privacy è protetta dalla legge. 5. Il formatore spiega che ci sono altri due concetti legati alla privacy: dati personali e dati sensibili.	• Computer, proiettore, accesso a internet

		I dati personali possono essere intesi come qualsiasi informazione relativa ad una persona identificata o identificabile (es. nome, cognome, data di nascita). Anche le informazioni individuali che, combinate insieme, possono portare all'identificazione di una data persona, sono trattate come dati personali. I dati sensibili sono un tipo speciale di dati personali, la cui raccolta ed elaborazione è assicurata con regole più severe rispetto all'uso di altri tipi di dati. I dati sensibili includono, tra gli altri, i dati relativi all'origine razziale o etnica, la salute, la sessualità o l'orientamento sessuale, le convinzioni religiose o filosofiche.	
Attività AGISCI (tempo: 20 minuti)	Conoscere le istituzioni e gli atti giuridici che garantiscono il diritto alla privacy.	- Il formatore ricorda che il diritto alla privacy è stato menzionato nella parte precedente della lezione - Il formatore chiede ai partecipanti di trovare: - atti legali che assicurano il diritto alla privacy per tutti - istituzioni che proteggono la privacy Gli allievi possono essere divisi in gruppi che cercano informazioni su atti internazionali (per esempio il Patto internazionale sui diritti civili e politici o la Convenzione europea sui diritti umani), così come informazioni su regolamenti legali nei singoli paesi. Nell'attività, non ci concentriamo sui dettagli degli atti giuridici, ma è importante sottolineare qui che ci sono molte istituzioni che si preoccupano della privacy, e il diritto alla privacy è trattato come uno dei diritti personali e ci sono una serie di regolamenti giuridici relativi a queste questioni. - Gli allievi discutono tutti insieme ciò che hanno trovato su Internet riguardo alla protezione della privacy.	- Computer, proiettore, accesso a internet - Computer per gli allievi
Attività	Mostrare un processo di raccolta dei dati	Il formatore divide gli allievi in squadre di più persone. Ogni squadra sceglie una persona tra di loro. Su un pezzo di carta, gli allievi scrivono alcuni dati (7-10) su questa persona, che sono stati	Computer, proiettore,

ACT (time: 25 mins)	degli utenti e di creazione del profilo digitale degli utenti	resi disponibili su Internet (ad esempio in un motore di ricerca, su Facebook e altri social media, tra cui siti web visitati, musica ascoltata, film visti, opinioni politiche, età, o nome e cognome, se ha commentato vari argomenti da qualche parte, se partecipa a discussioni su forum online, o naviga in pubblicità o negozi online). Dopo aver scritto i dati su un pezzo di carta, questo pezzo di carta viene passato alla squadra seduta vicino. 2. Dopo aver consegnato il pezzo di carta, incaricate le squadre di interpretare il ruolo di impiegati di aziende che si occupano di raccolta dati e, sulla base delle informazioni ricevute, di cercare di descrivere la persona e di pensare a cosa possono servire i dati. Oppure possiamo chiedere quali prodotti potrebbe comprare questa persona. 3. Le squadre presentano i risultati delle loro riflessioni sul forum, e le persone a cui queste descrizioni si riferiscono si rivelano e valutano quale parte di questa descrizione è corretta.	accesso a internet • Fogli di carta, penne
BUONE PRATICHE (tempo: 10 minuti)	Capire che i limiti della privacy variano da persona a persona Capire che la privacy online è un valore	1. Il formatore chiede ai partecipanti: • Cosa non vale la pena di condividere su Internet? • Quali informazioni non vale la pena pubblicare sul web? • Quali informazioni non devono mai essere date in nessun caso? 2. Il formatore indirizza gli allievi a controllare i loro profili sui siti web riguardo a quali dati rendono disponibili pubblicamente e a controllare le politiche di sicurezza di questi siti web.	• Computer, proiettore, accesso a internet
ATTIVITÀ DI FEEDBACK/ RIFLESSIONE (tempo: 10 minuti)	Rivedere e verificare le conoscenze acquisite.	1. Il formatore sottolinea la natura speciale della privacy e dei dati nel mondo digitale. 2. Riassunto della lezione, un ripasso dei concetti relativi alla privacy ancora una volta. 3. Rispondere alle domande degli allievi.	• Computer, proiettore, accesso a internet

		Incoraggiare gli allievi ad approfittare del prossimo modulo su come proteggere la privacy sul web.	
Quiz di autoapprendimento Apprendimento esteso Consolidamento	Utilizza un altro modulo in cui imparerai come prevenire il phishing e come rilevare tali frodi - 'Contrastare e minimizzare le minacce e garantire la sicurezza della rete'.	Per ulteriori informazioni su come prevenire la perdita di privacy in Internet, vedere il modulo: <i>Contrastare e minimizzare le minacce e garantire la sicurezza della rete.</i>	

Un'estensione di questa lezione, che tratta il tema della privacy, è la seguente lezione sull'impronta digitale. Per questa lezione sono previsti due quiz multimediali.



Quiz 1

Il quiz è un riassunto della lezione e riunisce tutti i concetti chiave emersi durante la lezione. In brevi frasi, vengono suggerite le informazioni che gli studenti dovrebbero ricordare dalla lezione. Ci sono diversi modi per lavorare con il quiz. Il primo consiste nel visualizzarlo su uno Schermata e svolgerlo insieme al gruppo alla fine della lezione. La seconda opzione prevede che ogni studente lavori con il quiz in modo indipendente durante la lezione. La terza opzione prevede che il discente torni a leggere il quiz a casa, al termine della lezione, come riepilogo e riassunto della lezione. La quarta opzione prevede che il quiz venga trattato come un ripasso della lezione sulla privacy e come preludio alla lezione successiva sull'impronta digitale. Spetta al formatore decidere come utilizzare questo esercizio interattivo. Di seguito viene presentato il contenuto del quiz:

Schermata 1

Dati personali

- Informazioni su di voi, grazie alle quali è possibile trovarvi e riconoscervi tra gli altri.
- Questo include, ad esempio, nome, indirizzo, numero di telefono, indirizzo e-mail.
- I dati personali sono protetti dalla legge

Schermata 2

Trattamento dei dati personali

- Si tratta dell'esecuzione di operazioni sui dati personali con mezzi automatici o manuali.
- Si tratta, ad esempio, di attività quali la raccolta, l'organizzazione, la sistemazione, la conservazione, la visualizzazione, la diffusione, la cancellazione e la distruzione.
- Esistono norme di legge che regolano il trattamento dei dati personali

Schermata 3

La privacy

- La capacità di mantenere private le informazioni e i dati che riguardano la propria persona.
- Il diritto alla privacy è regolato da diversi atti normativi
- La vostra privacy online dipende in gran parte dalla quantità di informazioni che fornite su di voi.

Schermata 4

Impronta digitale

- Si tratta di informazioni sulle attività online di una determinata persona.
- Si tratta, tra l'altro, di foto, post su forum, blog, social media, informazioni sui siti web visitati dall'utente, ma anche del suo indirizzo IP, informazioni sul suo sistema o sul browser utilizzato.
- Ogni utente di Internet ha un'impronta digitale

Schermata 5

Profilazione

- Un meccanismo utilizzato per classificare gli utenti di Internet in base a caratteristiche, comportamenti e preferenze.
- Può essere osservato, ad esempio, nella presentazione di annunci pubblicitari più adatti alle esigenze di una determinata persona.
- Oltre che per scopi commerciali, il meccanismo di profilazione può essere utilizzato dalle autorità statali per migliorare la sicurezza.



Quiz 2

Il quiz consiste in dieci domande che gli studenti valutano come VERE o FALSE selezionando le caselle appropriate sullo Schermata. Il contenuto del quiz con le risposte corrette è mostrato di seguito. Il quiz può essere utilizzato alla fine della lezione come riepilogo di ciò che gli studenti dovrebbero sapere in seguito e può essere svolto insieme, ad esempio su una lavagna interattiva, o da ciascun studente individualmente sul proprio computer/tablet. In alternativa, si può chiedere agli studenti di fare il quiz a casa come autovalutazione.

- 1) *Su Internet non esiste l'anonimato. VERITÀ*
- 2) *I dati che utilizziamo ogni giorno possono essere usati per causare danni nelle mani sbagliate. VERO*
- 3) *Chiunque utilizzi Internet ha diritto alla privacy VERO*
- 4) *Esistono atti giuridici che tutelano la privacy. VERO*
- 5) *La mia privacy online è protetta anche dalla legge. VERO*
- 6) *È molto facile proteggere la propria privacy e i propri dati personali su Internet. FALSO*
- 7) *È necessario pubblicare con cura le informazioni su di sé. VERO*
- 8) *Su Internet lasciamo molte tracce, anche non del tutto consapevolmente. VERO*
- 9) *Le informazioni personali si limitano a dati quali nome e cognome. FALSO*
- 10) *Se non metto il mio nome e cognome su un forum, nessuno potrà identificarmi. FALSO*

Lezione 4

-

Impronta digitale

Questa lezione si basa sulla precedente sulla privacy online. Gli obiettivi di questa lezione sono di capire che cos'è un'impronta digitale e di rendere gli studenti consapevoli del fatto che i loro dati sono moneta corrente nell'Internet moderno e che non sono gli unici a poter condividere i dati che li riguardano.

Il termine "impronta digitale" ha diversi significati pratici. In teoria, comprende tutto ciò che rimane online dopo le azioni di un utente. Deve essere intesa in due modi: è costituita sia dai dati che lasciamo quando utilizziamo Internet sia dai dati che vengono memorizzati dalle aziende, come il database degli ordini dei clienti o il comportamento del loro sito web. L'impronta digitale viene lasciata più o meno consapevolmente.

I formatori devono spiegare al discente che diverse entità sono interessate ai dati che gli utenti lasciano sul web. Cercano di raccoglierne il più possibile e, a tal fine, tracciano le attività online. A questo scopo vengono utilizzati diversi strumenti.

Un altro aspetto su cui concentrarsi è il profiling. Si tratta di un meccanismo che prevede la categorizzazione delle persone in base a caratteristiche e comportamenti. La profilazione può essere riscontrata nei social network, che registrano l'attività degli utenti per poi presentare pubblicità su misura, così come in vari servizi di libri, musica e shopping. Il loro funzionamento si basa sull'analisi delle decisioni degli utenti e sull'adattamento ad esse dei contenuti proposti. Va notato che questo tipo di profilazione è talvolta utile, ma sempre limitante.

MODULO	Tipi e identificazione delle minacce su Internet	UNITÀ DI LEZIONE	4	ARGOMENTO	Impronta digitale
RISULTATI DI APPRENDIMENTO: - Gli allievi conosceranno e comprenderanno il concetto di impronta digitale - Gli allievi capiranno che le informazioni non possono essere condivise online solo da loro stessi - Gli allievi capiranno chi può raccogliere i dati e per quale scopo - Gli allievi sapranno che le informazioni non possono essere rimosse da internet - Gli allievi conosceranno le conseguenze dell'uso di un motore di ricerca su Internet - Gli allievi sapranno chi può essere interessato alle loro informazioni personali e che tipo di informazioni possono essere desiderate					
FASI	OBIETTIVI	PROCEDURA		RISORSE	
CASO DI STUDIO discussione (tempo: 20 minuti)	Familiarizzazione degli allievi con gli obiettivi della lezione, discussione sulla disponibilità di informazioni su Internet.	1. Il formatore saluta gli allievi. 2. Il formatore definisce gli obiettivi della lezione e li presenta agli allievi. Dopo la lezione di oggi: • Saprai cos'è un'impronta digitale • Capirai quali informazioni vengono condivise su internet e per cosa possono essere usate • Saprai quali entità e organizzazioni possono essere interessate alle informazioni su di te 3. Il formatore fa conoscere agli allievi il piano della lezione e le sue fasi successive. 4. Il formatore pone al gruppo le seguenti domande:		• Computer, proiettore, accesso a internet • Lavagna bianca	

		• Quali informazioni su di te sono disponibili sul web? Scrivi le risposte sulla lavagna. • Quali dati del tuo computer vanno in rete? Scrive le risposte sulla lavagna. 5. Il formatore attira l'attenzione degli allievi (specialmente se non appare nelle risposte) su dati come i dati di geolocalizzazione, l'indirizzo IP del computer, il tipo di browser web, il sistema operativo, il luogo di accesso alla rete, ecc. Il formatore può far notare che i singoli dati inviati alla rete possono non essere di grande importanza, ma quando sono combinati, possono essere una vera miniera di conoscenza sugli utenti. Se i dati non sono registrati sulla lavagna, il formatore li aggiunge.	
Attività PROVA A NOMINARE (tempo: 20 minuti)	Gli allievi sapranno chi può essere interessato alle loro informazioni personali e che tipo di informazioni possono essere desiderate Familiarizzare con il concetto di 'impronta digitale'.	1. Gli allievi dividono le informazioni sulla lavagna in tre categorie: • inviato automaticamente (browser, IP, sistema) • pubblicato semi-automaticamente (posizione, informazioni nelle foto sulla data e l'ora di scatto, il modello di fotocamera) • postati dagli stessi utenti (voci di forum, commenti, e-mail, voci di blog, video di YouTube) 2. Il formatore chiede agli allievi di pensare a quali organizzazioni potrebbero essere interessate alle informazioni sul web. 3. Gli allievi risolvono il quiz - Informazioni in internet 4. Il formatore fa una presentazione che riassume il quiz interattivo e gli allievi riflettono sullo scopo di un potenziale uso delle informazioni.. 5. Gli allievi insieme al formatore spiegano il significato del termine 'impronta digitale'.	• Computer, proiettore, accesso a internet • Lavagna bianca • Computer per gli allievi Quiz interattivo sull'informazione in internet

Attività AGISCI (tempo: 20 minuti)	Gli allievi vedranno quali possono essere le conseguenze della condivisione dei dati e come minimizzarle	1. Il formatore divide i partecipanti in gruppi e distribuisce fogli di lavoro a ciascuno di loro (vedi l'e-book). Il formatore chiede ad ogni gruppo di riflettere sulle risposte ed elencare i comportamenti che limiterebbero la quantità di informazioni divulgate su se stessi sul web. 2. Il formatore chiede ai gruppi di presentare soluzioni. 3. Il formatore riassume l'attività.	• Computer, proiettore, accesso a internet • Lavagna bianca • Fogli di lavoro disponibili nell'e-book
Attività AGISCI (tempo: 10 minuti)	Gli allievi conosceranno le conseguenze dell'uso di un motore di ricerca su Internet	1. Il formatore chiede agli allievi di riflettere su quali domande hanno recentemente inserito nel motore di ricerca e quali informazioni il motore di ricerca può raccogliere su di loro. 2. Il formatore sottolinea che, sulla base delle azioni relative al motore di ricerca - creando domande e inserendo singoli link - Google crea un profilo della persona, sulla base del quale presenta risultati di ricerca su misura per l'utente. Così, può adattare perfettamente le pubblicità che ci vengono mostrate.	• Computer, proiettore, accesso a internet
BUONE PRATICHE (tempo: 15 minuti)		1. Il formatore informa i discenti che possono usare i plug-in del browser per controllare quali entità tracciano la nostra attività, ma non erano siti web che erano stati aperti in precedenza. 2. Il formatore fa conoscere agli allievi i passi grazie ai quali l'informazione inviata a internet può essere limitata.	• Computer, proiettore, accesso a internet
ATTIVITÀ DI FEEDBACK/ RIFLESSIONE (tempo: 5 minuti)		1. Il formatore riassume la lezione. 2. Il formatore ha risposto alle domande dell'allievo. 3. Il formatore incoraggia gli allievi a fare uso del prossimo modulo sulla sicurezza informatica.	• Computer, proiettore, accesso a internet

**Quiz di
autoapprendim
ento**
**Apprendimento
esteso**
**Consolidament
o**

Come parte dell'esplorazione dell'argomento, gli allievi possono guardare il discorso di Gary Kovacs "Seguire gli inseguitori"

<https://www.youtube.com/watch?v=f5wNw-2c0>

o "Come i tracker online ti tracciano e cosa puoi fare" di Luka Crouch

<https://www.youtube.com/watch?v=jVeqAemtC6w>

Per questa lezione sono previsti due quiz e un foglio di lavoro:



Quiz 1

"Informazioni sul web". Quiz interattivo necessario per la seconda fase della lezione. La soluzione del quiz è la base per la discussione con gli studenti e per la definizione congiunta del termine "impronta digitale". Il quiz prevede l'abbinamento dell'entità con i dati a cui potrebbero essere interessati. Di seguito è riportato il contenuto del quiz con esempi di risposte. Questa non è l'unica soluzione corretta. Quando si discute dell'attività, possono sorgere dubbi sulla collocazione dei dati sotto le risposte. Il formatore dovrebbe considerare questo come un punto di partenza per la discussione. Poi gli studenti dovrebbero concentrarsi sulla capacità di giustificare il motivo per cui un ente potrebbe essere interessato a raccogliere dati. Il formatore può chiedere agli studenti quali sono i potenziali motivi per cui alcune entità raccolgono dati.

Domanda 1

Provider Internet	società di marketing che pubblica annunci pubblicitari
1. trasferimento dati	1. storia della ricerca 2. siti web visitati

Domanda 2

amministratore del server	società di marketing che pubblica annunci
3. trasferimento dati 4. Indirizzo IP	5. Video di YouTube visualizzati

Domanda 3

Proprietario del blog	fornitore di servizi di rete mobile
6. i numero di visite al sito web 7. età dei visitatori	8. informazioni sui messaggi di testo inviati 9. ore di telefonate

Domanda 4

sito web con contenuti video	provider internet
10. storia delle ricerche su google 11. storia dei video visualizzati	12. Indirizzo IP

Domanda 5

amministratore del server	sito web con contenuti musicali
13. trasferimento dati	14. ricerca di gruppi musicali 15. guardato i videoclip sul portale di condivisione video

Domanda 6

società di marketing che effettua ricerche di mercato	provider internet
16. articoli visualizzati nelle aste online 17. genere	18. quantità di dati scaricati

Foglio di lavoro da stampare o da esporre alla lavagna.

Quando si lavora con esso, possono emergere risposte diverse. Il formatore deve permettere agli studenti di argomentare e spiegare le loro risposte.

FOGLIO DI LAVORO per la lezione "L'impronta digitale".

Istruzioni: Leggete le storie qui sotto e riflettete sulle risposte alle domande.

- Perché il comportamento descritto nel testo non garantisce l'anonimato?
- Quali potrebbero essere le conseguenze di un simile comportamento per la privacy?
- Nella situazione descritta, come ci si può comportare per non rivelare agli altri tante informazioni su di sé?

Situazione 1

Desiderate condividere con altri le foto della vostra festa di compleanno. Le foto vengono pubblicate su un sito di social network. Le foto ritraggono voi e i vostri amici. Si taggano gli amici. Il vostro profilo è pubblico.

Situazione 2

Al lavoro, non siete d'accordo con le azioni del vostro manager. Secondo voi, il vostro manager organizza male il lavoro del vostro reparto. Su un sito di social network pubblicate un post poco lusinghiero sul vostro manager e sul lavoro in quell'azienda.

Situazione 3

State attraversando un momento difficile della vostra vita: è accaduto un evento triste e difficile per voi. Decidete di cercare aiuto su Internet. Create un account su un portale che offre aiuto psicologico, indicando il vostro nome e descrivendo la situazione nei dettagli.

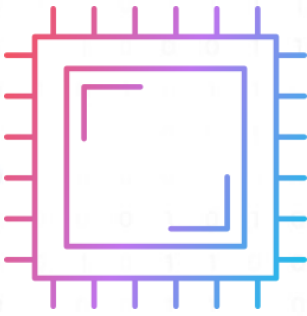


Quiz 2

Un quiz già noto dalle lezioni precedenti, sotto forma di dieci domande alle quali gli studenti rispondono VERO o FALSO barrando le caselle appropriate sullo Schermata. Il quiz con le risposte corrette è mostrato di seguito. Può essere utilizzato alla fine della lezione come riepilogo di ciò che gli studenti dovrebbero sapere dopo la lezione e può essere svolto insieme, ad esempio su una lavagna interattiva, o da ogni studente individualmente sul proprio computer/tablet. In

alternativa, si può chiedere agli studenti di fare il quiz a casa come autovalutazione.

- 1) *Su Internet si è completamente anonimi. FALSO*
- 2) *Nessuno è interessato a ciò che navigo su Internet. FALSO*
- 3) *È difficile prevedere le conseguenze future della pubblicazione di diverse informazioni su se stessi online. VERO*
- 4) *Il provider Internet non raccoglie alcuna informazione sugli utenti del web. FALSO*
- 5) *Il numero IP è un'informazione che viene pubblicata automaticamente sulla rete. VERO*
- 6) *Ho voce in capitolo nel definire la mia impronta digitale. VERO*
- 7) *Tutte le informazioni possono essere efficacemente rimosse dalla rete. FALSO*
- 8) *Il tipo di sistema operativo è un'informazione che viene pubblicata automaticamente. VERO*
- 9) *Il motore di ricerca non ricorda la cronologia delle interrogazioni. FALSO*
- 10) *Non è possibile individuare il luogo in cui utilizzo il computer. FALSO*



MODULO 2

CONTRASTARE E MINIMIZZARE I RISCHIE GARANTIRE LA SICUREZZA DELLA RETE

Ogni volta che gli utenti si collegano a Internet attraverso diversi tipi di dispositivi, sono esposti a pericoli, per cui è essenziale assicurarsi che sappiano come navigare in modo sicuro online.

Nel primo modulo sono stati presentati e identificati i rischi online. I discenti sono già a conoscenza dei diversi rischi e sono in grado di identificarli. Questo modulo intende fornire ai discenti conoscenze e competenze su come contrastare queste minacce. È un'estensione delle lezioni del primo modulo.

Il modulo 2 comprende 4 lezioni su:

1. *come proteggersi efficacemente da messaggi di spam e truffa e da siti web falsi*
2. *come riconoscere efficacemente i messaggi di phishing? Come proteggersi dal phishing*
3. *come prendersi cura in modo efficace della propria privacy e dei propri dati quando si utilizza Internet*
4. *come proteggersi efficacemente quando si usa internet*

Lezione 1

-

Come proteggersi efficacemente da messaggi di spam e truffa e da siti web falsi

Lo spam e le truffe sono minacce online comuni. La lezione del primo modulo ha mostrato come identificare queste minacce. L'obiettivo di questa lezione è di rendere gli studenti consapevoli dei rischi essenziali presenti su Internet e di sviluppare le capacità di riconoscere e difendersi dai messaggi di spam e di truffa.

Prima della lezione, i formatori dovrebbero preparare esempi di messaggi truffa diffusi nei Paesi interessati. Potrebbero essere messaggi di posta elettronica, SMS o di messaggistica istantanea.

MODULO	Contrastare e minimizzare le minacce e garantire la sicurezza della rete	UNITÀ DI LEZIONE	1	ARGOMENTO	Come proteggersi efficacemente da messaggi di spam e truffa e da siti web fraudolenti?
--------	--	------------------	---	-----------	--

RISULTATI DI APPRENDIMENTO:

- Gli allievi comprenderanno l'importanza della consapevolezza dei rischi presenti in Internet.
- Gli allievi sapranno riconoscere i messaggi di spam e di truffa e identificare i siti web fraudolenti.
- Gli allievi sapranno quali strumenti utilizzare per proteggersi da messaggi di spam e truffa e da siti web fraudolenti.
- Gli allievi conosceranno esempi di buone pratiche per proteggersi da spam, truffe e siti web fraudolenti.

FASI	OBIETTIVI	PROCEDURA	RISORSE
STUDIO DEL CASO (tempo: 20 minuti)	Presentazione di esempi di messaggi di spam e truffa e di siti web fraudolenti.	1. Il formatore presenta gli obiettivi della lezione insieme al piano della lezione e spiega agli allievi che durante questa lezione essi: • capiranno quanto sia importante essere consapevoli dei rischi mentre usano Internet, • impareranno a riconoscere i messaggi di spam e di truffa e a identificare i siti web fraudolenti, • conosceranno i metodi e gli strumenti da utilizzare per proteggersi dai messaggi di spam e di truffa e dai siti web fraudolenti,	• la presentazione • proiettore e computer con accesso a Internet per il formatore • set di e-mail di spam, truffa e phishing preparati • Set di siti web e link fraudolenti esemplari.

		• apprenderanno esempi di buone pratiche di protezione contro i fenomeni di spam e scam e i siti web fraudolenti. 2. Il formatore ricorda i concetti di base di spam, scam e siti web fraudolenti. 3. Il formatore presenta serie di e-mail di spam e di truffa ed esempi di siti web fraudolenti. 4. A coppie, i partecipanti classificano i messaggi di posta elettronica come: e-mail normali, spam o truffa. Analizzano inoltre gli esempi forniti e i link a siti web che possono essere classificati come siti fraudolenti. 5. Gli studenti spiegano cosa ha reso un determinato messaggio di posta elettronica o un sito web idoneo per una determinata categoria.	
Attività PROVA A NOMINARE (tempo: 25 minuti)	Gli studenti indicano le caratteristiche delle e-mail di spam e di truffa e le caratteristiche sospette che si possono trovare sui siti web fraudolenti.	1. Il formatore discute con i partecipanti su come i criminali possano usare il nostro stesso comportamento inappropriato quando usano la posta elettronica e navigano in Internet. Il formatore chiede se gli allievi stessi ricevono tali messaggi. 2. Il formatore chiede ai partecipanti di accedere ai loro account di posta elettronica personali e di verificare se tra i messaggi ci sono anche e-mail di spam o di truffa. 3. Il formatore richiama esempi pratici di attacchi informatici basati su e-mail di spam e truffa ed esempi di utilizzo di siti web fraudolenti. Il formatore fornisce i link alle informazioni sugli attacchi in questione.	• la presentazione • lavorare con i computer - i discenti hanno a disposizione computer con accesso a Internet • Esempi pratici di attacchi informatici basati su e-mail di spam e di truffa ed esempi di siti web fraudolenti.

		- Il formatore chiede le caratteristiche delle e-mail di spam e di truffa e come vengono utilizzati i siti web fraudolenti. - Il formatore fornisce statistiche e dati sullo spam negli ultimi anni e sottolinea l'uso di messaggi di spam e di truffa come mezzo per rubare i dati degli utenti di siti web e portali internet e per accedere ai conti bancari online.	statistiche e dati sullo spam negli ultimi anni
Attività AGISCI (tempo: 30 minuti)	Gli studenti acquisiranno familiarità con i metodi e gli strumenti di protezione contro le e-mail di spam e di truffa e i siti web fraudolenti. Gli studenti impareranno a utilizzare gli strumenti presentati durante la lezione.	- Il formatore presenta un'attività che dimostra l'applicazione di metodi e strumenti per la protezione da e-mail di spam e truffa e da siti web fraudolenti. - Il formatore presenta metodi di protezione, tra cui quelli per l'account di posta elettronica, il software di posta elettronica, il browser, l'uso di indirizzi temporanei, nonché i filtri. Il formatore introduce e mostra come utilizzare il software e le impostazioni consigliate. - I partecipanti valutano le soluzioni utilizzate nell'attività. Discussione. - Il formatore discute i singoli elementi dell'attività con i partecipanti, spiegando perché una determinata azione è importante dal punto di vista della protezione contro le e-mail di spam e di truffa e i siti web fraudolenti. - A coppie i partecipanti scelgono il software e i metodi da utilizzare nel loro caso tra quelli presentati	- presentazione - lavoro con i computer- gli allievi hanno accesso a un computer con la connessione a Internet - un'attività preparata che dimostri l'utilizzo di strumenti per proteggersi da e-mail di spam e di truffa e da siti web fraudolenti. - una lista stampata che include i metodi, le procedure e i software raccomandati per proteggersi da messaggi spam e scam e da siti web fraudolenti

BUONE PRATICHE (tempo: 15 minuti)	Gli allievi conosceranno una lista di buone pratiche per la protezione da messaggi di spam e truffa e da siti web fraudolenti.	Il formatore fornisce esempi di buone pratiche per la protezione da messaggi di spam e truffa e da siti web fraudolenti. Distribuisce un elenco di buone pratiche ai partecipanti e discute gli strumenti e i metodi più importanti per contrastare le minacce e gli attacchi informatici su Internet.	• presentazione • una lista stampata di buone pratiche che aumentano il livello di sicurezza informatica quando si usa Internet
ATTIVITÀ DI FEEDBACK/RIFLESSIONE (tempo: 5 minuti)	Domande degli allievi sui temi discussi. Riassunto della lezione.	Il formatore sottolinea la capacità di riconoscere i messaggi di spam e di truffa e i siti web fraudolenti nel contesto di garantire un livello più elevato di sicurezza informatica. Il formatore risponde alle domande dei partecipanti e riassume la lezione.	• presentazione

Il formatore deve fornire ai partecipanti un elenco di buone pratiche per aiutarli a proteggersi da messaggi di truffa e spam.

1. *Non credete ingenuamente che tutto ciò che vedete su Internet sia vero. Rimanete vigili e usate il buon senso.*
2. *Installate strumenti per rafforzare la vostra sicurezza online. Un software antivirus è d'obbligo, ma prendete in considerazione anche altre funzioni di sicurezza.*
3. *Aggiornate regolarmente il software installato sui dispositivi che utilizzate per accedere a Internet.*
4. *Controllare i filtri antispam. Questi vengono creati e configurati dagli amministratori dei server in cui vengono configurati gli account di posta elettronica. Prima di scegliere una particolare piattaforma, verificate quali sono le protezioni anti-spam presenti su quella piattaforma.*
5. *Evitare di registrarsi a servizi non affidabili; fornire il proprio indirizzo e-mail durante la registrazione ad alcuni servizi può portare alla diffusione del proprio indirizzo e-mail e alla ricezione di e-mail di spam.*
6. *Non rispondete a e-mail sospette. Non fidatevi di telefonate o messaggi che vi incoraggiano a investire, soprattutto se non conoscete il chiamante o il mittente del messaggio. Siate sospettosi quando qualcuno vi offre la garanzia di grandi profitti.*
7. *Utilizzate diversi indirizzi e-mail. È possibile utilizzare indirizzi e-mail temporanei per registrare un account su alcuni siti.*
8. *Non condividete mai le vostre informazioni personali.*
9. *In caso di dubbi, contattare i servizi competenti.*

Per la lezione sono stati preparati due quiz interattivi.



Quiz 1

Il quiz presenta le truffe online più comuni. I partecipanti possono familiarizzare con le truffe che possono incontrare online. Il quiz può essere utilizzato come presentazione durante la seconda fase della lezione, in cui il formatore presenta esempi pratici di attacchi informatici. Questo è anche un buon momento per discutere con i partecipanti delle loro esperienze con gli attacchi di truffa. È possibile che abbiano già avuto contatti con questa forma di truffa o che ne abbiano sentito parlare tra i loro familiari o amici. Si dovrebbe anche far notare agli studenti che le vittime degli attacchi sono spesso persone comuni. Di seguito viene riportato il contenuto dell'esercizio online:

Le truffe online più diffuse:

1. Promessa di denaro veloce e acquisti a prezzi stracciati

Questo tipo di truffa inizia spesso con una telefonata, un messaggio sui siti di social network, una messaggistica istantanea o un'e-mail che pubblicizza un lavoro che non richiede una formazione o qualifiche particolari, ma che offre alti profitti in un breve periodo di tempo. Negli acquisti a prezzi stracciati, i criminali spesso usano come esca il prezzo basso di un prodotto o di un servizio offerto per l'acquisto online.

2. Grooming online

I criminali informatici utilizzano conoscenze acquisite di incontri online per ottenere la fiducia della vittima e quindi truffarla di denaro o informazioni personali. Il truffatore spesso instaura una conversazione e poi inizia una relazione online con la vittima. Il truffatore inventa motivi per chiedere alla vittima di consegnare del denaro (ad esempio per spese mediche).

3. Riscatto forzato e minacce

L'estorsione del riscatto è un modo per il truffatore di trattenere informazioni presumibilmente imbarazzanti sulla vita della vittima o di un suo familiare. Spesso, il truffatore ottiene l'accesso a informazioni, foto o video pubblicati sui social media, in modo che la richiesta di riscatto e le minacce inviate diventino reali.

4. Acquisizione di identità sui social network

Oltre alla classica acquisizione di un account di social network, si riscontra anche la clonazione di profili social (ovvero l'utilizzo di nome, foto e informazioni di un account reale per creare un secondo profilo quasi identico da utilizzare nelle truffe pianificate). Spesso il truffatore invia inviti agli amici dalla lista dell'account originale nel tentativo di accedere ai dati di altre potenziali vittime. Il truffatore sfrutta la fiducia degli amici della vittima, ad esempio inviando loro messaggi con link falsi.

5. Negozi online falsi

I truffatori creano negozi online falsi che sembrano autentici o sono copie perfette di siti reali. I prezzi bassi e allettanti dei prodotti offerti dal truffatore sono spesso un'esca. Ciò consente loro di acquisire un gran numero di clienti prima che la truffa venga scoperta.

6. Truffe di phishing

Un truffatore vi invia un messaggio che sembra provenire da una fonte legittima, come una banca, un corriere, un social network o un negozio online. Nel messaggio si ricevono informazioni che richiedono di accedere al proprio account o di fornire dettagli finanziari. Il pretesto può essere che i termini e le condizioni sono cambiati o che è necessario pagare un piccolo extra per l'ordine. L'intero messaggio di phishing è fatto in modo da sembrare urgente e allo stesso tempo facile per la vittima che segue le istruzioni del truffatore senza riflettere.

7. Lotterie e premi attraenti

Si riceve un messaggio dal truffatore via e-mail o sui social media con informazioni su un allettante premio materiale, sulla possibilità di vincere un'ingente somma di denaro, un viaggio gratuito o una ricompensa per aver completato una vaccinazione. La truffa è organizzata in modo tale che per richiedere il premio promesso o partecipare al concorso o alla lotteria sia sufficiente che la vittima si registri e fornisca i propri dati o paghi una piccola somma per le spese di elaborazione, ecc.

8. Distribuzione di software dannoso

Il malware è spesso progettato per scansionare un telefono o un computer alla ricerca di informazioni personali e bancarie, registrare i tasti premuti, bloccare

l'accesso a un dispositivo, accedere a una fotocamera o criptare tutti i dati della vittima. Il più delle volte, la distribuzione del malware inizia con la disattenzione della vittima che clicca su un link falso in un'e-mail, apre un allegato con un virus nascosto o installa un programma da una fonte non attendibile.

9. Falsi servizi di assistenza informatica

Questo tipo di truffa inizia solitamente con annunci di false offerte di servizi relativi a tutti i tipi di assistenza per computer, smartphone e software. Praticamente tutte le forme di questa truffa richiedono alla vittima di installare un software di accesso remoto, consentendo all'autore del reato un accesso praticamente illimitato al computer della vittima.

10. Servizi finanziari falsi

I falsi servizi finanziari comprendono sia false pagine di login per servizi bancari (che comportano tentativi di accesso al conto bancario della vittima) sia false pagine di intermediari di pagamento (ad esempio Paypal, Multibanco, PayU, Nexi). L'attacco avviene solitamente tramite un link (inviato, ad esempio, in un'e-mail o in una messaggeria istantanea) che conduce a un sito falso che mira a impossessarsi del login e della password della vittima.



Quiz 2

Questo quiz introduce i diversi tipi di truffe nigeriane. Gli studenti possono mostrare questo quiz come riassunto della lezione alla fine della lezione o a casa come attività di trivia.

I tipi di truffa nigeriana più comuni riguardano:

1. Ricevere una grande eredità

In questo schema, alla potenziale vittima viene detto che è l'erede di un parente lontano molto ricco che è morto di recente. Per ricevere un'ingente somma di denaro dall'eredità, è necessario pagare solo piccole spese amministrative e giudiziarie. I truffatori descrivono i presunti problemi e incoraggiano la vittima a effettuare pagamenti per accelerare la procedura di eredità.

2. Partecipare a un'asta di oggetti di valore

L'offerta fatta dai truffatori contiene informazioni su un'opportunità unica per la vittima di guadagnare molto denaro. Si suppone che questa opportunità sia una vendita all'asta, ad esempio, di pietre preziose o oggetti d'antiquariato a un prezzo molto interessante. La gara d'appalto, in cui la vittima dovrebbe aggiudicarsi l'asta, si svolge su un sito web falso. Il tempo è fondamentale e i truffatori incoraggiano la vittima a effettuare il pagamento il prima possibile.

3. Un conto bancario senza proprietario

In questo caso di frode, di solito si riceve un messaggio da un impiegato della banca dove c'è un conto con una grossa somma di denaro da trasferire al destinatario del messaggio. Il truffatore ci assicura che il denaro appartiene già a noi, ma che il trasferimento sarà disposto sul conto della vittima dopo aver effettuato un piccolo pagamento per le tasse o le spese bancarie.

4. Vincita di una lotteria o pagamento di un compenso

La vittima riceve la notifica di una vincita alla lotteria o informazioni su un pagamento in attesa di risarcimento. Il truffatore incoraggia la vittima a reclamare il premio (ad esempio, un'ingente somma di denaro o un gioiello) a patto che si faccia carico delle tasse o delle spese di spedizione.

5. Partecipazione a un investimento

Nel messaggio viene presentata l'incredibile opportunità di guadagnare ingenti somme di denaro contribuendo a uno speciale fondo di investimento. Alla vittima vengono promessi alti rendimenti e la garanzia della sicurezza del denaro investito. Spesso l'incentivo a investire si trova nelle storie di altre persone che hanno moltiplicato la loro ricchezza in questo modo.

6. Assistenza a un rifugiato politico

Un rifugiato politico perseguitato dal regime e bisognoso di aiuto scrive alla vittima della truffa. Spesso all'inizio i criminali chiedono piccoli depositi di denaro, ma col tempo le loro richieste aumentano. Nei messaggi emotivi, scrivono della lotta politica e della minaccia alla salute e alla vita degli oppositori del regime per suscitare pietà e incoraggiare la vittima a effettuare ulteriori versamenti di denaro.

come riconoscere efficacemente i messaggi di phishing? Come proteggersi dal phishing

Il phishing è un metodo di frode che consiste nell'impersonare una fonte credibile, come una banca, per estrarre informazioni importanti come i dati della carta di credito, i dati personali o le password di sicurezza; l'attacco viene solitamente effettuato inviando e-mail false.

Gli studenti hanno imparato cos'è il phishing e come funziona nel primo modulo. Ora impareranno a riconoscere i messaggi di phishing e a proteggersi efficacemente dagli attacchi.

Le truffe di phishing più comuni variano da Paese a Paese, quindi il formatore dovrebbe fare delle ricerche sul phishing nel proprio Paese prima della lezione. I truffatori spesso si spacciano per istituzioni pubbliche di fiducia. Per ottenere i dati, si affidano all'anello più debole della protezione, l'essere umano, e invocano il potere dell'abitudine.

MODULO	Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete	UNITA'	2	TEMA	Come riconoscere efficacemente le email di phishing?
RISULTATI DI APPRENDIMENTO: - Gli studenti sapranno come riconoscere un'e-mail di phishing - Gli studenti sapranno come rispondere alle e-mail di phishing sospette - Gli studenti sapranno come riconoscere un messaggio di phishing inviato a un messaggero o tramite SMS / MMS - Gli studenti capiranno l'importanza di verificare il mittente e il contenuto dei messaggi sospetti - Gli studenti sapranno dove cercare strumenti e informazioni per verificare il mittente e il contenuto dei messaggi sospetti					
FASI	OBIETTIVO	PROCEDURE		RISORSE	
ARGOMENTO DI STUDIO (tempo: 15 minuti)	Per presentare e-mail di esempio e messaggi da messaggistica istantanea e SMS / MMS con contenuto di phishing	1. Il formatore presenta gli obiettivi e il piano della lezione e spiega agli studenti che durante questa lezione: - imparare a riconoscere i messaggi di phishing inviati tramite e-mail, messaggistica istantanea o tramite messaggi di testo o mms, - capire come reagire alle e-mail di phishing sospette - comprendere l'importanza di verificare il mittente e il contenuto dei messaggi sospetti - scoprire dove cercare strumenti e informazioni per verificare il mittente e il contenuto dei messaggi sospetti.		• la presentazione • una serie di messaggi sospetti stampati • una serie di messaggi sospetti in una versione elettronica • un proiettore e un computer con accesso a Internet per il formatore	

		- Un promemoria della definizione di phishing e dei suoi tipi, discussa nel modulo precedente. - Il formatore chiede agli studenti di leggere il campione fornito di messaggi di phishing e messaggi regolari, ad es. messaggi pubblicitari. Analizzano i messaggi da soli per circa 5-10 minuti. I messaggi sospetti includono anche messaggi "normali" non minacciosi che gli studenti dovrebbero riconoscere.	
Compito PROVA A NOMINARE (tempo: 15 minuti)	In base alle loro conoscenze, gli studenti devono classificare i messaggi come quelli di natura phishing	- Il formatore chiede le prime osservazioni sul contenuto e sulla forma del messaggio. Commenti degli studenti. - Il formatore chiede loro di qualificare i messaggi a causa del sospetto phishing e dei suoi tipi (phishing, spear phishing, clone phishing, whaling, pharming, SMS / mms phishing, voice phishing). - Analisi del messaggio iniziale moderata da parte degli studenti - Il formatore chiede agli studenti se loro, i loro amici o familiari hanno ricevuto messaggi di phishing simili.	- lavorare con i computer - gli studenti hanno accesso a un computer con Internet - una serie di messaggi sospetti stampati - una serie di messaggi sospetti in una versione elettronica - la presentazione
Compito ATTO (tempo: 45 minuti)	Per rendere gli studenti familiari con i metodi per verificare le e-mail di phishing sospette sulla	Il formatore presenta una checklist di domande che saranno la base per l'analisi dei singoli messaggi in termini di phishing. Le domande in caso di messaggi sospetti di phishing sono alla	- la presentazione - lavorare con i computer

	base di un elenco di controllo. Per consentire agli studenti di valutare e verificare in modo indipendente le e-mail di phishing.	base delle dichiarazioni dei singoli discenti che valutano uno specifico messaggio sospetto. 2. Il formatore discute le domande successive e fornisce esempi che illustrano i problemi di una determinata domanda, ad es. frasi sospette o reindirizzamento di link. Quindi gli studenti verificano se i messaggi forniti all'inizio della lezione hanno una natura di phishing in base alle domande della lista di controllo, quindi effettuano una valutazione e una verifica. 3. Il formatore fa notare agli studenti che tra le domande di controllo ci sono questioni legate all'incertezza sull'identità del mittente del messaggio. Il formatore fa conoscere agli studenti le informazioni riguardanti i dati contenuti nell'intestazione del messaggio e le regole che consentono l'analisi dell'intestazione del messaggio e-mail. 4. Il trainer mostra come controllare l'intestazione del messaggio con l'uso di strumenti di verifica, quindi discute i risultati ottenuti. 5. Gli studenti in coppia controllano le intestazioni dei messaggi ordinari. Il formatore supervisiona l'attività e fornisce supporto. 6. Gli studenti in coppia controllano le intestazioni preparate delle e-mail di phishing. Le coppie presentano e discutono i risultati ottenuti.	• gli studenti hanno accesso a un computer con Internet • un elenco di domande per verificare se si tratta di phishing • un elenco di collegamenti a strumenti che verificano le intestazioni delle e-mail • intestazioni di posta elettronica regolari per gli studenti da analizzare • intestazioni di posta elettronica sospette da analizzare per gli studenti
BUONE PRATICHE (tempo: 7 minuti)	Per far conoscere agli studenti un elenco di buone pratiche contro il phishing.	Il trainer fornisce un esempio di buone pratiche su come proteggersi dal phishing. Distribuisce un elenco di buone pratiche agli studenti e discute i singoli punti.	• la presentazione • l'elenco stampato delle buone pratiche contro il phishing.

CAPITOLO 4

COMPITO DI RISPOSTA / RIFLESSIONE (tempo: 8 minuti)	Revisionare e verificare le conoscenze acquisite.	Gli studenti verificano le conoscenze e le abilità acquisite facendo un quiz.	• la presentazione • lavorare con i computer • i partecipanti hanno accesso a un computer con Internet • link al quiz "Riconosci il phishing?"
Quiz di autoapprendimento Apprendimento esteso Consolidamento	riassumere	Il formatore riassume la lezione.	

Nella terza fase della lezione, il formatore presenta un elenco di domande di screening che costituiranno la base per analizzare i singoli messaggi per verificare l'esistenza di phishing. L'elenco delle domande è riportato di seguito. Tuttavia, se il formatore ha un po' di tempo libero durante la lezione, può incoraggiare i discenti a provare a creare tale elenco. Gli studenti hanno già visto esempi di e-mail e siti web falsi e, sulla base della loro esperienza, possono determinare quali domande si porrebbero se volessero verificare se un messaggio è falso. Il formatore può quindi integrare tale elenco.

Elenco di domande per verificare se si tratta di un caso di phishing:

- 1. Riconosco il mittente dell'e-mail?*
- 2. L'indirizzo e-mail del mittente proviene da un dominio sospetto?*
- 3. Si tratta di un messaggio inaspettato contenente link o allegati?*
- 4. L'e-mail ha un oggetto irrilevante o incoerente con il contenuto dell'e-mail?*
- 5. L'e-mail è una risposta a qualcosa che non ho mai inviato?*
- 6. Il mittente ha incluso un allegato con un tipo di file potenzialmente pericoloso?*
- 7. L'e-mail è insolita, contiene errori grammaticali o di ortografia?*
- 8. Il mittente mi chiede di cliccare su un link o di aprire un allegato che sembra strano o illogico?*
- 9. Il messaggio mi chiede di inserire i miei dati, di accedere al mio conto bancario o a un altro servizio?*
- 10. Il messaggio contiene pressioni per trasferire denaro o pagare una tassa il prima possibile?*

Lo stesso vale per la parte delle attività dedicata alle "buone pratiche". Il formatore potrebbe provare a stilare un elenco con i partecipanti, in modo che le idee per le buone abitudini provengano dai partecipanti stessi. Il formatore può utilizzare il metodo del brainstorming e annotare le idee che emergono nel gruppo. Alla fine, la lezione dovrebbe essere semplicemente riassunta e il lavoro di gruppo completato, se necessario. In alternativa, il formatore può dare ai partecipanti un documento già pronto e discuterne con loro.

Buone abitudini online:

1. *Non aprite mai i messaggi che vi sembrano sospetti. Prestate sempre attenzione al mittente del messaggio e al titolo.*
2. *Fate attenzione se notate errori di ortografia e di battitura in un messaggio ufficiale.*
3. *Non rispondete mai a un'e-mail che vi sembra sospetta. Ignorate le richieste di login e password, di dati personali o di scansione del vostro documento d'identità.*
4. *Non fidatevi dei messaggi di richiesta di denaro, anche se provenienti da amici o colleghi stretti. Ricordate che il loro account potrebbe essere stato violato e usato contro le loro intenzioni.*
5. *Non scaricate o aprite allegati sospetti. Scaricare file da fonti sconosciute è estremamente rischioso.*
6. *Non cliccate mai su link sospetti. Passate sopra il link con il mouse e vedete dove porta. Controllate attentamente l'indirizzo web e assicuratevi che sia sicuro.*
7. *Non inviate via e-mail dati riservati o informazioni sul vostro conto bancario o sulle vostre password.*
8. *In caso di dubbi sull'effettiva provenienza di un messaggio da una determinata società o istituzione, contattate un rappresentante di tale società o istituzione tramite un altro canale di comunicazione o cercate conferma delle informazioni da altre fonti.*
9. *Segnalare all'istituzione competente qualsiasi sito web, e-mail o SMS che possa risultare fraudolento.*

Anche per questo programma di lezioni ci sono due esercizi interattivi.



Quiz 1

Questo quiz sarà un'ottima attività per concludere la lezione. Fornisce collegamenti a risorse in cui gli studenti possono mettere alla prova le proprie conoscenze e competenze sul phishing. Utilizzando i link forniti nell'esercizio, possono verificare se sono in grado di riconoscere o meno un tentativo di truffa di phishing.

Mettete alla prova la vostra capacità di riconoscere il phishing.

1. *Tutti gli attacchi di phishing sono molto simili tra loro. Hanno una cosa in comune: l'uso del fattore umano e dell'ingegneria sociale per ingannare le vittime ignare. Cercate di riconoscere i messaggi sospetti:*

Link alla risorsa: <https://phishingquiz.withgoogle.com/>

2. *Gli aggressori sanno esattamente come scrivere un messaggio per suscitare nella vittima emozioni che la portino ad agire in modo rapido e sconsiderato. I truffatori sono sempre più creativi, quindi possiamo aspettarci un attacco quasi a ogni angolo. Scoprite se riuscite a individuare la minaccia:*

Link alla risorsa: <https://www.phishingbox.com/phishing-iq-test>

3. *I criminali che utilizzano gli attacchi di phishing amano impersonare aziende note, istituzioni finanziarie e autorità. Sapete distinguere tra un messaggio reale e un messaggio di phishing?*

Link alla risorsa: <https://www.sonicwall.com/phishing-iq-test-landing/>



Quiz 2

Questo quiz può essere utilizzato alla fine della lezione. Contiene i nomi di diversi tipi di phishing. Il compito è quello di abbinare il nome alla descrizione dell'attacco. Il contenuto dell'esercizio è illustrato di seguito:

- ❖ *Gli attacchi di phishing sono molto simili tra loro, ma hanno un elemento in comune: l'uso dell'ingegneria sociale che facilita il phishing dei dati delle vittime ignare.*
- ❖ *Gli attacchi personalizzati rivolti a specifici utenti del Web sono particolarmente sgradevoli. Queste attività, note come SPEAR-PHISHING, sono più difficili da rilevare e molto più efficaci perché i truffatori raccolgono dati sulle potenziali vittime e selezionano accuratamente l'obiettivo dell'attacco.*
- ❖ *Una forma comune di attacco consiste nel copiare in modo molto preciso un'e-mail reale, per cullare l'attenzione della vittima e incoraggiarla a cliccare su falsi link che conducono a un sito dannoso. Questa forma è chiamata CLONE-PHISHING.*
- ❖ *Il tipo di attacco personalizzato che cerca di acquisire dati dalle persone più anziane di un'azienda si chiama WHALING.*
- ❖ *Un tipo di phishing che prevede lo spoofing di un dominio o di un numero di telefono. Un criminale informatico che utilizza lo SPOOFING impersona un dominio o un numero di telefono esistente per far sembrare reali le proprie e-mail o telefonate.*
- ❖ *Un attacco che utilizza messaggi di testo o MMS contenenti un link dannoso è classificato come SMISHING.*

Lezione 3

-

Come prendersi cura in modo efficace della propria privacy e dei propri dati quando si utilizza internet

La sicurezza e la privacy online sono due elementi prioritari che vengono per lo più trascurati dagli utenti. I vantaggi dell'utilizzo del web possono far passare in secondo piano le questioni legate alla sicurezza e alla privacy. L'utilizzo di Internet e dei suoi numerosi servizi può essere sicuro, ma è essenziale ricordare una serie di elementi importanti. Un obiettivo chiave di questa lezione è acquisire la capacità di riconoscere i rischi legati alla privacy e ai dati e imparare a proteggere la propria privacy online.

Il formatore può utilizzare il quiz 1 della terza lezione del primo modulo per ricordare agli studenti i concetti di privacy, dati personali e sensibili discussi nel modulo precedente. Per condurre la lezione in modo efficace e illustrare tutti gli aspetti della lezione agli studenti, il formatore dovrebbe preparare in anticipo un account di posta elettronica e un account di social media con i dati di un utente campione.

MODULO	Contrastare e ridurre al minimo le minacce e garantire la sicurezza della rete	UNITA'	3	TEMA	Come prendersi cura della propria privacy e dei propri dati in modo efficace durante l'utilizzo di Internet?
--------	--	--------	---	------	--

RISULTATI DI APPRENDIMENTO:

- Gli studenti sapranno quali dati vengono raccolti quando usiamo Internet.
- Gli studenti capiranno quanto sia importante essere consapevoli dei rischi per la privacy e i dati che lasciamo online.
- Gli studenti sapranno come riconoscere le minacce alla loro privacy e ai loro dati.
- Gli studenti sapranno come proteggere la loro privacy online.

FASI	OBIETTIVO	PROCEDURE	RISORSE
ARGOMENTO DI STUDIO (tempo: 25 minuti)	Per presentare un insieme esemplare di informazioni raccolte su uno specifico utente di Internet	1. Il formatore presenta gli obiettivi della lezione e il programma della lezione e spiega agli studenti che durante questa lezione: - conoscere quali dati vengono raccolti quando usiamo Internet, - capire quanto sia importante essere consapevoli dei rischi per la privacy e i dati che lasciamo online, - imparare a riconoscere le minacce alla loro privacy e ai dati, - apprendere i metodi per proteggere la loro privacy e i dati su Internet.	• la presentazione • un account Google preparato con i dati di un utente esemplare • un account Facebook preparato con i dati di un utente esemplare • un elenco di 98 informazioni che Facebook mette a disposizione degli inserzionisti • un proiettore e un computer con accesso a Internet per il formatore

		2. Ricordare l'ambito del concetto di privacy, dati personali e dati sensibili discusso nel modulo precedente. 3. Il formatore presenta quali dati vengono raccolti dai fornitori di servizi selezionati (Google e Facebook), inclusi: dati sulla posizione, attività nel web e nelle applicazioni, cronologia di ricerca e acquisto. 4. Il formatore presenta un elenco di dati raccolti da Facebook e messi a disposizione degli inserzionisti. Vengono discusse le categorie di dati e le fonti della loro acquisizione.	•
Compito PROVA A NOMINARE (tempo: 25 minuti)	Gli studenti devono elencare quali minacce possono apparire alla privacy e ai dati che divulghiamo su Internet.	1. Il formatore chiede quali sono i rischi associati a così tanti dati che lasciamo sul web. Discussione. 2. Il formatore discute con gli studenti come i criminali possono utilizzare i dati, sia quelli che lasciamo non protetti nella rete, sia i dati rubati, ad esempio, da un attacco di phishing. Il formatore fornisce esempi specifici di utilizzo dei dati da parte di criminali. 3. Il formatore chiede agli studenti di indicare quali dati forniamo più spesso durante la registrazione. Discussione moderata basata su esempi forniti dagli studenti e sulle loro esperienze durante la registrazione, creazione di account sui siti web.	• lavorare con i computer • gli studenti hanno accesso a un computer con Internet gli studenti trovano su Internet la documentazione sull'informativa sulla privacy di siti Web e fornitori selezionati (ad esempio Google, Microsoft, Apple, Twitter, Yahoo, Vimeo, Netflix) • la presentazione

		3. Il formatore introduce i concetti della politica sulla privacy. Insieme agli studenti, analizzano le informazioni che trovano.	
Compito ATTO (tempo: 30 minuti)	Gli studenti devono conoscere il fenomeno della profilazione e cosa fare in caso di fuga di dati.	1. Il formatore presenta il concetto e la procedura del cosiddetto "Diritto all'oblio" e assomiglia alla normativa GDPR. 2. Viene discusso il problema della profilazione dell'attività di rete. 3. Il formatore chiede agli studenti se loro stessi (oi loro amici) sono stati vittime di fuga di dati personali e violazione della privacy su Internet. 4. Il formatore fornisce esempi di fuga di dati e violazioni della privacy e presenta la portata degli attacchi informatici, spesso volti a rubare i dati degli utenti del sito Web e del portale. 5. Il formatore presenta un catalogo esemplare di azioni che dovrebbero essere intraprese dall'utente in una situazione di fuga di dati.	• presentazione di un modello di attività nell'ambito del "diritto all'oblio" • condivisione di link riguardanti fughe di dati degli utenti • presentare un catalogo delle azioni da intraprendere da parte dell'utente in caso di fuga di dati • lavorare con i computer • i partecipanti hanno accesso a un computer con Internet la presentazione
BUONE PRATICHE (tempo: 8 minuti)	Far conoscere agli studenti un elenco di buone pratiche nel campo della privacy e della protezione dei dati su Internet.	Il formatore fornisce un esempio di buone pratiche nel campo della privacy e della protezione dei dati su Internet, nonché distribuisce un elenco di buone pratiche tra gli studenti e discute i punti principali.	• presentazione • un elenco stampato di buone pratiche nel campo della privacy e della protezione dei dati su Internet

COMPITO DI RISPOSTA / RIFLESSIONE

**(tempo: 2
minuti)**

- Per rispondere alle domande degli studenti sulle questioni discusse.
- Per riassumere la lezione.

Il formatore sottolinea la natura speciale della privacy e dei dati nel mondo digitale e risponde a tutte le domande degli studenti. Alla fine, il formatore riassume la lezione.

- presentazione

Per condurre la lezione, il formatore avrà bisogno di altri elementi, tra cui un elenco di 98 informazioni che Facebook fornisce agli inserzionisti sui suoi utenti. L'elenco è molto facile da trovare online e può essere consultato in inglese al seguente link, tra gli altri:

<https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/>

Inoltre, la lezione fa riferimento a un catalogo esemplificativo di azioni che un utente dovrebbe intraprendere in caso di fuga di dati. Definiamo una fuga di dati come un incidente che comporta la divulgazione involontaria o intenzionale di dati. A seconda del gruppo con cui il formatore sta lavorando, i discenti stessi possono proporre le azioni da intraprendere dopo una fuga di dati. È possibile distinguere i tre passi più importanti da compiere dopo essere stati informati di un incidente. Se la perdita ha riguardato le credenziali di accesso, il primo passo è quello di disconnettersi e cambiare la password di accesso, utilizzando se possibile l'autenticazione in due fasi. Il secondo passo dovrebbe essere quello di bloccare i documenti presso la banca e il terzo dovrebbe essere quello di segnalare l'incidente ai servizi competenti.

Buone pratiche di privacy e protezione dei dati online:

1. *Utilizzate password diverse e complesse. Non utilizzate una sola password per più account.*
2. *Compilate con attenzione i moduli web e non fornite mai dati non richiesti.*
3. *Bloccate le app sul vostro telefono per impedirgli di tracciare la vostra posizione.*
4. *Non caricate mai foto compromettenti o intime sui social media. Molte cose restano su Internet per sempre.*
5. *Non lasciate mai i vostri dati su siti web che non hanno una connessione crittografata.*
6. *Cancellare regolarmente la cronologia di navigazione ed eliminare i cookie.*
7. *Limitate l'uso del Wi-Fi nei luoghi pubblici. Non accedete mai alla vostra e-mail o al vostro conto bancario dal computer di qualcun altro.*
8. *Non memorizzate mai dati preziosi e sensibili nel cloud.*
9. *Installate sul vostro computer un software antivirus e di blocco degli annunci pop-up.*

Per la lezione sono previsti due quiz.



Quiz 1

Raccoglie i link alle risorse web dove gli studenti possono verificare se il loro indirizzo e-mail è stato coinvolto in fughe di dati. Il quiz può essere presentato in classe o si può chiedere ai discenti di controllare questi siti a casa ed eventualmente condividere i risultati. Il contenuto del quiz e le risorse in esso contenute sono presentati di seguito.

1. La fuga di dati è una grave minaccia alla nostra privacy nello spazio Internet. Può verificarsi a seguito di un attacco da parte di hacker che violano la sicurezza e accedono al database di un'azienda o di un'istituzione. Purtroppo, capita anche che la fuga di dati avvenga a causa di un errore umano, quando il responsabile della sicurezza non adempie ai propri doveri. I media riportano notizie di ulteriori fughe di dati da siti web o istituzioni. L'entità dei rischi associati alla fuga di dati dal sito può essere facilmente valutata ottenendo informazioni sui maggiori incidenti di questo tipo.

Link alla risorsa:

<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

2. Have I Been Pwned? è un sito web che consente agli utenti di verificare se i loro dati sono stati compromessi in una fuga di dati. Il sito raccoglie e analizza i dati a cui si è avuto accesso in seguito a una fuga di dati e consente all'utente di cercare informazioni sulla fuga dei propri dati dopo aver inserito un indirizzo e-mail o un numero di telefono. L'utente può anche essere avvisato se il suo indirizzo e-mail compare in future fughe di dati.

Link alla risorsa: <https://haveibeenpwned.com/>

3. Firefox Monitor è un sito web che rappresenta una risorsa preziosa per chiunque desideri proteggere la propria sicurezza e privacy. Firefox Monitor vi avvisa se i vostri account di servizi web sono stati esposti a una fuga di dati. Scoprite se le vostre informazioni sono state esposte in una violazione di dati, imparate quali misure adottare per proteggere meglio i vostri account online e come impostare un avviso se il vostro indirizzo e-mail compare in una nuova fuga di notizie.

Link alla risorsa: <https://monitor.firefox.com/>



Quiz 2

Le informazioni contenute in questo quiz mostrano agli studenti quali rischi per la privacy possono comportare i prodotti per la casa intelligente. In molte case ci sono dispositivi elettronici che tutti usano ma non pensano alla sicurezza del loro utilizzo. Il quiz mira a rendere gli studenti consapevoli del fatto che anche l'uso improprio dei dispositivi elettronici domestici può mettere in pericolo la loro privacy. Il quiz può essere utilizzato in classe e visualizzato su una lavagna interattiva, ad esempio. In alternativa, si può chiedere ai partecipanti di riflettere da soli sui pericoli di un particolare dispositivo e poi verificare la loro risposta rispetto alla spiegazione del quiz. Contenuto del quiz:

1. Aspirapolvere intelligente

Spiegazione:

Con l'aiuto di sensori, riproduce la pianta della casa, la sua superficie e le distanze tra mobili ed elettrodomestici. Il dispositivo registra l'attività dell'utente all'interno della casa. I produttori di aspirapolvere hanno annunciato che stanno valutando la possibilità di mettere le planimetrie piatte a disposizione di altri operatori del settore della casa intelligente. Con questi dati, le aziende potrebbero consigliare agli utenti i loro prodotti, ad esempio mobili, prodotti per la pulizia, ecc.

2. Telecamera per la camera dei bambini

Spiegazione:

Ha la funzione di trasmettere video e suoni dalla stanza in cui si trova il bambino. Può anche trasmettere il segnale nella direzione opposta. Con questo tipo di dispositivo, si sono verificati molti casi di fughe di dati e attacchi di hacking a causa della scarsa sicurezza e della mancanza di crittografia dei dati e di aggiornamenti del software.

3. **Uno smart speaker a controllo vocale attraverso il quale comunica un assistente vocale.**

Spiegazione:

I produttori assicurano che l'altoparlante inizia ad ascoltare solo quando l'utente pronuncia una parola chiave. Tuttavia, già nel 2018, un dispositivo ha registrato una conversazione privata dell'utente senza il suo consenso, e la registrazione è stata poi inviata automaticamente a una persona a caso nell'elenco dei contatti. Alcuni produttori offrono una gamma più ampia di servizi offerti dal dispositivo (ad esempio, il controllo del riscaldamento), ma in cambio si aspettano che il partecipante accetti di monitorare continuamente le conversazioni dell'utente per raccogliere feedback sui prodotti e quindi personalizzare meglio i contenuti pubblicitari.

4. **TV intelligente**

Spiegazione:

Per impostazione predefinita, alcuni produttori hanno lasciato delle impostazioni che consentivano al televisore di raccogliere dati su tutto ciò che l'utente guardava. I dati raccolti venivano venduti agli inserzionisti che, attraverso l'indirizzo IP, potevano integrarli con le loro informazioni sugli stessi individui. Si sono verificati anche mancati aggiornamenti del software del televisore, con conseguente esposizione ad attacchi di hacking e, ad esempio, al controllo del microfono e della telecamera.

Lezione 4

-

Come proteggersi efficacemente quando si usa internet

Nell'ultima lezione del secondo modulo, gli studenti impareranno a riconoscere le minacce alla sicurezza informatica, a conoscere i metodi e gli strumenti per aumentare il livello di sicurezza informatica degli utenti di Internet e a conoscere esempi di buone pratiche per aumentare la sicurezza informatica quando si usa Internet. Il formatore può iniziare la lezione spiegando il concetto di sicurezza informatica e ricordando che la sicurezza informatica funziona come la sicurezza tradizionale, ma il suo scopo è quello di mantenere gli utenti e i loro sistemi informatici al sicuro.

La prima fase della lezione si riferisce a un test di autovalutazione della sicurezza informatica online. Il Quiz 1 descritto nel programma della lezione può essere utilizzato come test.

MODULO	Contrastare e minimizzare le minacce e garantire la sicurezza della rete	UNITÀ DI LEZIONE	4	ARGOMENTO	Come garantire efficacemente la tua sicurezza informatica mentre usi Internet?
--------	--	------------------	---	-----------	--

RISULTATI DI APPRENDIMENTO:

- Gli allievi sapranno riconoscere le minacce per l'utente di Internet
- Gli allievi capiranno l'importanza di essere consapevoli dei rischi presenti su Internet
- Gli allievi sapranno quali strumenti utilizzare per aumentare la loro sicurezza informatica su Internet
- Gli allievi conosceranno esempi di buone pratiche per aumentare la sicurezza informatica durante l'uso di Internet

FASI	OBIETTIVI	PROCEDURA	RISORSE
STUDIO DEL CASO (tempo: 20 minuti)	Presentazione del test di autovalutazione della sicurezza informatica di un utente su Internet.	1. Il formatore presenta gli obiettivi della lezione insieme al piano della lezione e spiega agli allievi che durante questa lezione essi: • capiranno quanto sia importante essere consapevoli dei rischi mentre usano Internet, • impareranno a riconoscere le minacce alla sicurezza informatica, • impareranno i metodi e gli strumenti per aumentare il livello di sicurezza informatica dell'utente di Internet e saranno in grado di applicarli, • conoscere esempi di buone pratiche che aumentano la sicurezza informatica quando si usa Internet.	• la presentazione • lavagna bianca • un proiettore e un computer con accesso a Internet per il formatore • preparazione del test di autovalutazione della sicurezza informatica di un utente di Internet

		• Promemoria dei concetti di base sulle minacce di Internet. • Il formatore presenta un test di autovalutazione della cybersicurezza di Internet che permette ad ogni allievo di valutare quali dei suoi attuali comportamenti aumentano il rischio quando usa Internet. • Gli allievi completano individualmente il test di autovalutazione della sicurezza informatica su Internet. 2. Il formatore e gli allievi indicano quali minacce possono essere causate dal comportamento inappropriato descritto nel test di autovalutazione. Il formatore scrive le risposte sulla lavagna nel seguente schema: comportamento inappropriato - minaccia alla sicurezza informatica.	
Attività PROVA A NOMINARE (tempo: 20 minuti)	Gli allievi indicano quali azioni portano a una minaccia alla sicurezza quando si usa Internet.	1. Il formatore discute con gli allievi come i criminali possono usare il nostro comportamento inappropriato per lanciare attacchi informatici. 2. Il formatore chiede agli allievi di indicare quali comportamenti possono proteggere l'utente di Internet dalle minacce elencate sulla lavagna. 3. Il formatore cita esempi pratici di minacce e cyber-attacchi agli utenti di internet, e poi chiede agli allievi di indicare quali misure di sicurezza dovrebbero essere prese quando si usa un computer, uno smartphone, un browser, e-mail, acquisti online e pagamenti, e operazioni bancarie online. 4. Il formatore chiede se gli allievi stessi o i loro amici sono stati vittime di attacchi informatici.	• lavagna bianca • presentazione • esempi pratici di minacce e attacchi informatici agli utenti che utilizzano un computer, uno smartphone, un browser web, la posta elettronica, gli acquisti e i pagamenti online, così come la banca online • statistiche e tipi di attacchi informatici negli ultimi anni

		5. Il formatore discute la portata degli attacchi informatici, spesso mirati a rubare i dati degli utenti da siti web e portali così come l'accesso alle banche elettroniche.	
Attività AGISCI (tempo: 30 minuti)	Gli allievi acquisiranno familiarità con i metodi e gli strumenti per aumentare la sicurezza e la protezione contro gli attacchi informatici. Agli allievi verrà insegnato ad usare gli strumenti presentati durante la lezione.	1. Il formatore presenta un'attività su come garantire praticamente la propria sicurezza informatica e i propri dati mentre si usa Internet. Gli allievi valutano le soluzioni usate nell'attività. 2. Il formatore discute con gli allievi gli elementi particolari dell'attività, spiegando perché una data azione è importante dal punto di vista della sicurezza informatica e della protezione dei dati. 3. Il formatore introduce e dimostra come usare il software consigliato che ci protegge dagli attacchi informatici. 4. A coppie gli allievi scelgono dall'elenco presentato il software e le applicazioni che dovrebbero essere installate sul computer o sullo smartphone di ogni utente di Internet che si preoccupa della propria privacy e vuole essere protetto contro i cyber-attacchi.	• presentazione • lavoro con i computer- gli allievi hanno accesso a un computer con la connessione a Internet • è possibile utilizzare gli smartphone degli allievi con accesso ad Internet tramite Wi-Fi • un'attività preparata su come garantire praticamente la propria sicurezza informatica e i propri dati mentre si usa Internet, incluso l'uso di metodi, procedure e software • uso della directory dal repository https://prism-break.org/pl/all/
BUONE PRATICHE (tempo: 15 minuti)	Gli allievi conosceranno una lista di buone pratiche che aumentano	Il formatore fornisce un esempio di buone pratiche che aumentano il livello di sicurezza informatica quando si usa Internet. Lei/lui distribuisce una lista di buone pratiche agli allievi e discute i metodi più importanti per	• presentazione • una lista stampata di buone pratiche che aumentano il livello di sicurezza informatica quando si usa Internet

CHAPTER 4

	il livello di sicurezza informatica quando si usa Internet.	contrastare le minacce e gli attacchi informatici su Internet.	
ATTIVITÀ DI FEEDBACK/RIFLESSIONE (tempo: 5 minuti)	Domande degli allievi sui temi discussi. Riassunto della lezione.	Il formatore sottolinea l'importanza della capacità di riconoscere e contrastare le minacce utilizzando gli strumenti di sicurezza informatica conosciuti. Il formatore risponde a qualsiasi domanda degli allievi e successivamente riassume la lezione.	• presentazione

Ci sono due quiz per questa lezione:



Quiz 1

Si tratta di un breve test sulla sicurezza online. Il compito del discente è quello di rispondere alle domande del quiz in base al proprio comportamento online. Il quiz sommerà i punti di tutte le risposte e il discente potrà vedere in che misura si prende cura della propria sicurezza digitale. Il quiz deve essere svolto individualmente da ciascun discente sul proprio computer o tablet. È stato progettato per essere visualizzato e svolto nella prima fase della lezione, mentre si introducono i temi della sicurezza informatica. Le domande incluse nel quiz sono le seguenti:

- 1) *Le password per i miei account (ad esempio, computer, account di posta elettronica, siti di social network, siti di aste) sono di solito:*
 - a. *breve e semplice (ad esempio, lo stesso login, la data di nascita, il nome dell'animale domestico, una singola parola)*
 - b. *la stessa password di altri servizi con un numero diverso alla fine, perché utilizzo la stessa password per molti account*
 - c. *lunga, composta da lettere maiuscole e minuscole, nonché da numeri e caratteri non alfanumerici o da una frase lunga, utilizzo una password diversa per ogni account*
- 2) *Accedo a uno dei miei account in un luogo pubblico utilizzando un punto di accesso WiFi pubblico?*
 - a. *molto spesso*
 - b. *a volte*
 - c. *mai*
- 3) *Devo inserire i miei dati reali quando utilizzo le risorse Internet?*
 - a. *sempre quando il sito lo richiede (es. partecipazione a concorsi)*
 - b. *a volte*
 - c. *solo quando è necessario ed essenziale (ad esempio, per fare acquisti)*

- 4) *Utilizzo un programma antivirus sul mio computer con un database aggiornato e le estensioni del browser consigliate per la sicurezza?*
- a. Non utilizzo nessuno dei suddetti strumenti*
 - b. Ne uso alcuni, ma non sempre mi ricordo di aggiornarli.*
 - c. Li uso tutti*
- 5) *Quando qualcuno mi invia un'e-mail, un link o un allegato, lo apro:*
- a. sempre e da chiunque*
 - b. a volte, ma l'e-mail deve essere indirizzata a me direttamente*
 - c. solo se è inviato da un amico e sembra plausibile - in caso di dubbio controllo il link*
- 6) *Sul mio smartphone è installato un programma antivirus:*
- a. no*
 - b. Non lo so*
 - c. sì*
- 7) *Quando si fanno acquisti online:*
- a. Non penso alla sicurezza perché mi preoccupa del tempo*
 - b. Cerco sempre l'offerta più conveniente*
 - c. Cerco di controllare i termini e le condizioni del negozio e le recensioni dei clienti e faccio attenzione a quale sito viene effettuato il pagamento.*

Nel test, per impostazione predefinita, la risposta C è corretta: descrive l'azione ottimale in termini di sicurezza.

Feedback:

21- 19 Siete utenti consapevoli, vi prendete cura della vostra sicurezza su Internet. Potete prendervi cura dei vostri dati e della vostra privacy online, evitate rischi inutili nei punti di accesso WiFi pubblici e proteggete adeguatamente il vostro computer e smartphone. Potete evitare le minacce quando utilizzate le risorse di Internet, ma fate attenzione: dovete essere prudenti perché ogni giorno compaiono nuove minacce informatiche!

18-16 È necessario prestare maggiore attenzione alla sicurezza informatica quando si utilizza Internet. Anche se avete buone abitudini quando utilizzate le risorse di Internet, ci sono situazioni in cui cliccate su un link sconosciuto senza pensarci o dimenticate di aggiornare il vostro software. Sapete molto sulle minacce informatiche, ma potete sempre aumentare le vostre conoscenze a un livello superiore.

<15 I vostri dati non sono al sicuro su Internet. Dovete prestare maggiore attenzione a ciò che cliccate e ai dati che condividete. Dovete lavorare sulla vostra sicurezza in Internet. Siete spesso esposti a minacce informatiche a causa delle vostre azioni. Iniziate a utilizzare le buone pratiche per le minacce informatiche, ad esempio quando utilizzate i punti di accesso WiFi pubblici o aprite gli allegati nelle e-mail.



Quiz 2

Si tratta di un materiale didattico di supporto che il formatore può utilizzare in classe o come risorsa per il discente da svolgere individualmente a casa. Il quiz raccoglie vari strumenti che possono aiutare gli utenti del web a prendersi cura della propria sicurezza. Grazie al quiz, i discenti avranno facile accesso agli strumenti online per aumentare la loro sicurezza informatica. Di seguito è riportato un elenco delle risorse presentate nel quiz:

1. VirusTotal è uno strumento utile per valutare le minacce sotto forma di allegati o link sospetti che arrivano da Internet nelle caselle di posta elettronica. Viene utilizzato sia da privati che da professionisti nella lotta alle minacce informatiche. L'idea alla base è molto semplice: si indica un file sospetto o si incolla un link a una pagina e si riceve un feedback da circa 70 diversi motori antivirus.

Link alla risorsa: <https://www.virustotal.com/>

2. Scoprite come modificare le impostazioni dei vostri servizi online per avere il controllo dei vostri dati e aumentare la sicurezza.

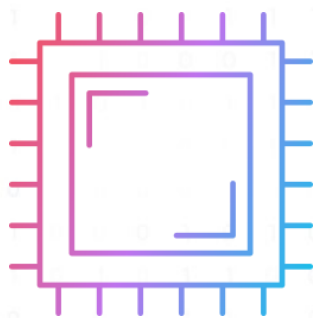
Link alla risorsa: <https://privacy.kaspersky.com/>

3. Verificare la sicurezza della password e la possibilità di decifrarla con un attacco di forza bruta. Inoltre, il servizio consente di verificare se la password utilizzata può essere trovata in un database di password pubblicate.

Link alla risorsa: <https://password.kaspersky.com/pl/>

4. Consultate una guida completa per aumentare la vostra sicurezza e privacy online. Il catalogo comprende anche il software suggerito.

Link alla risorsa: <https://prism-break.org/en/>



MODULO 3

PARTECIPAZIONE ATTIVA ALLA SOCIETÀ
DELL'INFORMAZIONE

La tecnologia offre strumenti di comunicazione sempre più perfezionati e sofisticati. Utilizziamo quotidianamente i siti di social network, vari servizi di messaggistica istantanea e la posta elettronica. I giovani sono più propensi a utilizzare le risorse di Internet rispetto ai mezzi di informazione tradizionali come la televisione, la radio o i libri.

Una società dell'informazione è una società che beneficia di mezzi tecnologicamente avanzati per la raccolta, la ricerca e l'elaborazione di informazioni e comunicazioni. Il termine stesso può essere considerato una sorta di scorciatoia mentale, essendo solo uno dei tentativi di definire le caratteristiche più importanti, i meccanismi di funzionamento e gli effetti dei fenomeni contemporanei legati allo sviluppo delle tecnologie dell'informazione. Non c'è dubbio che lo sviluppo di Internet sia alla base della nascita e dello sviluppo della società dell'informazione. Nella società dell'informazione, le tecnologie dell'informazione sono utilizzate in quasi tutti i settori della vita sociale o personale e il tenore di vita è determinato dall'accesso alle risorse informative.

Le seguenti lezioni sono incluse nel Modulo 3 "Partecipazione attiva alla società dell'informazione":

1. *Identità digitale e media mobili*
2. *Remix - multimedialità libera nella vita di tutti i giorni*
3. *Impegnarsi nella cittadinanza attraverso le tecnologie digitali*
4. *Giornalismo civico, condividere storie nel mondo digitale*

Identità digitale e media mobili

Ogni interazione che avviene in un ambiente digitale fornisce dati sull'attività dell'utente in quell'ambiente, svolgendo un ruolo nella personalizzazione, nel destination marketing, nella reputazione digitale, nei social media e nei servizi grafici. In altre parole, l'impronta digitale lasciata è tanto grande quanto il numero di persone o entità con cui interagiamo online. Il modulo 1 contiene la lezione 4, il cui argomento è proprio l'impronta digitale, un concetto direttamente collegato all'identità digitale. Come introduzione a questa lezione, i discenti possono ricordare i concetti associati all'impronta digitale utilizzando i quiz multimediali assegnati alla lezione 4, modulo 1.

Un'identità digitale può essere definita come l'insieme delle informazioni e dei dati online relativi a una persona specifica e consiste in informazioni/dati quali:

- *Identità digitale e media mobili*
- *Remix - multimedialità libera nella vita di tutti i giorni*
- *Impegnarsi nella cittadinanza attraverso le tecnologie digitali*
- *Giornalismo civico, condividere storie nel mondo digitale*

Gli obiettivi della prima lezione di questo modulo sono la comprensione dell'importanza dei dati personali e del ruolo dei media mobili nella loro produzione e organizzazione, nonché l'acquisizione e l'utilizzo efficace di software dedicati all'organizzazione dei dati personali.

MODULO	Partecipazione attiva alla società dell'informazione	UNITA'	Identità digitale e media sul dispositivi mobili	TEMA	Uso di dispositivi mobili e applicazioni di auto-misurazione e produzione di dati per costruire l'identità digitale.
--------	--	--------	--	------	--

RISULTATI DI APPRENDIMENTO:

- Gli studenti comprenderanno il valore dei dati personali e il ruolo dei media su dispositivi mobili.
- Gli studenti sapranno come utilizzare i sensori multimediali su dispositivi mobili per raccogliere e gestire i dati personali.
- I discenti sapranno acquisire e utilizzare software dedicati all'organizzazione dei dati personali.
- Gli studenti sapranno come organizzare i flussi di dati per ottenere gli obiettivi personali richiesti con i dati.

FASI	OBIETTIVO	PROCEDURE	RISORSE
1 - Caso di studio: "Sé quantificato" (tempo: 15 minuti)	Far conoscere agli studenti l'idea generale della lezione e il suo programma.	Il formatore presenta sinteticamente un caso di studio sotto forma di progetto "Quantified self" e: - spiega il significato socio-culturale del progetto, indicando i contesti di circolazione dei dati in rete, meccanismi di supervisione elettronica e controllo sociale; - indica le tecniche utilizzate nel progetto: le applicazioni e gli strumenti utilizzati (smartphone, smartwatch, notebook, cinturino sportivo), si riferiscono alle loro versioni moderne e alle possibilità che offrono ai propri utenti; - discute le possibilità di digitalizzare i dati per le proprie esigenze sulla base di un caso di studio e allo stesso tempo cerca ulteriori possibilità oltre al materiale analizzato. 1. Il trainer indica e nomina i sensori più diffusi disponibili negli smartphone. A tale scopo, utilizza una	• proiettore & computer

		delle popolari applicazioni che consentono di riconoscere le capacità dei dispositivi mobili e leggere il funzionamento dei sensori in tempo reale - es: per Android e iOS questi saranno: Sensors Multitool, SensorLab e My Device . 2. Gli studenti installano le applicazioni selezionate dal trainer per creare un elenco di sensori disponibili nei loro smartphone e dispositivi mobili. Altri dispositivi mobili associati a uno smartphone possono essere analizzati allo stesso modo. 3. Ogni studente crea il proprio elenco di sensori che possono essere utilizzati, associandoli ai dati che può e desidera trovare per ulteriori analisi. (qui si tratta di un quiz) MULTIMEDIA: a) un grafico informativo dei sensori dello smartphone e delle sue capacità e connessioni b) quiz interattivo che associa sensori selezionati a possibili flussi di dati	
2 – Prova a nominare: nomi e mappature di sensori e flussi di dati (tempo: 25 minuti)	Riconoscere le capacità hardware dei media mobili nel campo dell'acquisizione di dati personali e caratterizzare questo tipo di dati	1. Il trainer indica e nomina i sensori più diffusi disponibili negli smartphone. A tale scopo, utilizza una delle popolari applicazioni che consentono di riconoscere le capacità dei dispositivi mobili e leggere il funzionamento dei sensori in tempo reale - es: per Android e iOS questi saranno: Sensors Multitool, SensorLab e My Device . 2. Gli studenti installano le applicazioni selezionate dal trainer per creare un elenco di sensori disponibili nei loro smartphone e dispositivi mobili. Altri dispositivi mobili associati a uno smartphone possono essere analizzati allo stesso modo.	• proiettore e computer, accesso a Internet, smartphone

		3. Ogni studente crea il proprio elenco di sensori che possono essere utilizzati, associandoli ai dati che può e desidera trovare per ulteriori analisi. (qui si tratta di un quiz) MULTIMEDIA: a) un grafico informativo dei sensori dello smartphone e delle sue capacità e connessioni b) quiz interattivo che associa sensori selezionati a possibili flussi di dati	
3 – Azione: combinare sensori e dati con le app (tempo: 25 minuti)	Per collegare i dati personali con le applicazioni per la loro organizzazione e il loro utilizzo	1. Il trainer presenta le applicazioni selezionate che consentono un'analisi automatica e personalizzata dei dati dai sensori nello smartphone e nelle periferiche connesse. * (Elenco delle applicazioni per l'analisi dei dati personali). 2. A seconda delle proprie preferenze e necessità, ogni studente installa applicazioni selezionate e inizia la raccolta e l'analisi preliminare dei dati raccolti in questo modo. 3. Gli studenti cercano di lavorare con i dati e le applicazioni in modo tale da preparare un breve riassunto di questo tipo di attività e presentarlo al resto della classe alla fine della lezione. Qui puoi seguire le risposte alle domande sui dati che gli studenti vogliono condividere, che non desiderano condividere, quali dovrebbero e quali dati dovrebbero essere puramente privati.	• proiettore e computer, accesso a Internet, smartphone
4 – Condivisione di esperienze e confronto.	Confrontare le possibilità delle attività e discutere i risultati raggiunti	1. Il formatore invita gli studenti a condividere gli effetti del loro lavoro e organizza una discussione attorno a loro.	

CAPITOLO 4

(tempo: 17 minuti)		2. Il formatore presenta ulteriori esempi e buone pratiche che non sono apparsi durante la lezione, ampliando il campo delle possibili attività future.
5 – Riepilogo e feedback (tempo: 8 minuti)	Per riassumere la lezione	Il docente riassume la lezione corrente facendo riferimento ad altre lezioni e moduli, nonché a quiz e materiali multimediali disponibili nell'ambito del progetto.



Quiz 1

Questo è un quiz progettato per essere utilizzato durante le attività degli studenti. Mostra quali sensori si trovano negli smartphone e le possibilità di utilizzo. Nella fase 'Naming' dell'attività, che riguarda i sensori e il flusso di dati, il formatore mostra il quiz ai discenti e questi cercano di individuare le possibilità di utilizzo di un particolare sensore. Di seguito viene presentata una tabella con i sensori elencati nel quiz:

Sensore	Il suo utilizzo
sensori di telecamere disponibili	foto, trasmissioni video, filmati, biometria
GPS	posizione, percorsi, cronologia dei movimenti
Accelerometro	movimento, accelerazione, mobilità
Giroscopio	modalità di applicazione del dispositivo
Magnetometro	orientamento rispetto ai poli magnetici
Sensore di luce	Risposte alla luce ambientale
Microfoni	segnali acustici
Sensore di prossimità	prossimità del dispositivo al corpo
Pedometro	attività corporea
Termometro	variazioni di temperatura
Sensore di umidità	variazioni dell'umidità dell'aria
Sensore di pressione	variazioni della pressione atmosferica
Sensore di impronte digitali	biometria
Touchscreen	modalità touch, biometria
WiFi	localizzazione precisa, monitoraggio dei trasferimenti e delle connessioni
Bluetooth	monitoraggio dei trasferimenti e delle connessioni



Quiz 2

Questo quiz, come il primo, è da utilizzare nella stessa fase della lezione. Si tratta di un quiz a scelta multipla che consente agli studenti di verificare le proprie conoscenze. Consiste nell'individuare le corrette opportunità di acquisizione dei dati in base ai sensori indicati. Il compito del discente è quello di fare clic sul rispettivo sensore e selezionare le opportunità di acquisizione dati per le quali il sensore è responsabile. Di seguito è riportata una tabella con i sensori utilizzati nel quiz e le risposte corrette (contrassegnate da un più).

- Matrici di telecamere disponibili**

1.	Modelli biometrici	+
2.	Modelli comportamentali	+
3.	Informazioni visive sui luoghi	+

- GPS**

1.	Stato di salute	-
2.	Posizione geografica attuale	+
3.	Attività quotidiane	+

- Accelerometro**

1.	Coordinazione dei movimenti nelle dimensioni X, Y, Z	+
2.	Modelli di mobilità	+
3.	Periodi di movimento e di riposo	+

- Giroscopio**

1.	Modelli comportamentali	+
2.	Preferenze di acquisto	-
3.	Dati biometrici	+

- **Magnetometro**

1.	Dati biometrici	-
2.	Preferenze di acquisto	-
3.	Mobilità	+

- **Sensore di luce**

1.	Modelli comportamentali	+
2.	Interazioni sociali	+
3.	Mobilità	-

- **Microfoni**

1.	Conoscenza delle interazioni sociali	+
2.	Profilazione biometrica	+
3.	Profilazione comportamentale	+

- **Sensore di prossimità**

1.	Attività quotidiane	+
2.	Preferenze di acquisto	-
3.	Profilazione biometrica	-

- **Pedometro**

1.	Attività quotidiane	+
2.	Modelli comportamentali	+
3.	Stile di vita	+

- **Termometro**

1.	Dati sulla posizione	+
2.	Profilazione biometrica	-
3.	Preferenze di acquisto	-

- **Sensore di umidità**

1.	Preferenze di acquisto	-
2.	Profilazione biometrica	-
3.	Dati ambientali	+

- **Sensore di pressione dell'aria**

1.	Preferenze di acquisto	-
2.	Profilazione biometrica	-
3.	Dati ambientali	+

- **Sensore di impronte digitali**

1.	Profilazione biometrica	+
2.	Preferenze di acquisto	-
3.	Attività giornaliere interattive	+

- **Schermo tattile**

1.	Attività giornaliere interattive	+
2.	Conoscenza delle interazioni sociali	-
3.	Modelli comportamentali	+

- **WiFi**

1.	Numero e nomi delle reti wireless nelle immediate vicinanze	+
2.	Posizione rispetto ai router WiFi vicini	+
3.	Registrazioni audio e video	-

- **Bluetooth**

1.	Interazioni sociali	+
2.	Trasferimenti di dati	+
3.	Monitoraggio delle periferiche	+

Lezione 2

-

Remix - il multimediale libero nella vita quotidiana

I metodi tradizionali di ricerca di informazioni di interesse online si basano sulla navigazione nel World Wide Web. È importante ricordare che Internet non è fatto solo di siti web, ma è pieno di diversi motori di ricerca, directory, database e altri servizi che permettono ai suoi utenti di cercare informazioni e risorse di vario tipo. Tuttavia, quando si cerca materiale sul web, è importante ricordare che solo una piccola parte di esso può essere utilizzata liberamente. È importante verificare in anticipo a quali condizioni il materiale è stato reso disponibile.

Nelle fasi iniziali della lezione, il formatore può spiegare ai discenti che le risorse aperte sono materiali resi universalmente accessibili, gratuiti e disponibili per l'uso con una licenza aperta. Le risorse aperte possono assumere la forma di testi scritti e parlati, immagini, registrazioni radiofoniche e televisive, animazioni e altri video, test, quiz o giochi, o codici sorgente.

La lezione mira a far conoscere agli studenti il concetto di risorse aperte. Impareranno dove cercare i contenuti multimediali gratuiti, a cosa prestare attenzione quando si utilizzano opere trovate sul web e il ruolo essenziale delle risorse multimediali aperte e gratuite.

L'argomento della lezione utilizza la parola "remix". Il termine può essere associato alla musica, ma qui è usato come tecnica che può essere utilizzata nella creazione di vari materiali. Il remix consiste nel prendere pezzi di lavoro già esistenti (musica, film, grafica, ecc.) e combinarli in modo tale da creare un lavoro completamente nuovo. L'uso di qualsiasi software di fotoritocco, con il quale si può rielaborare una fotografia nel modo immaginato e creare così una nuova immagine, è un esempio di questo fenomeno.

MODULO	Partecipazione attiva alla società dell'informazione	UNITA'	Remix: come ottenere e utilizzare contenuti multimediali gratuiti nella vita di tutti i giorni.	TEMA	Ricerca e utilizzo di contenuti multimediali aperti per uso personale.
--------	--	--------	---	------	--

RISULTATI DI APPRENDIMENTO:

- Gli studenti acquisiranno familiarità con le opzioni di ricerca per le risorse informative multimediali.
- Gli studenti conosceranno i siti web open media più popolari.
- Gli studenti comprenderanno il ruolo culturale delle risorse multimediali aperte e gratuite.

FASI	OBIETTIVO	PROCEDURE	RISORSE
1 – Case study: capolavori d'arte scaricati, remixati e stampati per la tua parete o t-shirt! (tempo: 20 minuti)	Presentare possibilità esemplari per ottenere risorse multimediali legali e gratuite disponibili su Internet.	Il trainer presenta le possibilità di cercare siti Web selezionati che offrono risorse multimediali aperte e gratuite come alternativa all'acquisto di file in archivi di file e risorse piratate. Come introduzione al caso, il formatore utilizza il progetto Rembrandt Remix offerto dal Rijksmuseum. In questo contesto, introduce i partecipanti alla formazione alla disponibilità e alla circolazione delle risorse multimediali su Internet, sottolineando innanzitutto tali circolazioni e ambienti di natura aperta e sociale. Trainer: - indica siti web e servizi che offrono contenuti multimediali ad uso gratuito: film, musica, foto, disegni, modelli (MULTIMEDIA: un'infografica che presenta fonti selezionate di risorse multimediali aperte e legali) - presenta progetti selezionati realizzati con l'utilizzo di social multimedia gratuiti • - ricorda brevemente la possibilità di raccogliere file multimediali sotto forma di raccolta online nonché la	• proiettore & computer

		possibilità di scaricare risorse selezionate sui propri dispositivi digitali sotto forma di file. (MULTIMEDIA: un'infografica che mostra le fasi del processo dalla ricerca all'utilizzo del materiale multimediale)	
2 – prova a nominare: Seguendo parole chiave, argomenti e strutture dati. (tempo: 25 minuti)	Riconoscere possibili tecniche di navigazione tra banche dati Internet che contengono materiali multimediali.	Il formatore divide i partecipanti in coppie. Il loro compito sarà quello di selezionare uno dei database aperti precedentemente indicati contenente multimedia e di navigarvi secondo la tecnica indicata dal formatore. Gli studenti possono scegliere tecniche basate sull'uso di parole chiave, timeline, formato tecnico dei materiali cercati (foto, registrazioni, clip, articoli) o paternità. Ai singoli gruppi viene chiesto di testare tecniche selezionate al fine di spiegare le possibilità che sono state ottenute grazie a loro all'interno di singoli database multimediali. Ogni gruppo svolge questo compito in relazione a 1-2 siti web (es: il gruppo cerca prima le risorse generali di Europea.eu utilizzando il tag piante orientali. Quindi, allo stesso modo, il gruppo cerca le risorse in un museo nazionale di sua scelta , nella raccolta di un'istituzione scientifica, un blog specializzato o un servizio fotografico).	• Computer con accesso a internet
3 – Atto: Crea la tua raccolta multimediale gratuita. (tempo: 25 minuti)	Cercare e raccogliere materiali multimediali per le proprie esigenze.	I partecipanti cercano di lavorare da soli con il multimediale. Cercano, raccolgono e pre-catalogano materiali multimediali da varie fonti aperte e legali per le proprie esigenze. A tal fine, indicano le proprie parole chiave, stabiliscono le esigenze tecniche e fanno una prima selezione di siti web precedentemente noti e cercano altri siti che offrano i materiali necessari.	• Computers

		La raccolta creata in questo modo può assumere la forma di un elenco di collegamenti diretti a file specifici o di un catalogo di questi file archiviati nella memoria del computer.	
4 – Condivisione di esperienze e confronto. (tempo: 15 minuti)	Presentare i risultati della propria ricerca, vantaggi e svantaggi delle soluzioni adottate e condurre una discussione di sintesi.	Ogni studente spiega il proprio modo e i risultati raggiunti concentrandosi su risorse selezionate. Il trainer sta concludendo l'argomento della lezione e i suoi risultati cercando di indicare i pro e i contro delle strategie presentate. Gli studenti sono invitati a commentare e condividere le proprie buone pratiche.	
5 – Riepilogo e feedback (tempo: 5 minuti)	Riassumendo.	Il formatore riassume le lezioni, facendo riferimento ad altre lezioni e moduli, nonché a quiz e materiali multimediali disponibili nell'ambito del progetto.	

Anche per questa lezione sono previsti due quiz, entrambi necessari per lo studio del caso fornito in questa lezione.



Quiz 1

Il quiz raccoglie i link a varie risorse web gratuite. L'utente clicca su ogni categoria e gli vengono presentati i siti gratuiti che forniscono contenuti appartenenti alle categorie indicate.

categoria	risorse
Creatori	Le risorse più numerose ma anche le più disperse sono quelle creati e resi disponibili da singoli creatori. Si possono trovare, ad esempio, su siti che raccolgono e promuovono il loro lavoro. jamendo.com, Flickr.com, medium.com
Comunità	Un ruolo importante nella ricerca di risorse rilevanti può essere svolto dalle comunità di fan, che consultano le fonti online, indicizzano le risorse disponibili e le curano per sé e per gli altri. Thenounproject.com, openculture.com, deviantart.com
Istituzioni	Un numero crescente di istituzioni culturali, artistiche, mediatiche e digitali sceglie di rendere disponibili le proprie collezioni in formato digitale ad accesso libero. www.metmuseum.org, www.europeana.eu
immagini	Flickr.com, Thenounproject.com, pixabay.com
film	pexels.com, vimeo.com, adobe.com
suoni	jamendo.com, soundcloud.com, spotify.com
testi	openlibrary.org, otwartelektury.pl, www.gutenberg.org



Quiz 2

Si tratta di un quiz intitolato "Dal bisogno al remix - come trovare e utilizzare risorse multimediali aperte" e di un'infografica interattiva che illustra come reperire risorse multimediali libere, aperte e legali. I passi successivi sono presentati sotto forma di icone e l'utente fa clic su di esse sullo schermo per passare alle fasi successive dell'esercizio. Contenuto del quiz:

1. *Un'idea - Avete un'idea per un vostro video, un proclama, una presentazione multimediale, un clip audio, una playlist, un articolo o altri semplici progetti multimediali? Potete prepararli sulla base di materiali acquistati da banche di immagini, clip e contenuti, oppure provare a fare lo stesso utilizzando risorse legali e modelli disponibili gratuitamente sul web sulla base di varie licenze.*
2. *Un'esigenza: forse avete bisogno di foto, canzoni, videoclip o materiale grafico vettoriale. Tali risorse possono essere facilmente ottenute dai creatori stessi, da istituzioni aperte o con l'aiuto di comunità di fan. Se sapete cosa state cercando, l'elenco dei servizi specializzati è molto lungo.*
3. *Ricerca - Raccogliere, etichettare e organizzare le risorse per il proprio uso. Quando raccogliete i materiali, assicuratevi di scegliere quelli che sono liberi da obblighi finanziari. Cogliete l'occasione per informarvi sulle licenze legali alternative a quelle dominanti che determinano le possibilità di utilizzo delle risorse - Imparate a conoscere le licenze Creative Commons - Creative Commons Polska.*
4. *Produzione - per modificare i vostri contenuti potete utilizzare non solo risorse multimediali aperte e gratuite. Dovreste anche utilizzare software e servizi digitali per produrre contenuti multimediali gratuitamente. La maggior parte dei programmi commerciali costosi e complicati hanno i loro equivalenti gratuiti e open-source. Vedi per cominciare - Top 10 Alternative gratuite a software costosi (lifehacker.com)*
5. *Pubblicazione e diffusione - anche per quanto riguarda la messa online dei contenuti completati e l'attrazione degli spettatori, vale la pena di utilizzare alternative alle opzioni a pagamento. Potete sempre inserire il vostro lavoro su quei portali e servizi gratuiti che avete utilizzato durante la fase di ricerca. In questo modo restituirete alla comunità ciò che avete guadagnato grazie ad essa. Si vedano, per cominciare, le 10 migliori alternative gratuite a software costosi (lifehacker.com), i 10*

migliori siti di hosting video gratuiti per privati e aziende online (wondershare.com).

6. *Sinergie di feedback: potete contare sul fatto che qualcuno sia interessato al vostro lavoro. Di conseguenza, inizierà a entrare nel mondo digitale e a diffondere la sua influenza. Forse non accadrà immediatamente e la portata non sarà grande all'inizio, ma certamente le reazioni alla sua presenza nella rete globale del flusso di informazioni vi daranno un feedback interessante su ciò che avete fatto e su come lo avete fatto.*

Lezione 3

Impegnarsi nella cittadinanza attraverso le tecnologie digitali

La realtà virtuale è parte integrante della vita moderna. Non si tratta solo del tempo trascorso davanti allo schermo di un computer, ma anche davanti agli schermi dei telefoni e persino degli orologi. In questo modo, il mondo digitale si sta fondendo con quello reale. Anche il modo in cui la società civile viene costruita e sviluppata sta cambiando. Le competenze civiche necessarie nella società dell'informazione si basano in larga misura sulle abilità mediatiche e sulle competenze tecniche pratiche.

I media elettronici stanno cambiando il modo di comunicare delle persone. La comunicazione online integra le interazioni tradizionali e i social media, in particolare, offrono l'opportunità di raggiungere un'ampia gamma di utenti di Internet. I social network e i media elettronici forniscono ai cittadini e alle istituzioni una serie di strumenti per condividere informazioni e organizzarsi. Forniscono un mezzo con cui ogni persona può esprimere la propria opinione e protestare, contribuendo così ad aumentare il coinvolgimento dei cittadini nelle questioni sociali, amministrative o politiche.

Molti utenti di Internet partecipano a vari servizi online o utilizzano diversi strumenti online (forum, chat room, gruppi, messaggistica istantanea, giochi online). Questo li mette in contatto con altri utenti di Internet e crea una comunità basata su caratteristiche comuni, come interessi, opinioni politiche, lavoro, problemi sociali o di salute.

Grazie a questa lezione, gli studenti apprenderanno le possibilità di impegnarsi in varie attività civiche attraverso le tecnologie digitali, comprenderanno il ruolo e l'importanza dei progetti di attivismo condotti nell'ambiente digitale e saranno in grado di interpretare criticamente le attività nell'ambiente dei media digitali.

MODULO	Partecipazione attiva nella società dell'informazione	UNITÀ DI LEZIONE	3	ARGOMENTO
				Impegnarsi in attività civiche attraverso le tecnologie digitali

RISULTATI DI APPRENDIMENTO:

- Gli allievi avranno familiarità con le varie possibilità di impegnarsi in attività civiche attraverso le tecnologie digitali.
- Gli allievi comprenderanno il ruolo e l'importanza dei progetti attivisti realizzati nell'ambiente digitale.

FASI	OBIETTIVI	PROCEDURA	RISORSE
STUDIO DEL CASO: attività civiche nel mondo digitale (tempo: 20 minuti)	Presentazione e discussione del concetto di attività civica realizzata con l'uso delle tecnologie digitali. Facendo riferimento all'idea di cittadinanza digitale e un'analisi preliminare di esempi selezionati.	Il formatore introduce il tema della cittadinanza digitale facendo riferimento alle categorie di rivoluzione digitale, società civile, sfera pubblica elettronica, stato aperto e democrazia. In questo contesto, il formatore indica le attività civiche esistenti e i progetti intrapresi dalla società civile con l'uso delle tecnologie digitali e dei siti di social networking. La generazione sociale, l'elaborazione e l'uso di dati- memoria dei luoghi e risorse storiche, attivismo civico, monitoraggio delle attività delle infrastrutture.	proiettore e computer MULTIMEDIA: una compilation di azioni sociali iconiche, di successo e non, realizzate nell'ambiente digitale MULTIMEDIA: infografica che presenta le direzioni dell'impegno civico attraverso i media digitali e il web

PROVA A NOMINARE: Forme di impegno digitale e modi di progettare azioni civiche. (tempo: 20 minuti)	Discussione delle possibilità e dei limiti legati all'uso di varie forme di coinvolgimento nell'attivismo digitale. Panoramica dei metodi funzionali di funzionamento: app, format di scambio di informazioni, così come standard esistenti per la circolazione di informazioni e dati.	Il formatore divide i partecipanti in squadre di tre persone. Il compito di ogni squadra è quello di tentare un'analisi approfondita di un esempio tra quelli discussi in precedenza. Gli allievi devono scrivere la sequenza delle attività intraprese nel progetto discusso e valutare l'efficacia della selezione di strumenti specifici, formule e regole di comunicazione. Elementi importanti da prendere in considerazione qui sono la copertura delle attività e la costruzione di comunità di rete e di relazioni inclusive intorno ad esse, utilizzando vari canali di comunicazione e risorse digitali disponibili - multimedia, dati, siti web e servizi pubblici e commerciali, così come la loro generazione.	• Computer con accesso a Internet
AGISCI: Progettare un piano di attività civica per aiutare a comunicare un problema locale e costruire una rete sociale intorno ad esso. (tempo: 30 minuti)	Progettare attività civiche in un ambiente digitale.	Gli allievi affronteranno la sfida di progettare uno schema generale per possibili attività di comunicazione nell'ambiente digitale. In gruppi di diverse persone che condividono interessi, idee o bisogni comuni, cercheranno di ideare uno scenario per un'azione volta a pubblicizzare il problema, costruire comunità di rete e un forum per lo scambio di opinioni intorno ad esso, raccogliere le risorse digitali necessarie - multimedia, app e dati.	• Computer
BUONE PRATICHE Condivisione di esperienze e discussione. (tempo: 15 minuti)	Presentazione dei risultati del lavoro del progetto e discussione successiva.	Ogni compagno di classe spiega il suo modo e i risultati ottenuti concentrandosi sulle risorse selezionate. Il formatore sta concludendo l'argomento della lezione e i suoi risultati cercando di evidenziare i pro e i contro delle strategie presentate. Gli allievi sono invitati a commentare e a condividere le loro buone pratiche.	

In the first stage of the lesson, i.e. a case study, the use of two multimedia quizzes is planned.



Quiz 1

Cosa possiamo fare insieme con l'uso dei media? Un quiz che raccoglie varie azioni sociali di successo e non, realizzate in un ambiente di rete. Mentre l'utente clicca sulle icone, il quiz mostra entrambe le azioni in diverse categorie e gli esempi corrispondenti:

Blockchain - uno dei modi più popolari di operare nelle reti sia al di fuori delle aziende che della supervisione statale. Ogni membro di una comunità online autentica gli eventi in questa rete annotandone l'esistenza e memorizzandoli sotto forma di certificato digitale. La regola della blockchain è stata utilizzata per creare valute digitali circolanti (Bitcoin), certificati digitali di unicità (NTF) o per confermare identità digitali (identità digitale).

Applicazioni - le persone collaborano tra loro attraverso i media elettronici non solo per risolvere problemi attuali. Molti di loro sono coinvolti in progetti che danno vita a strumenti per altri, basati sulla logica del codice aperto e della facile disponibilità e che, nella maggior parte dei casi, rimangono gratuiti anche per l'utente medio, non commerciale. Esempi: LibreOffice, una suite di applicazioni per ufficio gratuita, Firefox un browser web aperto, o SETI@home, una ricerca volontaria di vita extraterrestre.

Banche dati - anche la raccolta e l'organizzazione dei dati sulla base del bene comune portano effetti molto tangibili. Esistono numerosi esempi di coinvolgimento dei cittadini in progetti finalizzati alla costruzione e alla condivisione di banche dati dedicate a diversi campi della conoscenza. Esempi: OpenStreetMap o la mappa del mondo, o molti progetti della famiglia wiki, come WikiMedia dedicato alla raccolta di risorse educative.

Crowdsourcing - ovvero il finanziamento comunitario di iniziative, attività o organizzazioni selezionate tramite applicazioni o siti web. In questo modo, i cittadini possono cofinanziare direttamente eventi necessari e, a loro avviso, di valore. Esempi (con finanziamenti record): una serie sulla vita di Gesù (The Chosen), o un progetto comunitario legato al ricordo della guerra (Europeana 1914-1918).

Forum e gruppi di discussione - una delle forme più note e comuni di attività civica che coinvolge i media digitali. Per molti utenti di questi media è ancora la forma più accettabile e conveniente di impegno. Esempi: Ushahidi -

un'applicazione e una piattaforma per la collaborazione in caso di eventi di crisi, o OpenIDEO per lo scambio di opinioni e la formazione di idee insieme.

Giornalismo di base - i giornalisti e i media spesso non sono in grado di svolgere autonomamente il necessario lavoro di ricerca. Spesso le istituzioni mediatiche non riescono a coprire gli argomenti a causa di vari vincoli, interessi e giochi politici. Questo è un campo eccellente per i giornalisti dilettanti e i progetti mediatici comunitari. Esempi: collaborazione della comunità su materiale giornalistico d'inchiesta (Guardian), o un giornale locale curato e pubblicato dalla comunità locale (Fitzrovia News).



Quiz 2

Prima di mostrare questo quiz, a seconda del gruppo di partecipanti e del tempo assegnato alla lezione, il formatore può chiedere ai partecipanti le loro esperienze di impegno civico online e le indicazioni per il suo sviluppo. Questo quiz può essere considerato un riassunto della discussione che emergerà tra i partecipanti. Mostra diverse direzioni per l'impegno civico utilizzando i media e le reti digitali. Non si tratta di tutte le direzioni possibili, ma solo di esempi. I partecipanti possono aggiungere le loro idee.

Comunità locali - rafforzamento dei legami, progetti di base, monitoraggio dei cittadini

Comunità sparse - collaborazione attraverso il tempo e lo spazio, circoli di influenza, articolazione delle idee

Attivismo politico - controllo delle élite politiche, scambio di idee, software e servizi elettronici

Giornalismo cittadino - oltre il mainstream, dibattito locale, collaborazione comunitaria

Raccolta di dati - database aperti, controllo sociale dei dati, memoria collettiva

Lezione 4

-

Giornalismo Civico. Condividere storie nel mondo digitale

Il Giornalismo Civico o citizen journalism può essere inteso come un tipo di giornalismo praticato da giornalisti non professionisti nell'interesse pubblico. Il più delle volte questa attività è legata allo sviluppo di Internet e, in particolare, all'emergere di siti di notizie online i cui contenuti sono creati o co-creati dagli utenti di Internet. Oggi sono possibili varie forme di citizen journalism, ad esempio la pubblicazione di testi o immagini sui propri siti di notizie o su piattaforme esistenti, oppure la scrittura di un blog.

L'obiettivo di questa lezione è esplorare le condizioni di base per la creazione e la pubblicazione di informazioni in ambiente digitale, comprendere le opportunità e i vincoli che si presentano nelle varie fasi della comunicazione di progetti informativi in ambiente digitale e acquisire le competenze necessarie per selezionare gli strumenti adatti all'ambiente digitale.

Il formatore deve prestare particolare attenzione ad alcuni aspetti del citizen journalism, che comporta sempre la responsabilità per i contenuti pubblicati. I contenuti devono essere veritieri, affidabili e verificati. Sebbene ogni testo contenga il punto di vista dell'autore e sia quindi soggettivo, è comunque necessario essere onesti con le persone descritte. I citizen journalist sono anche responsabili dell'impatto che avranno con il loro testo. Bisogna essere consapevoli delle possibili conseguenze della pubblicazione di un test. Anche se tutte le informazioni fornite sono verificate e colte in modo corretto, la loro pubblicazione può talvolta avere conseguenze negative, che dovrebbero essere anticipate dall'autore del testo.

Il citizen journalism riunisce diverse attività, come esporre o evidenziare i problemi della comunità locale, scrivere reportage su eventi e luoghi interessanti e sconosciuti, descrivere personaggi interessanti e scrivere testi giornalistici o di divulgazione scientifica.

MODULO	Partecipazione attiva nella società dell'informazione	UNITÀ DI LEZIONE	4	ARGOMENTO	Giornalismo cittadino- condividere storie nel mondo digitale Strumenti di comunicazione di base e regole per il giornalismo cittadino.
---------------	--	-------------------------	----------	------------------	--

RISULTATI DI APPRENDIMENTO:

- Gli allievi conosceranno le condizioni di base per creare e pubblicare informazioni nell'ambiente digitale.
- Gli allievi comprenderanno le possibilità e i limiti che si presentano nelle diverse fasi di comunicazione dei progetti di informazione nell'ambiente digitale.
- Gli allievi saranno in grado di scegliere un set di strumenti adeguati all'ambiente digitale.

FASI	OBIETTIVI	PROCEDURA	RISORSE
STUDIO DI CASO: Giornalismo cittadino: idee, strumenti, pratiche (tempo: 20 minuti)	Presentazione dell'idea di giornalismo civico e discussione sulla circolazione dell'informazione in condizioni digitali.	Il formatore introduce il tema del giornalismo civico, indicando le differenze con il funzionamento delle istituzioni dei media professionali, gli svantaggi e i vantaggi di questo modello di funzionamento e presentando gli esempi più famosi in questo settore. Il formatore continua a discutere un possibile workshop per un giornalista cittadino, indicando gli strumenti e le piattaforme per lavorare sul contenuto, renderlo disponibile nella circolazione della rete e costruire una base ambientale per esso. Nell'introduzione, il formatore fa riferimento a categorie come dibattito pubblico, reportage, raccolta di informazioni, ricerca di informazioni e dati aperti, nonché giornalismo collaborativo.	proiettore e computer MULTIMEDIA: infografiche che dimostrano le fasi che vanno dalla raccolta dei dati, attraverso la progettazione di informazioni per introdurle nella circolazione della rete e costruire una portata dei social media per esso MULTIMEDIA: infografiche che presentano una raccolta delle più popolari, strumenti accessibili per il giornalismo cittadino.

PROVA A NOMINARE: Fasi di progettazione e comunicazione di contenuti giornalistici in un ambiente digitale. (tempo: 20 minuti)	La specificità dei compiti e delle fasi del lavoro dei giornalisti cittadini sulla base dell'analisi dei casi studio.	Il formatore divide gli allievi in tre squadre. Il compito di ogni squadra sarà quello di identificare i componenti di ogni fase del flusso dei contenuti, i suoi requisiti e le sue limitazioni. Agli allievi viene chiesto di scrivere la sequenza delle attività intraprese in tre fasi individuali dei progetti indicati - casi di studio e di valutare l'efficacia della selezione di strumenti specifici, formule e regole di comunicazione. La prima squadra si occuperà della fase di raccolta delle informazioni e della strutturazione del messaggio - i metodi e le condizioni di acquisizione delle conoscenze, la verifica della credibilità e dell'utilità delle informazioni, la creazione di semplici messaggi mediatici. La seconda squadra si concentrerà sulle possibilità di diffusione dell'informazione civica e analizzerà le piattaforme mediatiche per la distribuzione dell'informazione, oltre a indicare i canali più efficaci in casi specifici. La terza squadra deve analizzare l'efficacia comunicativa delle strategie giornalistiche selezionate. I membri del team cercheranno di rispondere alle domande su quanti destinatari hanno raggiunto e quanto successo ha avuto la diffusione del contenuto selezionato. C'è stato un cambiamento nello stato delle cose grazie ad essa?	• Computer con accesso a Internet
AGISCI: Progettiamo un evento informativo dal basso verso l'alto. (tempo: 30 min)	Progettare uno scenario completo di un'azione nello spirito del giornalismo civico.	Divisi in due gruppi, gli allievi affronteranno la sfida di creare uno scenario generale volto a diffondere il contenuto in un ambiente digitale. Nella discussione, il gruppo identifica un problema che richiede pubblicità nell'ambiente di rete e cerca di scegliere i modi più appropriati di procedere in particolari fasi della sua comunicazione. Come risultato di questa riflessione, viene creato uno scenario che definisce le regole generali di	• Computer

		funzionamento, gli strumenti necessari, la durata, le spese e le risorse necessarie.	
Riassunto e discussione (tempo: 15 minuti)	Discussione che riassume i risultati del lavoro del progetto.	I gruppi presentano le ipotesi dei loro scenari e insieme analizzano i loro vantaggi e svantaggi.	
Riassunto e feedback (tempo: 5 minuti)	Riassunto	Il formatore riassume la lezione facendo riferimento ad altre lezioni e moduli così come a quiz e materiali multimediali disponibili nell'ambito del progetto.	

Anche per questa lezione vengono fornite due risorse multimediali da utilizzare nella fase di studio dei casi.



Quiz 1

Questo quiz illustra le fasi dall'idea alla realizzazione. È stato progettato per essere utilizzato in classe, ma grazie alla disponibilità di tutto il materiale sulla piattaforma, gli studenti possono tornarci in qualsiasi momento. Il quiz può essere visualizzato sulla lavagna interattiva o può essere svolto da ciascun discente in modo indipendente. Include le fasi di lavoro per la creazione di materiali di citizen journalism. I discenti cliccano sui nomi delle fasi e familiarizzano con il loro ruolo.

Messaggio - La cosa più importante è quello che volete dire; idealmente se avete un argomento preciso, informazioni interessanti da trasmettere e volete convincere un pubblico specifico del vostro punto di vista. Pensate alle informazioni che volete trasmettere e alla forma di racconto che adatterete. Avrete bisogno di una sceneggiatura, di dati in forma grafica e di materiale grafico come foto, icone e grafici.

Ricerca - Sapete già cosa volete dire e cosa dovete convincere il vostro pubblico. La storia deve essere documentata e basata su fonti affidabili. Fate la vostra ricerca: trovate i dati e le informazioni necessarie, organizzateli e disponete i punti dello scenario sulla base di essi. Annotate con cura le fonti, scrivendole nel contenuto dell'infografica in modo che gli spettatori possano accedervi.

Formato - Date al vostro lavoro una forma di racconto. Utilizzate argomenti concreti supportati da dati e illustrazioni che siano logicamente collegati. Iniziate la storia con un titolo e una breve descrizione, che può assumere la forma di una domanda. Infine, riassumete la storia, traete le conclusioni e incoraggiate la discussione.

Layout - Un'infografica può essere più pittorica o più testuale o avere più o meno elementi iconici, grafici e stili. Abbinare il profilo visivo al significato della storia: può essere più artistico o più "tabellare", a seconda del tono e della ricezione che desiderate ottenere. È possibile utilizzare modelli già pronti offerti da molti portali.

Pubblicazione - Per ottenere un pubblico, il vostro lavoro ha bisogno dei giusti canali di distribuzione. Utilizzate i social media, le piattaforme mediatiche, la stampa o le forme di comunicazione diretta. Dopo aver pianificato in anticipo il vostro pubblico di riferimento, cercate di raggiungerlo e di mostrargli ciò che avete fatto.

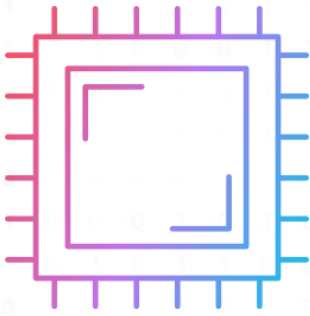
Portata - Assicuratevi di ottenere la giusta portata per il vostro lavoro. Avviate discussioni, fate in modo che le persone commentino e inoltrino l'infografica. Più cose accadono intorno ad essa, più persone vedranno l'infografica e voi imparerete molto sulla sua percezione, sulle reazioni dell'ambiente e sui modi in cui può essere utilizzata.



Quiz 2

It collects links to online tools that can be helpful for content creation within citizen journalism. The trainer can remind the learners that all the multimedia that appear in the class are available on the platform and any learner can access it at any time. In the quiz there are links to the tools in question, divided into thematic categories. Of course, these are not all the possible tools available on the web, but only some examples. The trainer can expand the tool portfolio if they are aware of any interesting and helpful sites. Below the table presents the examples used in the quiz.

categoria	strumento
Foto	scattare foto: Google Camera , Open Camera , riprese: FiLMiC Pro , ProCam X , scansione: Adobe Scan , Office Lens , elaborazione: Adobe Photoshop Express , GIMP , organizzazione: Adobe Bridge , FastStone Image Viewer , banche fotografiche: Pixabay , pexels
Suono	registrazione ed editing: audacityteam , pubblicazione: souncloud , spotify
Testo	Google Docs , Libre Office , WordPress
Informazioni	Feedly , Pocket , Slack
Dati	Tableau Desktop , Datawrapper
Visualizzazioni	canva , infogramma , visme
Infografiche	visual.ly , piktochart



MODULO 4

USO CONSAPEVOLE DELLE TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Sul web è possibile trovare una miriade di informazioni. Tuttavia, non sempre sono di grande valore. È risaputo che le possibilità di controllo dei contenuti su Internet sono decisamente limitate. Diversi portali possono pubblicare informazioni, ma dipende dalla decisione dell'utente se considerarle attendibili e provenienti da una fonte affidabile o se considerarle inutili e non veritiere. Nel cyberspazio, le pubblicazioni sono monitorate e commentate dagli stessi utenti di Internet. I commenti e le critiche ai contenuti pubblicati non sono sempre oggettivi, poiché chiunque può esprimersi online. Per questo motivo, le lezioni di questo modulo sono orientate a un approccio critico al materiale online e a dotare gli studenti del programma "iAware" della capacità di verificare il contenuto di un sito web e la correttezza delle informazioni in esso contenute.

Il quarto modulo comprende argomenti quali:

1. *Notizie false*
2. *Alfabetizzazione mediatica: come riconoscere le fake news?*
3. *Disinformazione e cattiva informazione*
4. *Uso consapevole delle TIC*

Lezione 1

-

Fake news

Questa lezione si concentra sul concetto di "fake news", ovvero, in inglese, semplicemente informazioni false. Si tratta di contenuti non veritieri o non del tutto veritieri, ma che vengono comunque pubblicati su siti web di notizie o social network. Non sempre viene pubblicato in forma testuale, ma può anche utilizzare grafici, immagini e persino video in cui il contenuto viene manipolato attraverso l'elaborazione.

Le fake news fanno parte di un fenomeno più ampio di falsificazione della realtà e delle immagini su Internet. Vengono create e diffuse, ad esempio, per motivi politici o finanziari e possono anche essere create a scopo di intrattenimento per, tra l'altro, attirare l'attenzione sul mezzo o sulla persona che le promuove.

Le fake news possono essere camuffate da informazioni reali, articoli dei media o persino contenuti scientifici. A volte si presentano come tweet pubblicati da persone inesistenti, così come meme su Internet o testi di propaganda. Ciò che accomuna queste forme di fake news è l'intento di ingannare il pubblico. Le fake news possono essere diffuse immediatamente con questa intenzione, ma molto spesso vengono trasmesse attraverso persone che credono nel loro contenuto.

La prima lezione mira a preparare gli studenti a essere critici nei confronti delle informazioni che appaiono su Internet, ad acquisire la capacità di riconoscere le fake news e le diverse fonti di notizie e a comprenderne i pericoli.

MODULO:

Tipi e identificazione di Fake News

catiaalvescruz@gmail.com

Cátia Cruz

UNITA':**TEMA:**

Fake News

RISULTATI DI APPRENDIMENTO:

- Gli studenti capiranno le diverse fonti di notizie
- Gli studenti capiranno il valore di essere ben informati e il pericolo delle notizie false
- Gli studenti saranno in grado di identificare le notizie false

FASI	OBIETTIVO	PROCEDURE	RISORSE
CASE STUDY: "Il peschereccio di Carcavelos" (tempo: 10 min.)	Far conoscere agli studenti gli obiettivi e i risultati della formazione Per familiarizzare gli studenti con un esempio di notizie false prima dell'era digitale	1. Il formatore saluta gli studenti e fa conoscenza con il programma della lezione e le sue fasi successive 2. Il formatore presenta sinteticamente un famoso caso di studio avvenuto in Portogallo nel 2005 e introdurrà: Fiducia, verità e giornalismo	• proiettore & computer
Task Introduzione alle notizie false (time: 10 mins)	Introdurre cosa significano le notizie false e familiarizzare gli studenti da dove provengono le "notizie"	1. Gli studenti guarderanno un video che introdurrà questi argomenti: • Trasformazione delle informazioni sulle notizie: tecnologia digitale, piattaforme social e diffusione di notizie false • Il fenomeno del "disturbo dell'informazione": formati di Disinformazione, Disinformazione e Mal-informazione.	• proiettore & computer
Task Effetti della disinformazione	Familiarizzare gli studenti con l'importanza di essere ben	1. Il formatore introduce gli studenti alle restanti attività della lezione. Sulla base della fase di lezione precedente, il formatore descrive i tipi più famosi di notizie false e come si diffondono al giorno d'oggi.	• un proiettore e un computer con accesso a

dei media (tempo: 15 min.)	informati e le conseguenze delle notizie false	- Il formatore parla agli studenti dei Social media, cerca di capire se controllano le notizie prima di condividerle e se hanno mai segnalato a Facebook una notizia falsa. - Il formatore interagisce con gli studenti e cerca di capire come pensano che dovremmo combattere la disinformazione e la disinformazione - Il formatore mostra un video con un esempio pratico sulla capacità critica di decostruire le notizie false. - Gli studenti rispondono alle domande del formatore e condividono le loro riflessioni sul video guardato.	Internet per il formatore
Task Come identificare le notizie false (tempo: 25 min.)	Per capire come verificare e identificare le fake news Gli studenti insieme accederanno a fonti di notizie e contenuti visivi e faranno un esercizio di verifica dei fatti e verifica dei social media.	- Il formatore spiega come identificare una fonte di notizie affidabile - Il formatore chiede agli studenti di pensare ai contenuti che hanno letto nell'ultima settimana e che pensano siano notizie false - Il compito dello studente sarà quello di classificare e dividere quali notizie verranno presentate e quelle che credono siano vere o false: - o Giornali ben consolidati in Portogallo - o Notizie dai blog online - o Notizie condivise sui social media - o Esempi di fatti che vengono raccontati dai politici nelle interviste Con il supporto del formatore gli studenti verificheranno se la notizia è falsa.	• un proiettore e un computer con accesso a Internet per il formatore • lavorare con i computer: gli studenti hanno accesso a un computer con connessione Internet • Fonti: • Siti web • Video di Youtube • Social media • Motori di ricerca

BUONE PRATICHE (tempo: 10 min.)	Insieme al formatore gli studenti saranno divisi in gruppi e creeranno notizie	1. Gli studenti produrranno notizie. I colleghi dovranno identificare quali sono vere e quali no.	• un proiettore e un computer con accesso a Internet per il formatore e gli studenti
FEEDBACK/ RIFLESSIONI TASK (tempo: 5 min.)	Rivedere e verificare le conoscenze acquisite. Per ottenere feedback dagli studenti in merito alla lezione.	Il formatore riassume la lezione e controlla la reazione dello studente alla lezione (positiva/negativa). Gli studenti riceveranno un batch vincitore che dice "Non mi imbrogli, sono un verificatore di fatti"	

Il formatore deve spiegare ai partecipanti che le fake news non si diffondono solo attraverso i social media, ma possono essere trovate anche nei media tradizionali. Le persone sono abituate ad associare le fake news a Internet e ai social media, ma il materiale falso si è già diffuso e continua a diffondersi anche attraverso i media tradizionali. Paradossalmente, fornire informazioni false su un giornale o una televisione tradizionale le rafforza molte volte e si diffonde facendo riferimento a quella fonte.

Per questo piano di lezioni viene creato un materiale didattico su misura sotto forma di video e quiz interattivi. Tutti i materiali multimediali sono disponibili sulla piattaforma del programma "iAware" nelle sezioni formatori e discenti.



Quiz 1

Un quiz interattivo che può essere visualizzato sullo schermo e svolto durante la lezione, oppure può essere richiesto agli studenti di svolgerlo da soli dopo la lezione. Si tratta di un test sulle conoscenze che gli studenti dovrebbero avere dopo aver trattato l'argomento della lezione. Consiste in domande con una risposta corretta, che deve essere scelta dal discente.

1. Come si definiscono le fake news? Quali caratteristiche possono avere?
 - a. Disinformazione
 - b. Mancanza di informazioni
 - c. Disinformazione
 - d. Tutti i precedenti (corretto)
2. Una voce può essere una forma di fake news?
 - a. Sì (corretto)
 - b. No
3. Se un'emittente dei media tradizionali inizia a distorcere una storia per guadagnare audience, questo può essere considerato una falsificazione della realtà?
 - a. Sì (corretto)
 - b. No

4. Le fake news mirano a:

- a. ingannare e manipolare (correttamente)
- b. manipolare e richiedere
- c. comunicare
- D. tutti i precedenti



Quiz 2

Analogamente al quiz 1, può essere utilizzato durante una lezione o durante il lavoro indipendente dell'allievo. Consiste in una serie di domande in cui deve essere segnata una risposta corretta tra quattro possibili. Il quiz può essere visto come una verifica della comprensione del materiale della lezione da parte dell'allievo. Di seguito viene presentato il contenuto con le risposte corrette.

1. Una fake News ha le seguenti caratteristiche

- a) Essere come un virus
- b) Si propaga facilmente
- c) Può essere facilmente dato per scontato
- d) Tutti i precedenti (corretto)

2. Quali sono le fasi del disturbo da informazione?

- a) Creazione, produzione e distribuzione (corretto)
- b) Preparazione, produzione e lancio
- c) Produzione e distribuzione
- d) Tutti i precedenti

3. Quali sono le fasi di diffusione?

- a) Creare un blog; scrivere contenuti; vendere pubblicità; divulgare via SMS; ripetere.
- b) Creare un sito di notizie false; rubare contenuti; vendere pubblicità; pubblicare sui social network; ripetere. (Corretto)
- c) Scrivere contenuti; vendere pubblicità; divulgare tramite il sito web; ripetere.

Lezione 2

Alfabetizzazione mediatica: come riconoscere le fake news?

Con questa lezione, gli studenti apprenderanno il concetto di alfabetizzazione mediatica e il suo ruolo nel contesto delle fake news. Acquisiranno inoltre competenze su come identificare le fake news e su quali strumenti possono essere utilizzati per farlo.

L'alfabetizzazione mediatica può essere intesa come la formazione di competenze per un uso consapevole dei media, basato su conoscenze, atteggiamenti, motivazioni e abilità, in cui gli utenti sono in grado di interpretare il significato dei messaggi e di capire come vengono costruiti i messaggi o i contenuti dei media, nonché di conoscere le conseguenze della diffusione di informazioni non verificate. L'alfabetizzazione mediatica non è solo la capacità di usare Internet e i dispositivi mobili, ma soprattutto la capacità di usare i media in modo appropriato e consapevole. Una persona alfabetizzata ai media dovrebbe essere in grado di distinguere tra un messaggio valido e accurato e uno destinato a suscitare emozioni, paura, pregiudizi o a diffondere falsità.

Non esiste un metodo efficace al cento per cento per identificare le fake news. Ci sono molti indizi che possono suscitare e aumentare il sospetto di inganno. Questa lezione aiuterà a imparare a riconoscere le informazioni false. Tuttavia, il formatore deve rendere i discenti consapevoli del fatto che l'acquisizione di competenze mediatiche non può essere una tantum. Il mondo dei media, dell'informazione e delle nuove tecnologie sta cambiando così velocemente che è necessaria una continua educazione ai media e una costante alfabetizzazione mediatica.

MODULO:

Cultura dei media - Come riconoscere le fake news

UNITA': 1**TEMA:**

Alfabetizzazione mediatica - Come riconoscere le fake news

RISULTATI DI APPRENDIMENTO:

- Cos'è l'alfabetizzazione mediatica
- Comprendere il ruolo dell'alfabetizzazione mediatica nel contesto delle fake news.
- Come individuare le fake news
- Strumenti per individuare e smascherare le fake news
- Sviluppare le competenze di alfabetizzazione ai media e all'informazione.

FASI	OBIETTIVO	PROCEDURE	RISORSE
Introduzione e alla cultura dei media	Introdurre il concetto di Media Literacy	• Il formatore si presenta • Il formatore introduce il concetto principale cultura dei media utilizzando un power point. • Il formatore chiede agli studenti la loro comprensione del concetto di cultura dei media. • Il formatore introduce il concetto di pensiero critico. Il formatore fornisce esempi di collegamento tra cultura dei media e pensiero critico.	• Proiettore e accesso a Internet
Task (tempo: 15 min)	Sviluppare una mappa di parole per i concetti principali della cultura dei media	• Il formatore presenta il compito • Il compito consiste nell'identificare i concetti principali dell'alfabetizzazione mediatica trovati attraverso una ricerca sul web. • Ogni gruppo costruisce la propria nuvola di parole • Ogni gruppo presenta i risultati alla classe. • Il formatore promuove una discussione sui risultati in modo che gli studenti possano guardare e confrontare i propri risultati con quelli degli altri gruppi di studenti	• Projector and Internet access • Computer for students

Come riconoscere le fake news	Dare agli studenti le competenze necessarie per individuare le fake news.	• Il formatore presenta diverse tecniche per individuare le fake news. • Gli studenti guardano un video da youtube sulle fake news. https://www.youtube.com/watch?v=Q8su4chuU3M&ab_channel=TheFrance24Observers • L'insegnante/formatore fornisce esempi per ciascuno dei passi da seguire per verificare le fake news. Il formatore esplora i diversi contenuti mediatici presenti in una notizia che dovrebbero essere valutati criticamente.	• Proiettore e accesso a Internet • Computer per gli studenti
Task (tempo: 25 min)	Dare agli studenti una visione pratica dell'identificazione e delle fake news attraverso l'uso di un approccio critico.	• L'insegnante/formatore presenta 3 titoli e contenuti testuali e multimediali. • Il compito dello studente è quello di identificare se le notizie sono false o meno seguendo le fasi identificate nella lezione precedente. Gli studenti condividono i risultati e spiegano le ragioni delle loro conclusioni.	• Proiettore e accesso a internet
BUONE PRATICHE (tempo: 10 min.)	Come affrontare le fake news nella vita di tutti i giorni	• Il formatore riassume i concetti principali discussi durante la lezione. Il formatore chiede agli studenti di condividere le proprie conclusioni sul ruolo dell'alfabetizzazione mediatica.	•
FEEDBACK/ RIFLESSION I TASK (tempo: 5 min.)	Riflessione critica sulle fake news e sul loro impatto sulla democrazia e sulla cittadinanza.	• Il formatore fornisce agli studenti esempi di fake news. • Il formatore chiede agli studenti di pensare alle implicazioni per la società se la gente le prende per vere. • Discussione generale tra insegnante e studenti Il formatore conclude la sessione fornendo una panoramica generale della stessa.	

Per questa lezione sono previsti due quiz interattivi, che possono essere utilizzati in classe o che gli studenti possono essere invitati a svolgere da soli. Il quiz è un riassunto della lezione e un test di conoscenza sulle fake news. I quiz sono disponibili sulla piattaforma "iAware".



Quiz 1

Si tratta di un quiz a scelta multipla. Il compito della persona che lo esegue è quello di segnare tutte le possibili risposte corrette in ogni domanda. Di seguito è riportato il contenuto del quiz.

1) *Che cos'è l'alfabetizzazione mediatica?*

- a) Pratiche che consentono alle persone di accedere, valutare criticamente e creare o manipolare i media.
- b) Un insieme di competenze essenziali per il lavoro, la vita e la cittadinanza.
- c) intende promuovere la consapevolezza dell'influenza dei media e creare una posizione attiva nei confronti del consumo e della creazione dei media.
- d) Tutti i precedenti (corretto)

2) *Pensare in modo organizzato e razionale è una delle caratteristiche del pensiero critico?*

- a) Sì (corretto)
- b) No

3) *Selezionate alcune delle competenze importanti per il pensiero critico.*

- a) Analisi (corretta)
- b) Interpretazione (corretta)
- c) Valutazione (corretta)
- d) Spiegazione (corretta)
- e) Attenzione
- f) Apertura mentale (corretto)
- g) Risoluzione dei problemi (corretta)



Quiz 2

Analogamente al primo quiz di questa lezione, questo è un quiz con più di una risposta corretta. Il discente segna sullo schermo tutte le risposte corrette. Di seguito vengono presentate le domande che compaiono nel quiz con le risposte corrette segnate.

- 1) *A cosa dobbiamo prestare attenzione quando leggiamo le notizie?*
 - a) Leggere oltre il titolo
 - b) Controllare l'autore
 - c) Controllare le fonti di supporto
 - d) Data di controllo
 - e) Verificare se si tratta di uno scherzo
 - f) Tutti i precedenti (corretto)
- 2) *Come possiamo ridurre la produzione di Fake News? (Selezionare tutte le opzioni applicabili)*
 - a) Aumento dell'alfabetizzazione ai media e all'informazione (corretto)
 - b) Verificare i fatti (corretto)
 - c) Finanziamento e trasparenza nel giornalismo (corretto)
 - d) Regolamento (corretto)
- 3) *Cosa dobbiamo fare quando analizziamo le notizie?*
 - a) Controllare la fonte/autore dell'immagine (corretto)
 - b) Valutare la veridicità del giornale (Corretto)
 - c) Chiamare l'autore
 - d) Confermare se si tratta di un annuncio (corretto)
 - e) Confrontare le informazioni (corretto)

Lezione 3

-

Disinformazione e cattiva informazione

In questa lezione si è cercato di chiarire la differenza tra due termini: disinformazione e informazione fuorviante (cattiva informazione). Spesso vengono usati in modo errato e intercambiabile. La differenza tra i due termini sta nell'intenzione del mittente del messaggio. La disinformazione è un messaggio non corretto, fuorviante, parzialmente falso o completamente falso. Viene comunicato senza l'intento diretto di ingannare. La cattiva informazione è un'informazione falsa pubblicata con l'intento di ingannare le persone. Chi diffonde un messaggio di questo tipo sa perfettamente che è falso e vuole ingannare i destinatari.

Tuttavia, sia la disinformazione che la cattiva informazione sono fenomeni pericolosi, che forniscono alle persone informazioni false e vengono utilizzati per ingannare e manipolare.

Un altro concetto legato ai concetti di disinformazione e cattiva informazione è il caos informativo (rumore). È un concetto che si riferisce a un eccesso di informazioni, spesso poco essenziali, che rende difficile identificare ciò che è importante e prezioso. È tutto questo contenuto superfluo che inquina il messaggio informativo.

Per utilizzare consapevolmente le informazioni raccolte sul web, è essenziale selezionare i contenuti di valore. Pertanto, questa lezione mira a definire cosa si intende per disinformazione e informazioni fuorvianti e quali sono le tecniche per decostruire i contenuti dei media.

MODULO:		UNITA':	TEMA:
Disinformazione e cattiva informazione		2	Disinformazione e cattiva informazione
RISULTATI DI APPRENDIMENTO:: - Identificare cosa si intende per disinformazione e disinformazione. - Tecniche per la decostruzione dei contenuti dei media.			
FASI	OBIETTIVO	PROCEDURE	RISORSE
Introduzione	• Introduce trainees to the concept of disinformation in the media • Why it is important to be alert to this phenomenon • Misinformation, wrong information	• The trainer introduces the concept of information disorder • The trainer presents the differences between misinformation and misinformation • Trainer presents practical cases of misinformation and misinformation in the media	• Data show and computer • Internet access
CASE STUDY: (tempo: 10 min)	• Presentazione del caso di studio • Discussione sul caso presentato	• Il formatore presenta un caso di studio • Gli studenti guardano il video della prima conferenza stampa di Donald Trump. • https://www.theguardian.com/us-news/2017/feb/16/donald-trump-press-conference-administration-defense-media • Gli studenti discutono gli elementi che possono costituire elementi di disinformazione.	• Mostra dati e computer • Accesso a Internet
Tecniche di disinformazione (tempo: 15 min)	• Tecniche di decostruzione della disinformazione	• Presentazione delle tecniche di decostruzione della disinformazione • La decostruzione delle immagini - Strumenti online per identificare le immagini false	• Mostra dati e computer • Accesso a Internet • Computer per gli studenti

		- La decostruzione dei testi - Convalida dei testi attraverso altre fonti	
Task (tempo: 25 min.)	Identificazione dei contenuti	- Il formatore propone un esercizio agli studenti. - Il formatore consegna agli studenti il materiale per l'esercizio contenente diversi esempi di notizie nei media digitali - Gli studenti, in gruppo o individualmente, scelgono una o più notizie. - Gli studenti applicano le tecniche di decostruzione dei contenuti nei media - Gli studenti condividono i risultati indicando le principali conclusioni raggiunte. - Il formatore riassume l'esercizio e chiede un feedback agli studenti.	- Mostra dati e computer - Accesso a Internet - Computer per gli studenti
BUONE PRATICHE (tempo: 10 min.)	Come essere un cittadino critico	- Il formatore presenta le strategie per una cittadinanza attiva e critica in relazione ai contenuti che ci circondano; - Discussione su come possiamo essere cittadini critici in relazione ai contenuti che fruiamo ogni giorno nei media.	- Mostra dati e computer - Accesso a Internet - Computer per gli studenti
FEEDBACK/ RIFLESSIONI TASK (tempo: 5 min.)	Riflessioni sul modulo	- Cosa abbiamo imparato - Come possiamo metterlo in pratica - Come possiamo migliorare	

Per questa lezione sono stati preparati anche due quiz interattivi, che possono essere utilizzati in classe e svolti insieme a tutto il gruppo, oppure ogni studente può svolgerli autonomamente in qualsiasi momento.



Quiz 1

Il quiz riassume la conoscenza di tre termini: fake news, disinformazione e disinformazione. Il compito del discente è quello di abbinare il concetto al relativo termine. Il quiz è un test per verificare se i discenti hanno ricordato correttamente quali sono i diversi tipi di informazione. Di seguito viene presentato il contenuto del quiz.

Definizioni

Disinformazione - anche un'informazione diffusa, indipendentemente dall'intento di fuorviare.

Disinformazione - informazioni deliberatamente fuorvianti o distorte; narrazione o fatti manipolati; propaganda.

Fake news - informazioni create di proposito, sensazionali, cariche di emozioni, fuorvianti o totalmente inventate che imitano la forma delle notizie tradizionali.



Quiz 2

Questo è un quiz vero o falso e riguarda il fenomeno del deepfake, ovvero la creazione e la pubblicazione di informazioni false sotto forma di video, registrazioni audio e fotografie. Con il deepfake è possibile ottenere video realistici ma falsificati che creano opportunità di manipolazione o inganno. Un esempio è l'incapacità dello spettatore di distinguere i volti degli attori che appaiono in un film. Il quiz mira a sensibilizzare sui pericoli di questo fenomeno. Il contenuto del quiz con le risposte corrette è riportato di seguito.

- 1) *La tecnologia Deepfake è in grado di creare foto e video quasi reali, ma completamente fittizi, partendo da zero: VERO*
- 2) *I deepfake utilizzano l'intelligenza artificiale del deep learning per sostituire le sembianze di una persona con un'altra in video e altri media digitali VERO*
- 3) *Si teme che la tecnologia deep fake possa essere utilizzata per creare fake news e video fuorvianti e contraffatti. VERO*

Lezione 4

-

Uso consapevole delle TIC

La lezione riassume e riunisce le conoscenze e le competenze degli studenti per un uso consapevole delle tecnologie dell'informazione. Il formatore invita i partecipanti a discutere il ruolo e l'impatto delle tecnologie dell'informazione e della comunicazione sulla loro vita quotidiana. È importante notare che queste tecnologie non riguardano solo l'uso del computer, ma anche i dispositivi mobili o gli smartwatch. La discussione può essere condotta in molti modi. Si possono cercare i pro e i contro dell'uso di queste tecnologie nella vita quotidiana; ci si può concentrare solo sugli aspetti positivi, oppure si possono dividere gli studenti in due gruppi: uno si concentra sugli aspetti positivi e l'altro su quelli negativi. Lo scambio di esperienze durante questa discussione può permettere agli studenti di trovare nuovi usi creativi della tecnologia digitale nella loro vita quotidiana e professionale.

Oltre allo scambio di esperienze, durante la lezione deve essere creato un elenco di buone e cattive pratiche nell'uso delle tecnologie digitali. Il formatore può utilizzare il metodo del brainstorming tra gli studenti e annotare tutte le idee emergenti sulla lavagna, per poi riassumere e completare questo elenco. Un aspetto essenziale è quello di raccogliere le risposte degli studenti su cosa pensano sia l'uso consapevole delle tecnologie informatiche.

Un uso essenziale delle tecnologie informatiche è quello di comunicare con diversi gruppi di persone. Il formatore può specificare i diversi canali di comunicazione che utilizzano le tecnologie informatiche e gli strumenti utilizzati a questo scopo e diffusi nel suo Paese. È importante notare che la comunicazione con persone provenienti da diverse parti del mondo è sempre stata possibile con metodi tradizionali, ma l'uso delle tecnologie informatiche l'ha notevolmente accelerata.

MODULO:		UNITA':	TEMA:
Uso responsabile delle tecnologie dell'informazione e della comunicazione		1	Uso responsabile delle tecnologie dell'informazione e della comunicazione
LEARNING OUTCOMES:			
FASI	OBIETTIVO	PROCEDURE	RISORSE
Introduzione alle tecnologie dell'informazione e della comunicazione: (durata: 10 min)	- Vivere senza tecnologie dell'informazione e della comunicazione - Ricerca di un tema - Trovare una canzone (come?) - Comunicare con gli amici (come?)	- Cosa sono le tecnologie dell'informazione e della comunicazione - Esplorare con i partecipanti il ruolo e l'impatto delle tecnologie dell'informazione e della comunicazione nella vita quotidiana. - Il formatore condivide un video su Youtube https://www.youtube.com/watch?v=7Q67Poh7cGA&ab_channel=DilshanSoftLab	Mostra dati e connessione a Internet
task (durata: 10 min)	Trovare la risposta a un argomento o a un tema senza usare i motori di ricerca.	- Il formatore fornisce ai discenti una serie di domande che richiedono una risposta. - Il formatore fornisce o indica le risorse disponibili per trovare la risposta.	Libri o biblioteca
Task: Uso responsabile delle tecnologie dell'informazione e della comunicazione (tempo: 15 mins)	Che cos'è l'uso consapevole delle tecnologie informatiche?	- Il formatore presenta le buone e le cattive pratiche nell'uso delle TIC. - Il formatore raccoglie le opinioni dei partecipanti sulle loro pratiche di utilizzo delle TIC. - Il formatore e i partecipanti confrontano ciò che è stato presentato dal formatore in relazione alle loro pratiche.	Mostra dati e connessione internet

Comunicare con le TIC	• Esplorare l'uso di diverse TIC per comunicare a diversi gruppi di persone.	• Il formatore presenta diverse tipologie di TIC • Il formatore presenta diversi formati di contenuto • Il formatore fornisce esempi di uso multidimensionale delle TIC.	
task (tempo: 25 min)	• Il formatore presenta un esercizio	• I partecipanti svolgono l'esercizio presentato dal formatore su come comunicare un'idea. • I tirocinanti devono scegliere i formati più adatti per comunicare un'idea. • I partecipanti devono giustificare le ragioni della loro scelta. • Dopo l'esercizio, i tirocinanti e il formatore valutano i risultati.	• Mostra dati e connessione internet
FEEDBACK/ RIFLESSIONE ATTIVA (tempo: 5 min)	• Riflessione	• I tirocinanti riflettono su ciò che hanno appreso. • Gli apprendisti riflettono sui cambiamenti e gli aggiustamenti nell'uso delle TIC.	

Per questa lezione, come per le precedenti, sono disponibili due risorse multimediali sulla piattaforma "iAware". Possono essere utilizzate durante la lezione o come compito a casa indipendente. Lo scopo dei quiz è quello di riassumere e verificare le conoscenze degli studenti.



Quiz 1

Quiz "Scegli molti". Il compito dell'allievo è quello di segnare tutte le risposte corrette. Il quiz si concentra sull'uso delle tecnologie informatiche nella vita quotidiana.

1. Selezionate alcune delle TIC che conoscete:

- a) Computer (corretto)
- b) Frigorifero
- c) Mobile (corretto)
- d) Televisione (corretto)
- e) Internet (corretto)
- f) Libro
- g) Lampada
- h) e-mail (corretto)
- i) Penna

2. Sarebbe possibile comunicare con amici dall'altra parte del mondo senza l'uso della tecnologia? (Selezionare l'opzione più corretta)

- a) Sì, facilmente.
- b) Sì, ma non così facilmente.
- c) No.

3. Come si faceva ricerca prima dell'evoluzione tecnologica?

- a) Utilizzo della biblioteca.
- b) Interviste con esperti.
- c) Partecipazione alla formazione.
- d) Attraverso le riviste di settore.
- e) Tutte le situazioni precedenti.

4. Quali sono i possibili usi delle tecnologie?

- a) Istruzione
- b) Elaborazione dei dati
- c) Comunicazione
- d) Raccolta di informazioni
- e) Affari
- f) Tutti i precedenti (corretto)



Quiz 2

Analogamente al quiz 1, riguarda l'applicazione della tecnologia alle attività della vita quotidiana. Evidenzia che è già presente in quasi tutti gli aspetti della vita. Il quiz comprende domande sull'incidenza della tecnologia. Il suo scopo è quello di testare le conoscenze del discente. Il compito è quello di scegliere una risposta corretta alla domanda che appare sullo schermo. Di seguito viene presentato il contenuto del quiz con le risposte corrette.

1. È possibile trovare la musica utilizzando la tecnologia?

- a) Sì (corretto)
- b) No

2. Posso usare la tecnologia per cucinare?

- a) Sì (corretto)
- b) No

3. Posso comunicare con i miei amici attraverso la tecnologia?

- a) Sì, se utilizzano le stesse tecnologie. (Corretto)
- b) Sì, in qualsiasi circostanza.
- c) Sì, anche senza le stesse tecnologie.
- d) No.

4. L'uso della tecnologia è gratuito?

- a) Sì
- b) Dipende dai servizi utilizzati (Corretto)
- c) No

5. La tecnologia può essere utilizzata per scopi didattici?

- a) Sì (corretto)
- b) No

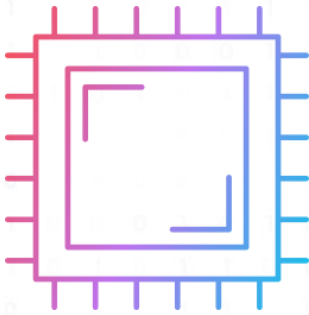
6. Quali sono le applicazioni più utilizzate per fare presentazioni?

- a) Canva
- b) Prezi
- c) Diapositive
- d) Keynote

- e) PowerPoint
- f) Nessuno dei precedenti
- g) Tutti i precedenti (corretto)

7. Quale delle opzioni non è considerata una rete sociale?

- a) Facebook
- b) TikTok
- c) Adobe (corretto)
- d) Reddit
- e) Twitter
- f) Whatsapp
- g) Nessuno dei precedenti



MODULO 5

DIREZIONI PER LO SVILUPPO DI INTERNET,
COSTRUZIONE ATTIVA DI UNA COMUNITÀ
GLOBALE DI E-CITTADINI

Le origini di Internet, la rete informatica globale, possono essere fatte risalire alla fine degli anni '60 negli Stati Uniti. Da allora si è sviluppata a un ritmo molto veloce, attraversando varie fasi. Internet è una rete informatica globale ed è la più grande al mondo, composta da un numero enorme di reti più piccole. Collega computer di tutti i continenti, consente lo scambio di informazioni e servizi e dà accesso a un vasto e crescente numero di informazioni provenienti da tutto il mondo.

Internet ha molti significati per persone diverse. È un luogo di incontro e di scambio di idee, un canale di comunicazione, una raccolta di risorse informative a disposizione di tutti, nonché un luogo di promozione e vendita di beni e servizi. Come tutte le tecnologie informatiche, Internet si sta sviluppando rapidamente. Il Modulo 5 raccoglie la storia dell'evoluzione di Internet e le direzioni più interessanti del suo sviluppo. All'interno di questo modulo vengono proposti i seguenti argomenti di lezione:

1. Passato, presente e futuro di Internet
2. IoT - Internet of Things
3. AI, Big Data e Cloud
4. Cittadinanza elettronica

Lezione 1

-

Passato, presente e futuro di Internet

L'obiettivo di questa lezione è comprendere il contesto in cui sono nati Internet e il WWW e capire la differenza tra Internet e il WWW. Inoltre, gli studenti svilupperanno le competenze necessarie per comprendere l'organizzazione delle informazioni sul World Wide Web.

La lezione inizia sottolineando la differenza tra due termini spesso usati erroneamente in modo intercambiabile: Internet e WWW (World Wide Web). Sebbene i due termini siano correlati, esistono differenze significative. Internet è un sistema globale di reti informatiche interconnesse, mentre il WWW è un modello di condivisione delle informazioni che risiedono su Internet, ovvero il WWW è solo un sottoinsieme di Internet, e non un sinonimo.

Nei moduli precedenti, gli studenti hanno acquisito le competenze per utilizzare vari strumenti di Internet, ma questo argomento li introduce anche a concetti come nome di dominio, protocollo di hosting e sistemi di gestione dei contenuti di Internet. Impareranno anche le differenze tra WEB 1.0, WEB 2.0 e altri modi di utilizzare le risorse di Internet.

Inoltre, è previsto un esercizio pratico sul funzionamento dei motori di ricerca. Prima di fare questo esercizio, il formatore può chiedere ai partecipanti di condividere le loro esperienze di utilizzo dei motori di ricerca. È utile mostrare ai partecipanti i diversi metodi per restringere i criteri di ricerca.

MODULO:

Indicazioni per lo sviluppo di Internet, costruzione attiva di una comunità globale di cittadini elettronici

UNITA':

5.1

TEMA:

Il passato, il presente e il futuro di Internet

RISULTATI DI APPRENDIMENTO:

- Gli studenti capiranno il contesto dell'emergere di Internet e del WWW
- Gli studenti capiranno le differenze tra Internet e il world wide web (WWW)
- Gli studenti acquisiranno familiarità con le diverse fasi del WWW 1.0, 2.0, 3.0 e 4.0.
- Gli studenti saranno in grado di identificare concetti come domini, protocolli, hosting e server
- Gli studenti svilupperanno competenze che consentiranno loro di comprendere come sono organizzate le informazioni sul WWW
- Gli studenti saranno in grado di identificare le criticità associate alla privacy su Internet
- Gli studenti saranno in grado di sviluppare strategie di utilizzo di Internet e WWW più sicure

FASI	OBIETTIVO	PROCEDURE	RISORSE
Antecedenti del WWW e contesto storico e sociale del villaggio globale. Alan Turing e le macchine pensanti, ARPANET e la necessità di comunicare globalmente	Comprendere il concetto di rete, i protocolli e le differenze tra Internet e il WWW	1 - Il formatore presenta gli argomenti della lezione 2 - Il formatore esplora le conoscenze di ogni tirocinante su Internet e sul WWW 3 - Contesto storico nell'emergere di Internet e dei suoi attori 4 - Contesto per lo sviluppo del WWW e dei suoi attori 5 - Caratteristiche tecniche di Internet e del WWW	- Computer con accesso a Internet
Argomento di studio Di tanto in tanto	Esercizio sul prima e dopo del web. Immagina 24 ore senza l'uso di WWW	Rifletti sulle logiche integrate e onnipresenti dell'uso di Internet e del WWW	• Post-it e pennarelli

L'evoluzione del WWW	Identificazione delle diverse fasi dell'evoluzione del WWW	1 - individuazione delle principali caratteristiche del WWW nelle sue diverse fasi 2 - L'evoluzione del WWW, dei servizi associati e della vita nella società	- Computer con accesso a Internet.
Domini, protocolli e hosting	Identificare i componenti di un dominio web Crea e registra un dominio e un hosting	1- Cos'è un dominio, sottodominio e come registrarsi 2 - Differenze tra dominio e hosting 3 - Sistemi di gestione dei contenuti per il web	- Lettore PDF. - Computer con accesso a Internet.
Come sono organizzati e strutturati i dati per essere disponibili sui motori di ricerca	Cos'è un motore di ricerca? Come vengono trovate, raccolte e classificate le informazioni	Come funzionano i motori di ricerca - https://www.youtube.com/watch?v=0eKVizvYSUQ&ab_channel=Google Esercitazioni pratiche basate sulla seguente proiezione video https://www.ted.com/talks/seth_stephens_davidowitz_what_google_searches_can_tell_us_about_who_we_really_are	- Computer con accesso a Internet
Cookies e Privacy	Comprensione del monitoraggio di Internet e WWW Cos'è un Cookies? Come funziona la pubblicità sul WWW	Comprendi come funziona il monitoraggio sul WWW Cos'è un cookie Identificazione delle reti di cookie Esempio con LightBeam Anteprima della serie di web documentari - DO NOT TRACK - https://donottrack-doc.com/en/	- Computer con accesso a Internet
Strategies for safer browsing	Develop skills for safe browsing on the WWW	Development of strategies to identify cookies, their management and preferences defined at the level of different browsers General framework of the GDPR and European legislation on data protection	- Computer with Internet access.

Per la lezione sono state preparate due risorse multimediali.



Quiz 1

Si tratta di un quiz con domande a risposta singola e multipla. A seconda del tempo a disposizione in classe, l'esercizio può essere svolto durante la lezione o può essere chiesto agli studenti di farlo da soli a casa. Tutti gli esercizi sono pubblicati sulla piattaforma "iAware" e il contenuto del quiz con le risposte corrette è presentato di seguito.

Selezionare la risposta corretta

1) *Che cos'è Internet?*

- a) *Un tipo di browser web*
- b) *Una rete globale di computer e dispositivi elettronici: X*
- c) *Una cartella del computer in cui sono archiviati file importanti*
- d) *Una raccolta globale di siti web diversi*

2) *Quali delle seguenti attività si possono svolgere online? Selezionare tutte le opzioni applicabili.*

- a) *Pagare le bollette e gestire i conti bancari X*
- b) *Utilizzare i motori di ricerca per trovare informazioni X*
- c) *Guardare film e programmi TV X*
- d) *Inviare e ricevere e-mail e messaggi istantanei X*

3) *Quale dei seguenti NON è un browser web?*

- a) *Windows X*
- b) *Bordo*
- c) *Chrome*
- d) *Firefox*

4) Quando si parla di Web, "link" è l'abbreviazione di _____.

- a) ammiccamento
- b) collegamento ipertestuale X
- c) catena
- d) superlink

5) A cosa servono principalmente le schede del browser?

- a) Apertura di più pagine web nella stessa finestra del browser X
- b) Garantire che le vostre informazioni personali non siano visibili agli hacker
- c) Visualizzazione di due pagine web affiancate
- d) Selezione di una rete Wi-Fi a cui connettersi

6) Il WWW e Internet sono la stessa cosa?

- a) No, sono cose diverse, ma il WWW è parte di INTERNET X
- b) Sì, sono la stessa cosa, ma con nomi diversi.



Quiz 2

Si tratta di un esercizio composto da più parti, la prima delle quali consiste nell'abbinare WEB 1.0, WEB 2.0 o WEB 3.0 alla funzionalità corretta. Gli esercizi successivi sono costituiti da domande in cui gli studenti segnano le risposte corrette. Il quiz può essere svolto con gli studenti in classe come riepilogo della lezione oppure si può chiedere loro di farlo da soli a casa. Il contenuto del quiz con le risposte corrette è riportato di seguito.

1) Abbinare le seguenti parole nei cestini corretti

Contenitore 1 - Web 1.0

Contenitore 2 - Web 2.0

Contenitore 3 - Web 3.0

- a) È costituito da pagine statiche collegate a un sistema tramite collegamenti ipertestuali.*
- b) Web sociale partecipativo*
- c) Wiki e blog*
- d) Contiene contenuti dinamici che rispondono agli input dell'utente.*
- e) 5 - Leggere-scrivere-interagire*
- f) Onde e flussi live*

2) Scegliere le risposte corrette

- a) Un cookie è un software che si può scaricare e installare*
- b) Un cookie è un file di testo che contiene informazioni di base sulla vostra posizione, sul sistema operativo e sulla lingua e che viene inserito nel vostro browser dal sito web che state visitando.*
- c) Il cookie è un'applicazione utilizzata dalle reti pubblicitarie.*
- d) Un cookie è un dolce*

3) Vero o falso?

- *Per navigare in un sito web devo accettare i cookie: FALSO*

4) Scegliere la risposta corretta

- a) *Un cookie di prima parte è un cookie impostato nel vostro browser dal sito web che state visitando. X*
- b) *Un cookie di prima parte è un cookie impostato nel vostro browser da un sito web diverso da quello che state visitando.*

5) Scegliere la risposta corretta

- a) *Un cookie di terze parti è un cookie impostato nel vostro browser dal sito che state visitando.*
- b) *Un cookie di terze parti è un cookie impostato nel vostro browser da un sito web diverso da quello che state visitando. X*

6) Scegliere le risposte corrette

- a) *Navigando in modalità privata, il browser non salva:*
- b) *La vostra cronologia di navigazione*
- c) *Informazioni inserite nei moduli*
- d) *Cookie e dati del sito*
- e) *Tutte le risposte sono corrette X*

Lezione 2

-

IoT - Internet of Things

Nei suoi termini più semplici, l'Internet of Things (IoT) è il concetto per il quale i dispositivi elettronici sono in grado di connettersi a Internet o ad altri dispositivi, direttamente tramite reti wireless o, raramente, tramite cavi. Per Things - "cose" si intendono dispositivi di uso quotidiano come i moderni telefoni, le macchine fotografiche, gli orologi per il fitness, la domotica e gli strumenti medici, le macchine agricole, le catene di distribuzione, i robot industriali e persino i segnali stradali. In altre parole, l'Internet of Things è una rete di dispositivi interconnessi che possono comunicare tra loro e condividere dati con gli utenti attraverso Internet. I dispositivi IoT possono connettersi via Internet e sono spesso dotati di vari sensori che consentono loro di raccogliere dati. Un dispositivo IoT può essere utile da solo, ma quando viene utilizzato con più dispositivi contemporaneamente ha ancora più valore. Uno degli obiettivi di questa lezione è comprendere il concetto di Internet of Things e acquisire le competenze per identificare dispositivi, strumenti e sistemi IoT. Il formatore può chiedere ai partecipanti esempi di dispositivi IoT che hanno in casa e che usano quotidianamente.

Dato che sempre più dispositivi sono intelligenti e si connettono a Internet, le dimensioni e l'importanza dell'Internet of Things stanno crescendo. Se il formatore ha precedentemente creato un elenco di oggetti IoT con i discenti, questi ultimi noteranno certamente che è molto ampio. Diversi dispositivi, dalle macchine di una fabbrica alle sottostazioni elettriche, agli edifici e alle infrastrutture, possono far parte dell'IoT e il numero di dispositivi connessi aumenta di giorno in giorno. Produttori, aziende di servizi pubblici, autorità locali, numerose organizzazioni e persone comuni fanno parte dell'Internet of Things.

La tecnologia IoT consente la raccolta automatica di dati da varie funzioni. Purtroppo, i dispositivi con caratteristiche di sicurezza più deboli sono facilmente presi di mira dai criminali online. L'invasione della privacy, il furto dei dati raccolti dai dispositivi (ad es. foto, registrazioni audio) sono solo alcuni dei rischi che si possono incontrare. Pertanto, un altro obiettivo di questa lezione sarà quello di acquisire una consapevolezza dei rischi associati all'Internet of Things e di sapere quali precauzioni adottare quando si utilizza questa tecnologia.

MODULO:

Indicazioni per lo sviluppo di Internet, costruzione attiva di una comunità globale di cittadini elettronici

UNITA':

2

TEMA

IoT - Internet of Things

RISULTATI DI APPRENDIMENTO:

- Gli studenti acquisiranno familiarità con i termini IoT e Internet of Things, comprendendone il concetto.
- Gli studenti saranno in grado di identificare dispositivi, strumenti e sistemi IoT.
- Gli studenti saranno consapevoli dei rischi IoT.
- *Gli studenti sapranno quali precauzioni adottare quando si utilizza questa tecnologia.*

FASI	OBIETTIVO	PROCEDURE	RISORSE
1 - Introduzione all'IoT - Internet of Things (tempo: 5 min.) (Video)	Spiegare il concetto di Internet delle cose.	Lo studente vedrà un video che riassume il concetto di Internet of Things, che includerà i seguenti argomenti: - Spiegazione di cosa consiste l'IoT e qual è l'obiettivo principale di questo tipo di sistemi e strumenti digitali; - Approccio alle tipologie di dispositivi collegabili e controllabili da remoto; - Semplice riferimento al tipo di tecnologia indispensabile per realizzare questi dispositivi interconnessi; - Esempi di piattaforme attualmente disponibili utilizzate per aggregare e interconnettere più dispositivi.	Computer con accesso a Internet.
2 - Esercizio 1 - Identificare dispositivi IoT (tempo: 10 min.) (Risposta Multipla)	Renditi conto se la conoscenza è stata acquisita dallo studente.	- Viene presentato un elenco di definizioni relative all'Internet of Things. Lo studente dovrà scegliere l'opzione più appropriata in ogni caso; - Il docente nomina alcuni dispositivi elettronici, in modo da consentire allo studente di identificare quali tra quelli presentati	Computer con accesso a Internet.

		possono essere oggetti IoT. - Es.: Frigorifero, Televisione, Aria Condizionata, Serratura, Prese, Interruttori.	
3 - Riepilogo (tempo: 5 min.) (PDF File)	Consolidamento della conoscenza. Rendere accessibili le informazioni in un unico documento.	Dopo aver completato l'Esercizio 1, lo studente avrà accesso a un documento che includerà un elenco di semplici definizioni, che riassumono il concetto, nonché i diversi tipi di dispositivi che possono essere considerati dall'IoT.	- Computer con accesso a Internet.- PDF.
4 - Caso di studio - I rischi: caso di dispositivi per il diabete (Negative) (tempo: 15 min.)	Mostra come la tecnologia può essere utilizzata anche per scopi negativi e può anche essere potenzialmente pericolosa.	Gli studenti vedranno un articolo con un esempio di integrazione utilizzando l'Internet of Things applicato all'area sanitaria, che presenta uno dei pericoli di questo tipo di dispositivo, se non hanno alcun approccio alla sicurezza. Articolo: https://bit.ly/2JVpZta Verrà inoltre presentato un video di esempio, con diversi pericoli che possono esistere nelle più diverse aree di business. Video - Sicurezza dell'Internet delle cose: https://www.youtube.com/watch?v=pGtnC1jKpMg	- Computer con accesso a Internet.
5 - Esercizio 2 - Che cura devo fare? (tempo: 10 min.) (Risposta Multipla)	Comprendere se lo studente è in grado di identificare alcuni dei pericoli dell'Internet of Things.	Lo studente dovrebbe essere in grado di riconoscere il problema menzionato nel caso di studio, nonché identificare le precauzioni da adottare per ridurre al minimo i rischi derivanti dall'utilizzo di dispositivi IoT. Verranno poste alcune domande, attraverso esercizi a risposta multipla, relativi all'esempio citato, per assicurare che lo studente abbia avuto la corretta comprensione dei concetti in esso impliciti.	Computer con accesso a Internet.

6 - Caso di studio - Boston Children's Hospital (positivo) (tempo: 15 min.)	Mostra una delle funzionalità dei dispositivi IoT.	Lo studente sarà confrontato con un caso di studio del Boston Children's Hospital, in cui utilizza i dispositivi Internet of Things come un modo per migliorare la trasmissione di informazioni da percorsi diversi ai suoi pazienti, come un modo per ridurre i tempi in cui si perdono l'ospedale o recarsi in un luogo in modo errato. Articolo: https://bit.ly/38uEtKE	Computer con accesso a Internet.
7 - Risorse - Curiosità e Potenzialità dell'IoT	Fornire contenuti che permettano allo studente di esplorare l'Internet of Things.	In questa sezione, gli studenti dovrebbero trovare diversi contenuti relativi all'IoT, vale a dire: video, notizie, siti Web o articoli. In questa sezione potranno esplorare Strumenti e Contenuti IoT, identificando più potenziale, oltre a riconoscere più esempi dei potenziali pericoli derivanti dall'utilizzo di dispositivi che utilizzano questo tipo di tecnologia (chiamati IoT Devices o Internet of Things Devices).	Computer con accesso a Internet.
8 - Esercizio finale (tempo: 10 min.) (Risposta Multipla)	Valutare se lo studente ha familiarità con il concetto di IoT, può identificare gli strumenti, nonché i benefici, i pericoli e i rischi di questa tecnologia.	L'esercizio finale segue tutti i contenuti presentati in precedenza, per validare l'acquisizione di conoscenze attraverso di essi. In questa sezione verranno poste allo studente diverse domande, che coinvolgono argomenti più generali, nonché altri relativi ai vantaggi e ai pericoli dell'utilizzo delle tecnologie IoT.	- Computer con accesso a Internet.

Per questo modulo sono previsti quattro materiali multimediali, ovvero un video e tre quiz interattivi.

Video - Si tratta di un materiale video che introduce i discenti all'Internet of Things e spiega cos'è e che deve essere utilizzato nella prima fase della lezione. Può essere un punto di partenza per discutere con gli studenti dei vari dispositivi IoT che utilizzano quotidianamente.



Quiz 1

Un quiz in cui gli studenti rispondono a domande relative al concetto di Internet of Things. Il loro compito è quello di segnare le risposte corrette. Può essere utilizzato già nella prima parte della lezione come riassunto del compito introduttivo sull'argomento. Il risultato del quiz mostrerà se gli studenti hanno compreso il concetto di Internet of Things.

1) Selezionare l'opzione più adatta. L'Internet of Things (IoT) è costituito da:

- a) Sfruttare la tecnologia applicandola ai dispositivi di uso quotidiano, creando attraverso la connettività una rete di dispositivi che comunicano tra loro in modo efficiente, consentendo l'automazione di attività ricorrenti. (Corretto)*
- b) Trasformare i dispositivi in modo che abbiano accesso a Internet, facilitando i processi di comunicazione.*
- c) interconnettere più dispositivi tramite Internet, consentendo loro di comunicare tra loro.*

2) Selezionare i tipi di componenti utilizzati:

- a) Dispositivi*
- b) Reti di comunicazione*
- c) Sistemi di controllo*
- d) Tutti i precedenti (corretto)*

3) *Identificare i dispositivi che possono essere integrati nell'IoT:*

- a) *Aria condizionata*
- b) *Frigorifero*
- c) *Prese di corrente*
- d) *interruttori*
- e) *microonde*
- f) *Tutti i precedenti (corretto)*
- g) *Nessuno dei precedenti*

4) *Esempi di applicabilità*

- a) *Un aspirapolvere può essere programmato per pulire la casa dopo l'ora di andare a letto.*
- b) *Le lampade di casa possono emettere luci di tonalità specifiche in vari momenti della giornata, oppure spegnersi quando tutti escono.*
- c) *L'aria condizionata può accendersi cinque minuti prima del vostro arrivo, lasciando la stanza alla temperatura corretta.*
- d) *Gli ospedali possono utilizzare apparecchiature in grado di raccogliere i dati memorizzati su smartwatch o braccialetti intelligenti, ottimizzando il servizio e facilitando la diagnosi.*
- e) *Tutti i precedenti (corretto)*



Quiz 2

Questo quiz affronta i pericoli dell'IoT e i comportamenti associati all'uso sicuro dell'IoT. Si tratta di rispondere alle domande che appaiono sullo schermo barrando le risposte corrette. Il quiz si riferisce al video presentato in classe. Il contenuto dell'esercizio è presentato di seguito.

- 1) *Nel caso dello studio precedente, quale tipo di dispositivi presentava una falla di sicurezza?*
 - a) Pompe per insulina (corretto)
 - b) Misuratori di glicemia
 - c) Tutti i precedenti
- 2) *Qual è il rischio che questo dispositivo sia controllato da un hacker?*
 - a) Può essere disattivato, con conseguenze per l'utente.
 - b) Variazioni improprie dei livelli di insulina somministrata. (A destra)
 - c) Variazione dei livelli di glucosio somministrati.
- 3) *Come possono le aziende prevenire questo tipo di attacchi?*
 - a) Monitorare i rischi
 - b) Essere proattivi
 - c) Tutti i precedenti (corretto)
- 4) *Nel video che avete visto, quali dispositivi IoT sono stati analizzati?*
 - a) serratura, bambola e router
 - b) bambola, serratura e brocca elettrica (bollitore) (Corretto)
 - c) smartwatch, bambola e brocca elettrica
 - d) telecamera di sicurezza, microonde e lucchetto
- 5) *Quali misure di sicurezza dovremmo adottare? (Selezione multipla)*
 - a) Regolamentare l'uso della tecnologia.
 - b) Utilizzare password complesse e più sicure.
 - c) Mantenere i sistemi aggiornati.
 - d) Utilizzare i dispositivi IoT su una rete separata.



Quiz 3

Un altro quiz relativo all'uso degli oggetti dell'Internet of Things. Contiene domande a risposta singola e multipla. Gli studenti segnano le risposte corrette sullo schermo del computer. Tutte le domande del quiz sono riportate di seguito.

1) Quali sono i vantaggi dell'IoT? (Selezionare tutte le opzioni applicabili)

- a) Monitoraggio dei dati (corretto)
- b) Dispositivi in tempo reale
- c) Multi-Tasking (corretto)
- d) Migliore gestione del tempo (corretto)
- e) Minore controllo
- f) Costo (corretto)

2) Posso utilizzare una spina intelligente per alimentare il mio computer?

- a) Sì (corretto)
- b) No

3) Selezionare uno degli svantaggi dell'IoT:

- a) Monitoraggio dei dati
- b) Violazione dei dati (corretto)
- c) Meno controllo
- d) Maggiore occupabilità

4) Quale dei seguenti sistemi non è un assistente virtuale?

- a) Amazon Homekit (corretto)
- b) Assistente Google
- c) Amazon Alexa
- d) Apple HomeKit
- e) Tutti i precedenti

5) *Quale delle tecnologie non è coinvolta nell'IoT?*

- a) Connettività
- b) Piattaforme di cloud computing
- c) Sensori ad alta potenza (corretto)
- d) Apprendimento automatico e analisi avanzata
- e) Intelligenza artificiale (AI)

6) *I dispositivi IoT possono essere utilizzati per migliorare l'assistenza nel settore sanitario?*

- a) Sì (corretto)
- b) No

7) *Come posso stare al sicuro quando utilizzo un dispositivo IoT?*

- a) Mantenere il sistema aggiornato.
- b) Utilizzare una rete separata per i dispositivi IoT.
- c) Evitare i marchi sconosciuti.
- d) Tutti i precedenti (corretto)
- e) Nessuna delle precedenti.

Lezione 3

-

AI, Big Data e Cloud

L'obiettivo della terza lezione è quello di acquisire conoscenze sui Big Data, sull'intelligenza artificiale e sul concetto di cloud, e di essere in grado di valutare criticamente questi fenomeni, di cui oggi ogni persona fa parte. Un altro obiettivo è quello di acquisire conoscenze sui legami tra le persone, sia individui che società, e i sistemi intelligenti computerizzati e su larga scala.

La capacità di raccogliere ed elaborare dati sta diventando un fattore sempre più importante. Per Big Data si intende la tendenza a cercare, recuperare e raccogliere informazioni da una varietà di fonti per poi analizzarle e utilizzarle per i propri scopi. L'aspetto più importante dei Big Data è quindi l'elaborazione delle informazioni e l'applicazione pratica delle loro conclusioni, piuttosto che la raccolta dei dati stessi. I Big Data sono oggi onnipresenti. Le entità che li utilizzano nelle loro operazioni sono, ad esempio, le banche, che raccolgono dati derivanti dai movimenti sui conti degli utenti, come i pagamenti effettuati, il loro volume e i tipi di beni acquistati. Le aziende che rilasciano le proprie applicazioni che vengono scaricate dagli utenti su smartphone o tablet sono un altro esempio. Installando il programma sul proprio dispositivo, il più delle volte si acconsente automaticamente all'accesso dell'applicazione ai propri dati. Anche i portali online che raccolgono dati attraverso i servizi che forniscono costituiscono un altro esempio.

Dopo aver fornito un elenco generale di esempi di insiemi di big data, il formatore può consentire ai partecipanti di proporre alcuni esempi propri. Idealmente, questi dovrebbero essere raccolte con cui hanno a che fare quotidianamente. Dopo aver elencato alcuni insiemi di Big Data, si può chiedere ai discenti di elencare i dati che vengono raccolti e di pensare a quali vantaggi può apportare all'ente l'analisi dei dati raccolti.

L'intelligenza artificiale (AI) è anche l'argomento di questa lezione. Può essere intesa come la capacità delle macchine di mostrare abilità umane come il

ragionamento, l'apprendimento, la pianificazione e la creatività. L'intelligenza artificiale consente ai sistemi tecnici di percepire l'ambiente circostante, di gestire ciò che percepiscono e di risolvere i problemi lavorando verso un obiettivo specifico. Il computer riceve i dati già preparati o raccolti con i suoi sensori, li elabora e reagisce. Si prevede che le applicazioni future dell'IA porteranno enormi cambiamenti, ma l'intelligenza artificiale è già presente nella nostra vita quotidiana.

Nella quinta fase della lezione, c'è un altro esercizio in cui il formatore incoraggia i discenti ad avere una discussione collegata all'esercizio uno. Il compito è quello di creare una nota in cui gli studenti scrivono come immaginano che l'intelligenza artificiale possa implementare soluzioni ai problemi sociali, aiutando l'umanità nel suo complesso. Il formatore può dare alcuni spunti per incoraggiare la discussione tra i partecipanti:

- *Sanità - analisi dei dati sanitari e riconoscimento dei modelli, che possono portare a nuove scoperte mediche e a una migliore diagnostica.*
- *Protezione civile - utilizzando un'ampia gamma di dati e il riconoscimento di modelli, l'intelligenza artificiale può fornire un allarme precoce di disastri naturali e consentire una preparazione efficace e la mitigazione delle conseguenze.*
- *Prevenzione della disinformazione e degli attacchi informatici - L'IA può rilevare fake news e disinformazione controllando le informazioni dei social media, cercando parole preoccupanti e identificando fonti di dati credibili. I sistemi di IA possono aiutare a identificare e combattere gli attacchi informatici e altre minacce informatiche basandosi sull'inserimento continuo di dati, sul riconoscimento dei modelli e sul tracciamento degli attacchi.*
- *Ambiente e fauna selvatica: l'intelligenza artificiale aiuta a proteggere la natura e l'ambiente monitorando le popolazioni di specie a rischio.*
- *Infrastrutture - l'intelligenza artificiale può migliorare gli ostacoli infrastrutturali come il consumo energetico, la gestione dell'acqua e dei rifiuti.*

MODULO:

Indicazioni per lo sviluppo di Internet, costruzione attiva di una comunità globale di cittadini elettronici

UNITA':

3

TEMA:

Intelligenza Artificiale, Big Data e Cloud.

RISULTATI DI APPRENDIMENTO:

- Acquisizione di intuizioni fondate su cosa siano Intelligenza Artificiale, Big Data e Cloud.
- La capacità di spiegare concetti relativi al lato client, lato server, ai dati, al calcolo e all'uso di calcoli derivati da grandi set di dati.
- La capacità di valutare criticamente i sistemi AI, Big Data e Cloud di cui tutti facciamo parte.
- Acquisizione di intuizioni fondate sui legami tra persone (individui e società) e sistemi informatici, su larga scala, intelligenti.

FASI	OBIETTIVO	PROCEDURE	RISORSE
1 – Intelligenza Artificiale, Big Data e Cloud: un'introduzione (tempo: 10 min.) (Video)	Fornisci agli studenti intuizioni pratiche sulle nozioni di AI, Big data e cloud computing che siano riconoscibili, piuttosto che troppo "tecnologiche"	Gli studenti sono esposti a contenuti video, che - Introduci idee attuali sull'intelligenza artificiale e sul perché le persone ne parlano così tanto in questi giorni. - Spiegare come e perché esistono i Big Data, con nozioni di base sulle architetture client-server utilizzando esempi come gli account di ricerca di Google. - Mettere in relazione Big Data e Cloud, utilizzando lo stesso esempio dell'account Google. - Spiega perché la crescita di Internet e l'aumento delle grandi applicazioni client-server hanno creato una perfetta opportunità di sinergia per AI, Big Data e Cloud.	Computer con accesso a Internet. Video dell'allenatore

2 - Esercizio 1 Identificare ed esaminare i sistemi AI/Big Data/Cloud di cui facciamo parte. (tempo: 20 min.) Apprendimento tramite valutazione	Identificare i sistemi AI/Big Data/Cloud di cui facciamo parte e disporre di una struttura per valutare ciò che fanno, come ci relazioniamo con ciò che fanno, come sono vantaggiosi per noi e quali precauzioni dobbiamo prendere riguardo a questi sistemi.	1. Presentiamo allo studente un elenco di criteri di valutazione (in varie aree) relativi a come i dati vengono registrati, archiviati, elaborati e applicati in modi che influenzano la vita delle persone (ad esempio, produttività, salute e altri). 2. Gli studenti sono quindi incoraggiati a identificare almeno due applicazioni che utilizzano AI, Big Data e Cloud. Forniamo un elenco generale di esempi dopo aver permesso allo studente di elaborare alcune opzioni da solo. 3. Gli studenti valutano le candidature scelte utilizzando i criteri di valutazione, annotando le proprie osservazioni e valutazioni per ciascun criterio. 4. Gli studenti sono quindi incoraggiati a registrare un promemoria vocale che spieghi la loro valutazione di una delle due applicazioni in modo sintetico e articolato. 5. Il gruppo docente chiede agli studenti il loro consenso per utilizzare i propri dati audio per supportare la costruzione di un sistema AI/Big Data/Cloud based che possa in futuro aiutare gli studenti di quest'area in modo autonomo.	- 1. Computer con accesso a Internet. - 2. Un dispositivo per prendere appunti fisico o digitale, ad es. un taccuino o un blocco note. - 3. Infografica PDF fornita
3 – Dargli un senso: articolare e relazionarsi. (tempo: 10 min.) Attivazione di nuove conoscenze attraverso l'articolazione e l'introspezione	Articolazione e creazione di significato su concetti che sono probabilmente molto nuovi per il pubblico.	In questo esercizio, gli studenti sono incoraggiati a fare un'introspezione individuale basata sulla valutazione che hanno eseguito nell'esercizio precedente. L'idea principale è che identifichino come AI/Big Data e il Cloud stiano già svolgendo un ruolo nelle loro vite, nonché come potrebbero diventare importanti nel loro futuro. Qui incoraggiamo gli studenti a diventare consapevoli di quanto sia importante capire, almeno a un livello di base, come funzionano questi sistemi e come svolgono un ruolo nella vita degli individui e delle società. Gli studenti possono portare idee sull'equità e l'etica in questo esercizio.	Un dispositivo per prendere appunti fisico o digitale, ad esempio un taccuino o un blocco note.

4 Caso di studio: Facebook (tempo: 20 minuti) Valutazione e analisi dei potenziali pericoli: caso di studio	Comprendi come le applicazioni AI/Big Data/Cloud presentano potenziali pericoli intrinseci e cosa possiamo fare al riguardo.	Forniamo un video che discute di come una combinazione di AI, Big Data e Cloud sia stata utilizzata per sperimentare la manipolazione delle emozioni delle persone. Gli studenti sono incoraggiati ad analizzare questo contenuto in modo strutturato, evitando speculazioni. Forniamo anche una procedura di valutazione che integra i criteri di valutazione presentati in (2) come Infografica PDF. Video in inglese: https://www.youtube.com/watch?v=Tslr8o2CxnQ	1. Computer con accesso a Internet. - 2. Un dispositivo per prendere appunti fisico o digitale, ad es. un taccuino o un blocco note. - 3. Video di YouTube
5 – Esercizio 2. Immagina un mondo in cui AI/Big Data e il cloud lavorano per il bene sociale (tempo 15 min.) AI/Big Data, il Cloud, il futuro e il Social Good	Metti in pratica le intuizioni in questo contesto immaginando possibili aree di applicazione che sarebbero utili allo studente e alla sua comunità	Questo esercizio si basa sul blocco appunti creato nell'esercizio 1. Ci si aspetta che gli studenti creino una seconda sezione/capitolo in cui immaginano come le tecnologie AI, Data Driver potrebbero implementare soluzioni ai problemi sociali, aiutando l'umanità nel suo insieme. Forniamo alcuni suggerimenti per affermarli (guida PDF), come aiutare le comunità di anziani, sostenere l'inclusione sociale e la diversità o risolvere i problemi relativi all'insegnamento online per bambini	1. Un dispositivo per prendere appunti fisico o digitale, ad esempio un taccuino o un blocco note. 2. Guida PDF fornita.
6 – Riflessione e messaggio da portare a casa (tempo 5 min.) Chiusura attività	Consolidare nella mente dello studente le idee e le pratiche che vale la pena ricordare dopo la sessione	Gli studenti sono incoraggiati a considerare il proprio quaderno come una nuova esperienza di apprendimento. L'obiettivo è aggiungere una nuova sezione/capitolo con due elementi: 1. Qual è la cosa più importante che ho imparato in questa sessione? 2. Quali passi posso intraprendere per portare questa conoscenza in azioni?	Un dispositivo per prendere appunti fisico o digitale, ad es. un taccuino o un blocco note.

Questo programma di lezioni è accompagnato da due quiz multimediali, disponibili sulla piattaforma "iAware".



Quiz 1

Questo quiz può essere utilizzato alla fine della lezione come riepilogo di ciò che i discenti dovrebbero sapere dopo la lezione e può essere svolto insieme, ad esempio su una lavagna interattiva, o da ciascun discente individualmente sul proprio computer/tablet. Il formatore può anche chiedere ai discenti di fare il quiz a casa come compito di autovalutazione. Il quiz consiste in dieci domande a cui rispondere VERO o FALSO. Il contenuto del quiz con le risposte corrette è riportato di seguito.

1. *Le aziende tecnologiche come Google e Meta (ex Facebook) sono in grado di anticipare le nostre esigenze grazie all'IA addestrata sui Big Data e di mostrare gli annunci di conseguenza. VERO*
2. *Il cloud computing offre una serie di complicati servizi tecnologici, quindi è utilizzato solo dalle aziende. FALSO*
3. *L'intelligenza artificiale addestrata sui Big Data può imparare più cose su di noi di quante ne sappiamo noi stessi. VERO*
4. *I Big Data riguardano solo la raccolta di dati web. FALSO*
5. *Più bassa è la varietà dei Big Data (fino a una certa soglia), meglio è per l'addestramento dell'IA. FALSO*
6. *Le aziende tecnologiche possono sapere molto di noi anche se non abbiamo interagito direttamente con loro. VERO*
7. *Il virtuale è la principale delle 3 V nei Big Data. FALSO*
8. *Il Cloud Computing è un mercato che offre servizi informatici tramite onde radio. FALSO*
9. *Quando le aziende tecnologiche acquisiscono altre aziende, si occupano soprattutto dei Big Data che hanno raccolto e dei dati che potranno essere raccolti in futuro. VERO*
10. *Il Cloud Computing può essere utilizzato in modo continuo o a intervalli irregolari e poco frequenti, il che lo rende molto versatile. VERO*



Quiz 2

Il quiz contiene diverse domande a cui gli studenti devono rispondere segnando la risposta corretta sullo schermo. Può essere svolto individualmente a casa con gli studenti. Il contenuto del quiz, con una X che indica le risposte corrette, è riportato di seguito.

1. Il concetto di Big Data si riferisce a

- a) Solo dati strutturati*
- b) Solo dati non strutturati*
- c) Dati strutturati e non strutturati X*

2. Di solito, qual è l'obiettivo principale dell'utilizzo dei Big Data e dei grandi insiemi di dati?

- a) Trovare modelli di business ripetibili X*
- b) Migliorare il test del software*
- c) Tenere il passo con le modifiche normative*

3. Come può l'IA aiutare l'agricoltura?

- a) Rilevamento in tempo reale delle condizioni del terreno, previsioni meteo tramite app*
- b) L'intelligenza artificiale non può aiutare l'agricoltura e le altre industrie pesanti X*
- c) Convincere un maggior numero di persone a entrare nel settore agricolo.*
- d) Produrre più raccolti*

Cittadinanza elettronica

Una e-society è anche nota come società dell'informazione. La caratteristica fondamentale di questo tipo di società è la gestione delle informazioni, il loro rapido flusso e la loro elaborazione. Il bene più importante nella società dell'informazione è l'informazione e Internet è diventato un mezzo che determina quasi ogni sfera dell'attività umana. Ha un impatto sul tempo libero, sulla gestione degli affari, ma anche sulle questioni ufficiali. I cittadini digitali fanno parte della società digitale. Usano la tecnologia digitale per impegnarsi con la comunità e agire insieme ad essa.

La cittadinanza digitale può essere intesa come il legame tra utenti e creatori del mondo digitale e il conseguente atteggiamento di creazione e utilizzo consapevole e responsabile delle nuove tecnologie a beneficio di sé stessi e della società. Ciò significa che un e-cittadino deve conoscere l'impatto delle nuove tecnologie sulle persone, conoscere i diritti e le responsabilità e le competenze per utilizzare gli strumenti tecnologici digitali in modo sicuro.

Gli obiettivi di questa lezione sono la comprensione del concetto di cittadinanza digitale, l'acquisizione della capacità di identificare i diritti e le responsabilità di un cittadino digitale e la capacità critica nei confronti dei cambiamenti apportati dalla digitalizzazione nelle società moderne. Nella prima fase della lezione, gli studenti guardano un video sulle dimensioni della cittadinanza digitale. Gli aspetti presentati sono illustrati di seguito.

Le nove dimensioni della cittadinanza digitale illustrate nel video comprendono:

- *Capacità di utilizzare le nuove tecnologie*
- *Accesso a Internet*
- *Diritti e libertà civili*
- *Salute*

- *Comunicazione*
- *Condizioni legali*
- *Sicurezza*
- *Netiquette*
- *Commercio*

La parte successiva della lezione si basa sull'analisi del sistema di fiducia sociale cinese. Si tratta di un sistema implementato in Cina per monitorare e valutare il comportamento dei cittadini in termini di rispetto della legge e delle regole del rapporto sociale. Il sistema si basa su database che ricevono informazioni da tutti i tipi di registri statali, tribunali, enti della pubblica amministrazione, ma anche da monitoraggi cittadini o applicazioni mobili. L'idea alla base della creazione del Social Trust System in Cina è quella di costruire una società con un alto livello di fiducia, in cui gli individui e le organizzazioni rispettino la legge e gli standard non legali della vita sociale. A tal fine, vengono assegnate valutazioni sociali ai cittadini in base al loro comportamento, che si traducono direttamente in agevolazioni o svantaggi nella vita quotidiana.

L'analisi di questo sistema in classe consiste nel trovare informazioni nelle informazioni (potete guardare il video di YouTube registrato nello script) e discuterle. Gli studenti devono essere in grado di elencare i vantaggi e gli svantaggi del sistema di credito sociale e di discuterne l'applicazione nelle società democratiche europee.

MODULO:

Indicazioni per lo sviluppo di Internet, costruzione attiva di una comunità globale di cittadini elettronici

UNITA':

4

TEMA:

Cittadini elettronici, punteggi sociali ed essere umani nelle società moderne

RISULTATI DI APPRENDIMENTO:

- Gli studenti comprenderanno il concetto di cittadinanza digitale.
- Gli studenti saranno in grado di identificare i diritti e le responsabilità del cittadino digitale.
- Gli studenti discuteranno del sistema di credito sociale, basato sul caso di studio del sistema di credito sociale cinese.
- Gli studenti potranno riflettere in modo creativo sui cambiamenti portati dal digitale nelle società contemporanee.

FASI	OBIETTIVO	PROCEDURE	RISORSE
1 – Introduzione al concetto di cittadinanza digitale (tempo: 15 min.) (Video)	Gli studenti comprenderanno il concetto di cittadinanza digitale.	Lo studente assisterà alla spiegazione sul concetto di cittadinanza digitale - Cos'è la cittadinanza digitale; - Le 9 dimensioni della cittadinanza digitale; - Esempi delle 9 dimensioni della cittadinanza digitale. Video: https://www.youtube.com/watch?v=f4B0q2oOLbs&ab_channel=TeachingsinEducation	Computer con accesso a Internet.
2 - Esercizio 1 Esercitazione sulla cittadinanza digitale (tempo: 10 min.) (Risposta Multipla)	Comprendere se la conoscenza è stata acquisita dallo studente, attraverso un esercizio a scelta multipla.	Viene presentato un elenco di definizioni ed esempi relativi alla cittadinanza digitale. Lo studente dovrà scegliere l'opzione più appropriata in ogni caso.	Computer con accesso a Internet.

3 – Esercizio 2 Diritti e responsabilità della cittadinanza digitale (Vero / Falso) (tempo: 10 min.)	Attraverso un'esplorazione approfondita di ciascuna delle dimensioni della cittadinanza digitale, lo studente deve identificare i diritti e le responsabilità della cittadinanza.	Viene presentato un elenco di situazioni e gli studenti dovranno identificare quali delle situazioni sono diritti o responsabilità del cittadino digitale.	Computer con accesso a Internet.
4 - Riepilogo (tempo: 5 min.) (PDF File)	Consolidare le conoscenze e raccogliere informazioni in un unico documento, in modo accessibile.	Dopo aver completato l'esercizio, lo studente avrà accesso a un documento che includerà un elenco di definizioni sulle dimensioni della cittadinanza digitale e un elenco di diritti e responsabilità in materia di cittadinanza digitale.	PDF.
5 – Caso di studio: il sistema di credito sociale cinese (tempo: 8 min.) (notizia)	Per visualizzare la conoscenza di una configurazione di cittadinanza basata sulla quantificazione delle azioni di cittadinanza, attraverso algoritmi e piattaforme.	Gli studenti leggeranno/guarderanno una notizia sul sistema di credito sociale cinese. News story: https://www.youtube.com/watch?v=0cGB8dCDf3c&ab_channel=NBCNews	Computer con accesso a Internet.
6 - Dibattito sui sistemi di credito sociale (tempo: 10 min.) (Riflessioni e dibattito)	Discutere l'attuazione (vantaggi e svantaggi) del sistema di credito sociale nelle società democratiche europee.	Gli studenti dovrebbero elencare i vantaggi e gli svantaggi del sistema di credito sociale e discutere la sua implementazione nelle società democratiche europee.	Computer con accesso a Internet.
7 - Manifesto per la cittadinanza digitale (tempo: 3 min.) (Video)	Conoscere le forme di partecipazione civica.	Lo studente leggerà/guarderà un estratto del Manifesto per la cittadinanza digitale. Video (integrale): https://www.youtube.com/watch?v=-aWRpwjj5VE&ab_channel=CentrodePesquisaAtopos	Computer con accesso a Internet.

8 – Esercizio 3 Scrittura creativa	Immagina, in modo creativo, come sarà la vita quotidiana degli esseri umani, nelle società del futuro	Lo studente deve usare l'immaginazione, così come le conoscenze acquisite durante il corso, per scrivere un breve racconto (fino a 350 parole) o una poesia (fino a una pagina) su come la vita quotidiana dell'essere umano (o un aspetto della vita quotidiana) sarà nell'anno 3000, immaginando l'interazione tra uomo e tecnologia (IoT, AI, nuvole...).	Computer con Microsoft Word o altro software di elaborazione testi.
9 - Risorse – Essere umani nelle società moderne	Fornire contenuti che consentano allo studente di esplorare il pensiero sociale contemporaneo sull'essere umano nelle società moderne.	Gli studenti troveranno diversi contenuti legati al tema, di diversa tipologia, ovvero: video, news, siti web e articoli.	Computer con accesso a Internet.
10 – Esercizio finale	Valutare se lo studente ha familiarità con il concetto di cittadinanza digitale e se può identificare i diritti e i doveri del cittadino digitale.	L'esercizio finale segue tutti i contenuti presentati in precedenza e mira a confermare l'acquisizione delle conoscenze. Verranno poste allo studente diverse domande, riguardanti temi legati alla cittadinanza digitale, ai diritti e alle responsabilità del cittadino digitale.	Computer con accesso a Internet.

Per questo piano didattico sono previsti due quiz multimediali.



Quiz 1

Il quiz può essere svolto con gli studenti durante la lezione o si può chiedere loro di farlo da soli a casa. Il quiz consiste in frasi vere o false. Il compito del discente è leggere la frase, analizzarla e segnare la risposta corretta - vera o falsa?

Risposta Vero o Falso

- La cittadinanza digitale si riferisce all'uso responsabile della tecnologia da parte di chiunque utilizzi computer, Internet e dispositivi digitali per impegnarsi nella società a qualsiasi livello. (Vero)

Risposta Vero o Falso

- La cittadinanza digitale negativa comporta il cyberbullismo, l'uso irresponsabile dei social media e una generale mancanza di conoscenze su come utilizzare Internet in modo sicuro (Vero)



Quiz 2

Il quiz consiste in due tipi di domande: un test a risposta singola e un compito vero/falso. Il discente segna le risposte corrette sullo schermo del computer o del dispositivo mobile. Il contenuto del quiz e le risposte corrette sono riportati di seguito.

Indicare la risposta corretta

- 1 - L'impronta digitale si riferisce alle nostre credenziali di accesso ai social network.
- 2 - La nostra carta del cittadino
- 3 - Le informazioni personali che lasciamo quando utilizziamo Internet (x)
- 4 - Nessuna delle risposte è corretta

Vero o falso?

- Quando utilizziamo per il nostro lavoro un contenuto (un'immagine o un testo, per esempio) che troviamo su Internet, non è necessario indicarne l'origine o l'autore perché ciò che si trova su Internet può essere utilizzato da tutti (F)



CAPITOLO 5

STRUMENTI PER LA VALUTAZIONE DEI LIVELLI DI COMPETENZA ICT

ICT

Le competenze digitali sono un insieme di abilità oggi fondamentali; sono la combinazione di conoscenze, abilità e attitudini che consente alle persone di vivere, imparare e lavorare in una società digitalizzata. L'alfabetizzazione digitale influenza il progresso in aree di vitale importanza per l'individuo e la società nel suo complesso, come la qualità della vita, l'economia, la sanità, l'istruzione, la scienza, la sicurezza, l'agricoltura, la cultura e il tempo libero.

Le competenze digitali sono state riconosciute dal Parlamento europeo tra le otto competenze chiave necessarie per l'apprendimento permanente. Esse sono collegate a una serie di competenze che tutti i cittadini dell'Europa del XXI secolo dovrebbero possedere per garantire la loro partecipazione attiva alla vita sociale ed economica.

Oggi le competenze digitali sono molto richieste. Sempre più servizi e attività si spostano verso la sfera digitale e Internet. Le questioni ufficiali e mediche, il lavoro e l'apprendimento sono tutti ambiti che è sempre più facile padroneggiare con le giuste competenze digitali. La pandemia COVID, in particolare, lo ha dimostrato. Già oggi molte attività quotidiane sono molto più difficili o addirittura impossibili senza l'uso di un computer o di uno smartphone. Vale quindi la pena di sviluppare le proprie competenze digitali e incoraggiare gli altri a fare lo stesso.

DIGCOMP

Come indicato nei paragrafi precedenti, il Parlamento europeo e il Consiglio d'Europa hanno identificato la competenza digitale come una delle otto competenze più importanti per l'apprendimento permanente. Tali competenze sono necessarie per la partecipazione attiva nella società e costituiscono le abilità di base attraverso le quali è possibile sviluppare competenze specifiche. In quest'ottica, la competenza digitale può essere definita come l'uso libero e critico delle tecnologie dell'informazione e della comunicazione per raggiungere obiettivi legati al lavoro, all'occupazione, all'apprendimento, al tempo libero e alla partecipazione alla società. La competenza digitale fa parte delle competenze trasversali, cioè è presente e persino essenziale per l'acquisizione di competenze in altre aree, ad esempio le competenze linguistiche o la consapevolezza culturale. Pertanto, si è cercato di definire quali siano effettivamente queste competenze digitali e quale sia la loro portata. DigComp, un quadro di riferimento per lo sviluppo e la comprensione delle competenze digitali in Europa (Digital Competence Framework), è stato preparato e pubblicato per la prima volta nel 2013 dalla Commissione europea. L'obiettivo era quello di creare uno strumento per migliorare le competenze digitali dei cittadini e per aiutare a pianificare iniziative di istruzione e formazione al fine di migliorare il livello delle competenze digitali.

Il Quadro Europeo delle Competenze Digitali dei cittadini, noto come DigComp, sviluppato dalla Commissione europea, è uno strumento per lo sviluppo delle competenze digitali dei cittadini. DigComp suddivide le 21 competenze considerate fondamentali in 5 aree. Inoltre, all'interno di queste aree ci sono diversi livelli di competenza (livelli A, B, C). Il quadro DigComp è stato progettato per facilitare la comprensione di cosa siano le competenze digitali e a cosa servano nel mondo di oggi.

Il quadro DigComp è suddiviso in cinque aree, tra cui:

1. *Informazioni*
2. *La comunicazione*
3. *Creazione di contenuti*
4. *Sicurezza*
5. *Risoluzione dei problemi*

Il modulo Informazioni è dedicato alla raccolta, all'organizzazione e alla conservazione delle informazioni digitali e alla valutazione della loro importanza e del loro scopo. Il modulo discute gli strumenti per il reperimento efficiente e sicuro delle risorse informative sul web, come organizzarle e come recuperare rapidamente le informazioni raccolte e conservate.

Il modulo Comunicazione è un compendio di conoscenze su come comunicare con altri utenti della rete, per mezzo di applicazioni e software, ampiamente disponibili tramite personal computer e dispositivi mobili, utilizzando le più recenti e gratuite tecnologie di comunicazione multimediale. Facilita l'organizzazione del lavoro professionale e privato e spiega le regole che lo governano per poter raggiungere rapidamente, legalmente ed efficacemente i propri obiettivi nel lavoro di gruppo e individuale.

Il modulo Creazione di contenuti è dedicato alla creazione e all'editing di nuovi contenuti (immagini, registrazioni audio e video, documenti di testo e presentazioni), alla combinazione creativa di informazioni provenienti da varie fonti e in varie forme all'interno di documenti, alle questioni relative alla protezione della proprietà intellettuale e alle licenze e all'introduzione alla programmazione. Oltre al minimo indispensabile di conoscenze teoriche, il modulo presenta l'uso pratico di software commerciali e gratuiti e di strumenti disponibili su Internet (conversione di file, modifica di registrazioni video, creazione di pagine web).

Il modulo Sicurezza è dedicato a come proteggere se stessi e i propri dispositivi elettronici dai pericoli a cui tutti gli utenti di Internet sono esposti. In particolare, vengono discussi l'uso di software antivirus, le funzioni di sicurezza

integrate nel sistema operativo, la gestione delle proprie identità digitali e i rischi per la salute legati all'uso delle moderne tecnologie.

Il modulo 5 Risoluzione dei problemi è rivolto a coloro che sono interessati ad auto-identificare e risolvere i problemi hardware e software più comuni e a come selezionare e acquisire in modo sicuro gli strumenti necessari per risolvere i problemi quotidiani utilizzando le TIC. Copre anche l'uso delle periferiche e come utilizzare le risorse multimediali e le TIC in modo creativo per aggiornare e approfondire la propria conoscenza delle competenze digitali e come adattare le soluzioni acquisite alle proprie esigenze.

Le aree possono essere suddivise in due tipi: le aree da 1 a 3 si concentrano, per definizione, su attività e applicazioni specifiche inerenti a queste aree, mentre le aree 4 e 5 possono essere indicate come tutte le attività che vengono svolte con strumenti digitali.

Ulteriori informazioni sul quadro DigComp (comprese le descrizioni delle competenze) sono disponibili sul sito web:

https://joint-research-centre.ec.europa.eu/digcomp_en.

Il programma sviluppato da "iAware" non è un'alternativa alla formazione secondo il quadro DigComp. È tuttavia una proposta per svilupparlo e portarlo a un livello superiore. Il contenuto non è duplicato e il programma di "iAware" estende e completa alcune competenze del quadro DigComp. Come si può notare, il programma "iAware" non presenta contenuti strettamente tecnici, ma si concentra sull'acquisizione di abilità pratiche, soprattutto per coloro che hanno scarse competenze digitali.

PANORAMICA DELLE CERTIFICAZIONI ICT

Il possesso di competenze informatiche è diventato indispensabile in molti settori professionali. Sempre più adulti sono interessati a ottenere un certificato per dimostrare le conoscenze e le competenze acquisite. Presentiamo una selezione di certificati che una persona con scarse competenze digitali può ottenere nei diversi partner del progetto.

ITALIA:

EIPASS

La certificazione EIPASS è senza dubbio una delle certificazioni informatiche più richieste e riconosciute dal Miur. Esistono diverse tipologie di certificazioni EIPASS, che si distinguono per il pubblico a cui sono rivolte: questi attestati riconosciuti di informatica possono essere conseguiti sia da giovani che da adulti, sono inoltre utili per ottenere crediti formativi e punti in più nelle graduatorie professionali.

EIRSAF

Per certificare le competenze informatiche e dimostrare di avere abilità con i dispositivi e i programmi tecnologici in uso corrente si possono anche indicare le certificazioni Eirsaf, riconosciute dal Ministero dell'Istruzione come valutabili nelle graduatorie di assunzione del personale docente.

ISTITUTO SALVEMINI

Sebbene sia meno conosciuta di altre, la certificazione informatica dell'Istituto Salvemini non va sottovalutata, in quanto fa parte anche delle

certificazioni informatiche riconosciute dal Ministero dell'Istruzione, e quindi valida sia a livello professionale che nel settore pubblico.

PORTOGALLO:

CERTIFICATO DI COMPETENZE DIGITALI

Il certificato di competenze digitali riconosce e certifica il livello di competenze digitali e mediatiche. Si può ottenere in due modi: uno frequentando un corso di formazione e l'altro testando le proprie competenze. Il certificato può essere ottenuto da persone di età pari o superiore ai 18 anni e i destinatari prioritari sono le persone con scarse competenze digitali e i giovani che non frequentano corsi di istruzione né lavorano.

POLONIA:

ITPASS

È un certificato conforme al quadro DigComp in tutte e cinque le aree di conoscenza. Conferma la competenza nelle TIC a tre livelli. L'esame può essere sostenuto al termine del corso o se il discente desidera verificare autonomamente le proprie competenze.

CEC

Il certificato ECCC è il Certificato Europeo di Competenza Digitale e copre una varietà di aree, tra cui diversi livelli di competenza. Ciò consente a tutti di adattare in modo flessibile il livello e la portata delle conoscenze da verificare. Inoltre, chiunque può sostenere gli esami ECCC (compresi gli studenti di diversi livelli scolastici) e allo stesso tempo può scegliere qualsiasi modulo e livello di certificazione delle proprie competenze.

Inoltre, esistono anche certificazioni internazionali molto diffuse, di cui un esempio è riportato di seguito:

ECDL (Patente europea del computer)

Si tratta di un certificato internazionale di competenze informatiche che, come un certificato linguistico, attesta la competenza nell'uso del software informatico. Si rivolge a coloro che desiderano sviluppare le proprie competenze e rimanere aggiornati con la tecnologia moderna. Non ci sono limiti di età nei diversi tipi di certificati ECDL. Per coloro che hanno una conoscenza digitale limitata, è stato introdotto il certificato ECDL e-Citizen. Le certificazioni ECDL si basano su competenze suddivise in diverse aree.

STRUMENTI DI VALUTAZIONE E AUTOVALUTAZIONE

La valutazione è il processo per determinare se un progetto ha raggiunto i suoi obiettivi e, nel caso della formazione, se i discenti hanno aumentato le loro conoscenze e competenze. La valutazione dei corsi svolti è essenziale perché indica se i discenti hanno acquisito le conoscenze e le abilità pratiche previste e se hanno aumentato le loro competenze in un determinato campo.

Per adattare il contenuto e il livello al gruppo di formazione, all'inizio del ciclo di formazione si può condurre un'indagine sul livello di conoscenza del discente. Questo può essere fatto sotto forma di un questionario stampato o utilizzando una serie di strumenti online. Ogni discente può anche utilizzare questi strumenti da solo, che lo aiuteranno a capire le proprie competenze digitali, a mostrare le aree in cui c'è una mancanza di competenza al livello appropriato e a facilitare la pianificazione del percorso formativo. Gli strumenti più comuni che si incontrano sono quelli basati sulle competenze descritte in DigComp.

MyDigiSkills

MyDigiSkills, è uno strumento di valutazione in linea con il modello DigComp 2.1 e basato su DigCompSAT. "The European Digital Competence Framework for Citizen", è disponibile in 7 lingue ed è stato tradotto in italiano da Formez PA nell'ambito del progetto "ACCEDI - Ambiente per la Cittadinanza Consapevole con l'Educazione Digitale" promosso da Repubblica Digitale in attuazione del Piano Operativo della Strategia Nazionale per le Competenze Digitali.

Gli interessati, dopo aver effettuato il test su MyDigiSkills, potranno in pochi mesi approfondire l'autovalutazione su ACCEDI e, sulla base delle aree di forza e di debolezza individuate, utilizzare le risorse a disposizione per superare eventuali gap di competenza digitale.

<https://mydigiskills.eu/index.php>

Test Europass

A questo proposito, è arrivato un nuovo strumento di autovalutazione molto utile per verificare le nostre competenze digitali. È stato proposto dalla Commissione Europea con l'obiettivo di aiutare gli studenti, ma anche chi ha già un lavoro o lo sta cercando, a capire il proprio livello di competenza rispetto al quadro di riferimento europeo. Nello specifico, si tratta di un test composto da una serie di domande che permettono di ricevere un report di valutazione dettagliato nelle diverse aree di competenza esaminate: Alfabetizzazione informatica, Comunicazione, Creazione di contenuti digitali, Sicurezza e Problem solving.

Sulla base della valutazione ottenuta, poi, la piattaforma vi darà i suggerimenti più adatti: quindi, corsi e opportunità di apprendimento basati sui risultati ottenuti, utili per migliorare le vostre competenze.

Voyager delle competenze digitali

Digital Skill Voyager è uno strumento sviluppato dal Ministero dello Sviluppo Economico e dalle Camere di Commercio italiane per la valutazione delle competenze digitali. Si rivolge a studenti e lavoratori e, più in generale, a tutti coloro che sono alla ricerca di uno strumento specifico per misurare le proprie competenze digitali e valorizzarle sul mercato del lavoro.

Digital Skill Voyager è un test online accessibile dal portale www.dskill.eu impostato con tecniche di gamification e, pur essendo uno strumento efficace e rigoroso, la sua esecuzione è divertente e dinamica.

Acceleratore di competenze digitali

È uno strumento di autovalutazione che fornisce una panoramica delle proprie competenze digitali secondo il quadro DigComp. Indica le competenze forti e quelle che devono ancora essere migliorate. Utilizzando questo strumento, è possibile confrontare i propri risultati con quelli degli altri e ottenere raccomandazioni sulla formazione. Al termine del test, i risultati vengono forniti sotto forma di "diagramma radar". Lo strumento può essere provato su

<http://www.digitalskillsaccelerator.eu/pl/learning-portal/online-self-assessment-tool/>

<https://digcomp.digital-competence.eu>

Questo strumento valuta il livello di ciascuna delle 21 competenze del quadro DigComp, suddivise in cinque aree tematiche. Il discente risolve un breve test e poi riceve un grafico colorato che indica il livello percentuale di ciascuna competenza.

LA BIBLIOGRAFIA

1. Aftański P. (2011), *Information society - the new value of the information*, *Dydaktyka informatyki* 6, p.66-73
2. Buregwa-Czuma S., Garwol K., *Definitions, properties, and functions of information society*, *Dydaktyka informatyki* 6, p.30-37
3. Cardoso, G., Costa, A., Conceição, C., and Gomes, M. (2005). *A Sociedade em Rede em Portugal*. Campo das Letras
4. Castells M., *Spółeczeństo w sieci*, Warszawa 2008
5. Costa, C., Tyner, K., Rosa, P. J., Sousa, C., & Henriques, S. (2018). *Desenvolvimento e Validação da Escala de Literacia Mediática e Informacional para Alunos dos 2º e 3º Ciclos do Ensino Básico em Portugal*. *Revista Lusófona de Educação*, 41, 11-28.
<http://dx.doi.org/10.24140/issn.1645-7250.rle41.01>
6. Cruz, J. (2008). *Evolução do fosso digital em Portugal 1997-2007: uma abordagem sociológica*. Instituto Superior de Ciências do Trabalho e da Empresa.
7. Czechowska-Derkacz, B. (2015). *Dziennikarstwo obywatelskie – o mediach w rękach odbiorców*. W: M. Łosiewicz, A. Ryłko-Kurpiewska (red.), *Media, business, culture*. T. 1, *Social and Political Role of the Media*. (s. 545-562). Kinvara Co. Galway: TrueSign; Gdynia: Novae Res.
8. Dias-Trindade, S., Moreira, J. A., & Nunes, C. S. (2019). *Escala de Auto-Avaliação de Competências Digitais de Professores: Procedimentos de Construção e Validação*. *Texto Livre: Linguagem e Tecnologia*, 12(2).
<http://dx.doi.org/10.17851/1983-3652.12.2.152-171>
9. *Digital Portugal*, <https://portugaldigital.gov.pt/en/>

10. *Goban-Klas T., Sienkiewicz P., Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji 1999*
11. *Golka M., (2005) Czym jest społeczeństwo informacyjne?, Ruch prawniczy, ekonomiczny i socjologiczny, rok LXVII, zeszyt 4*
12. *Harzyńska J. (2012), Metody pracy z uczniami dorosłymi, Edukacja Humanistyczna nr 1 (26), 201-206*
13. *Kompetencje przyszłości, red. nauk. Stefan M. Kwiatkowski, Fundacja Rozwoju Systemu Edukacji, Seria Naukowa, t. 3, Warszawa 2018*
14. *Krztoń W., XXI wiek – wiekiem społeczeństwa informacyjnego, Modern Menagement Review, MMR vol. XX, 22 (3/2015)*
15. *Kwiatkowska E., Rozwój internetu rzeczy - szanse i zagrożenia, internetowy Kwartalnik Antymonopolowy i Regulacyjny 2014, nr 8(3)*
16. *Lyon, D. (1992). A Sociedade da Informação. Celta Editora.*
17. *Making a European Area of Lifelong Learning a Reality, Komunikat Komisji Europejskiej, COM (2001) 678*
18. *Mikołajczyk K. (2011), Jak uczą się dorośli, czyli co powinien wiedzieć trener o specyfice kształcenia uczestników szkolenia, E-mentor nr 2 (39) / 2011*
19. *Morbitzer J. (2004), z metodyki wykorzystywania komputerów w edukacji, Dydaktyka Informatyki 1, 128-140*
20. *OECD (2019), Getting Skills Right: Future-Ready Adult Learning Systems, OECD Publishing*
21. *Olszewska S. (2013), Learning styles and activating methods in adult education, General and Professional Education, 2/2013 p. 20-25*
22. *Patrício, M. (2014). Aprendizagem Intergeracional com Tecnologias de Informação e Comunicação. Universidade do Minho.*

23. *Pereira, S., Pinto, M., & Moura, P. (2015). Níveis de Literacia Mediática: Estudo Exploratório com jovens do 12º ano. CECS/Universidade do Minho*
24. *Pizzirani, A., Di Gioia, R., Chaudron, S., Draper Gil, G. and Sanchez Martin, J., Privacy safeguards and online anonymity, EUR 28991 EN, European Commission, 2017, ISBN 978-92-79-77231-3, doi:10.2760/30934, JRC109792*
25. *Prywatność w sieci, Raport 2016/2017, IAB Polska*
26. *Punie, Y. and Brecko, B., editor(s), Ferrari, A., DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. , EUR 26035, Publications Office of the European Union, Luxembourg, 2013, ISBN 978-92-79-31465-0, doi:10.2788/52966, JRC83167*
27. *Rabka M., Internet XXI wieku – pułapka zagrożeń dla dzieci, młodzieży i osób starszych w dobie pandemii Covid-19, Współczesne Problemy Zarządzania, vol. 8, 1 (16), 2020, DOI:<https://doi.org/10.52934/wpz.85>*
28. *Rada Unii Europejskiej (2018), Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kluczowych kompetencji w uczeniu się przez całe życie. Dziennik Urzędowy Unii Europejskiej*
29. *Regulacje ws. sztucznej inteligencji: oczekiwania Parlamentu, Aktualności Parlamentu Europejskiego (21-10-2020)*
<https://www.europarl.europa.eu/news/pl/headlines/priorities/sztuczna-inteligencja-w-ue/20201015STO89417/regulacje-ws-sztucznej-inteligencji-oczekiwania-parlamentu>
30. *Rosa, P., Costa, C., Tyner, K., Sousa, C., & Henriques, S. (2019, July). Development and Validation of the Media and Information Literacy Scale (MILS) for the 2nd and 3rd Cycle of Basic Education in Portugal. Poster session presented at the XVI European Congress of Psychology, Moscow, Russia*
31. *ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO i RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu*

takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

32. *Sommer H., Sommer H., Michno J., Opportunities and threats of information society - selected aspects, Kultura – Przemiany – Edukacja, t. III (2015)*
33. *Sztuczna inteligencja: co to jest i jakie ma zastosowania?, Aktualności Parlamentu Europejskiego (04-09-2020),
<https://www.europarl.europa.eu/news/pl/headlines/priorities/sztuczna-inteligencja-w-ue/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania>*
34. *Sztuczna inteligencja: szanse i zagrożenia, Aktualności Parlamentu Europejskiego (24-09-2020),
<https://www.europarl.europa.eu/news/pl/headlines/priorities/sztuczna-inteligencja-w-ue/20200918STO87404/sztuczna-inteligencja-szanse-i-zagrozenia>*
35. *Szumilas-Praszek W., Wojtkowiak M., Internet jako współczesne medium zagrożenia czy edukacji?, Społeczeństwo i Rodzina, nr 37 (4/2013)*
36. *The Adult Education Survey (AES), 2016, Eurostat*
37. *Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48883-5,
[doi:10.2760/490274](https://doi.org/10.2760/490274), JRC128415*
38. *Wrońska, A., Rywczyńska, A. i Lew-Starowicz, R. (2020). Edukacja – relacja – zabawa. Wieloaspektowość internetu w wymiarze bezpieczeństwa dzieci i młodzieży. Warszawa: Fundacja Rozwoju Systemu Edukacji, Seria Naukowa, t. 6*