DIGITALISE ME

Competenze digitali di base per una partecipazione attiva alla vita civica e sociale

MODULO: SICUREZZA

RUTIS

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

Partner

RUTIS
A REDE QUE UNE AS UNIVERSIDADES SENIORES

Emphasys
CENTRE

VILLA GREPPI

ADR
Agenția pentru Dezvoltare Regională
N O R D - E S T

DOM SPAIN

IRIS
instytut re-integracji społecznej

DIGITALISE ME

Descrizione del modulo

Oggigiorno è difficile immaginare il mondo senza Internet e quindi senza cyberspazio.
Nel mondo sempre più dipendente dall'uso tecnologico, il cyberspazio è una delle sfide più sorprendenti del 21° secolo.
L'aumento dell'uso di Internet e del numero di dispositivi da cui è possibile accedervi ha creato numerose opportunità ma anche l'emergere di minacce reali e preoccupanti.
Allora...

Parliamo di sicurezza!

***Il modulo "SICUREZZA"** fornisce informazioni su come proteggersi quando si utilizzano nuove tecnologie come telefoni cellulari e computer.*
Affronteremo alcuni concetti e procedure che ci aiuteranno a navigare in sicurezza su Internet.
Impareremo a conoscere:

- *la terminologia e i concetti di base per l'utilizzo di Internet;*
- *a proteggere i dispositivi;*
- *a proteggere i dati personali e la privacy;*
- *a tutelare la nostra salute e il nostro benessere.*

DIGITALISE ME

Simboli chiave

1

DEFINIZIONI

2

SUGGERIMENTI

3

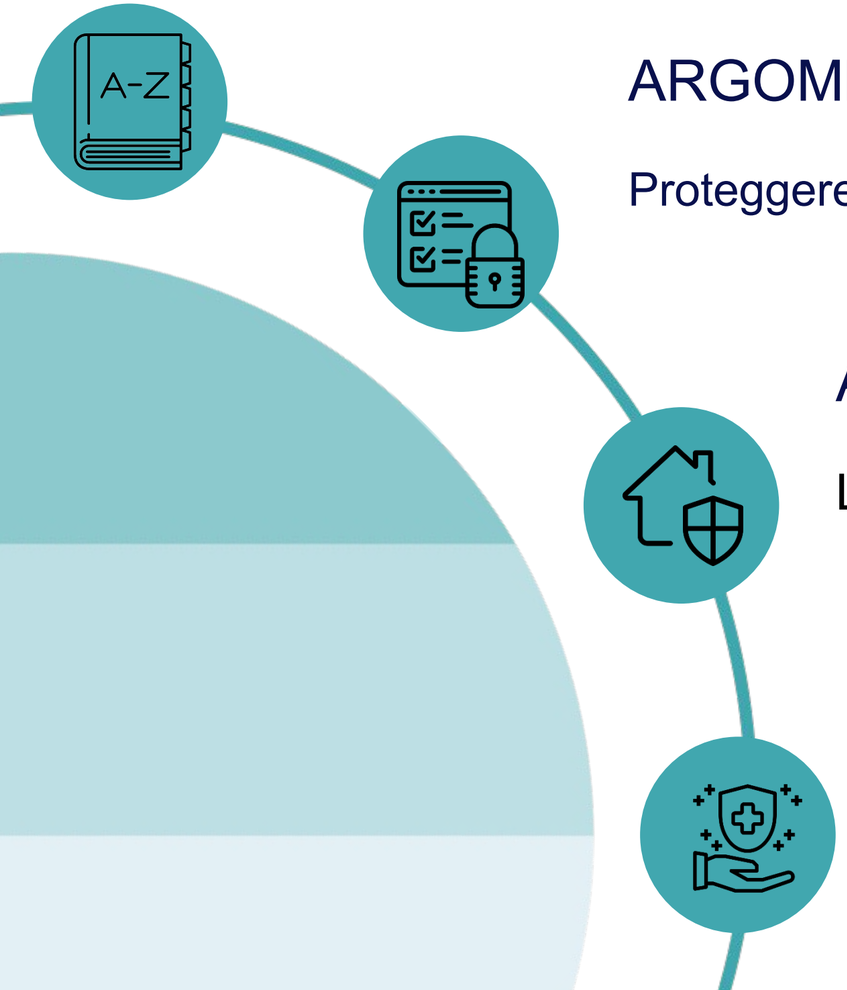
ATTIVITÀ

DIGITALISE ME

Argomenti

ARGOMENTO 1

La terminologia e i concetti di base per l’utilizzo di Internet



ARGOMENTO 2

Proteggere i dispositivi

ARGOMENTO 3

La protezione dei dati personali e la privacy

ARGOMENTO 4

La tutela della salute e del benessere

DIGITALISE ME

ARGOMENTO 1:
La terminologia e i concetti di base per l’utilizzo di Internet

Argomento 1: La terminologia e i concetti di base per l’utilizzo di Internet

INTRODUZIONE

L'obiettivo principale di questa lezione è fornire la terminologia e i concetti di base di Internet per garantire che il contenuto del modulo sulla sicurezza sia facilmente comprensibile.

Inoltre, conoscere i concetti di base associati ai computer/telefoni cellulari e all'uso di Internet aiuterà a comprendere i pericoli a cui siamo esposti e come possiamo navigare in sicurezza in Internet.

Scopriremo cosa sono *i firewall, i software antivirus e le app, nonché le differenze tra malware, spyware, virus, verme informatico, trojan, ecc., e approfondiremo le seguenti definizioni: cyberbullismo e cybercrime (crimine informatico).*

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Cosa è un firewall?

- È una barriera difensiva la cui funzione è fondamentalmente quella di bloccare il traffico dati indesiderato o dannoso e lasciare passare ciò che non è dannoso.

- È un'opzione di sicurezza basata su hardware* o software** che, da un insieme di regole o istruzioni, esegue un'analisi del traffico di rete per determinare quale trasmissione o ricezione dei dati/quali operazioni possono essere eseguite.

- Un firewall è il nome dato al dispositivo in una rete di computer che si propone di applicare una politica di sicurezza in un particolare punto di controllo della rete" (KUROSE, 2010).

- Come suggerisce il nome, un firewall è come un muro tagliafuoco che impedisce la propagazione del fuoco ad altre stanze di un edificio o di uno spazio; in questo caso, impedisce la diffusione della trasmissione dei dati.

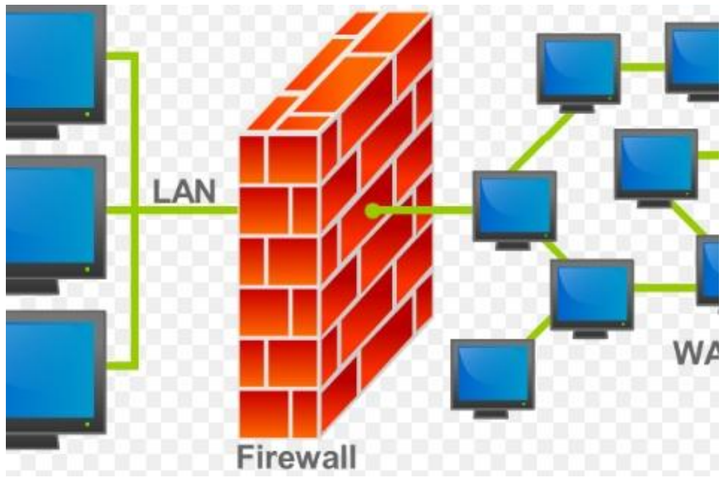
*L'hardware è costituito dalle componenti fisiche esterne di un computer.
** Il software è l'insieme di programmi e applicazioni che permette al computer o altro dispositivo di funzionare.

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l’utilizzo di Internet

ATTIVITÀ

- Lezione 1



Argomento 1: La terminologia e i concetti di base per l’utilizzo di Internet

Cos’è un software antivirus?

- Gli antivirus sono applicazioni che rilevano programmi dannosi e sono in grado di rimuoverli o di metterli in quarantena.
- Il software antivirus analizza costantemente il computer, i programmi o le applicazioni installati e anche le unità flash.
- L'antivirus è oggi una presenza fondamentale in ogni dispositivo informatico. Dalle postazioni di lavoro ai potenti server, da ogni personal computer al datacenter più evoluto, nella stragrande maggioranza di tutti sono presenti una o più soluzioni antivirus. Da quando si è iniziato a condividere file e a utilizzare i servizi di rete, virus, vermi informatici e altri contenuti dannosi sono diventati una presenza crescente nei computer. [Richardson, 2008].

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Software antivirus

- La crescita esponenziale dell'utilizzo di Internet con una larghezza di banda sempre più elevata ha portato a situazioni in cui virus (oltre a vermi informatici e altri tipi di contenuti dannosi) causano epidemie costanti con quantità impressionanti di computer infetti in tutto il mondo. [Ehm, 2008; Chen e Robert, 2004; Kamluk, 2008].

Examples

ATTIVITÀ

- Lezione 2

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Cosa sono le applicazioni (app)?

Programma o insieme di programmi progettato per aiutare gli utenti a svolgere attività sul telefono cellulare/tablet o sul computer.

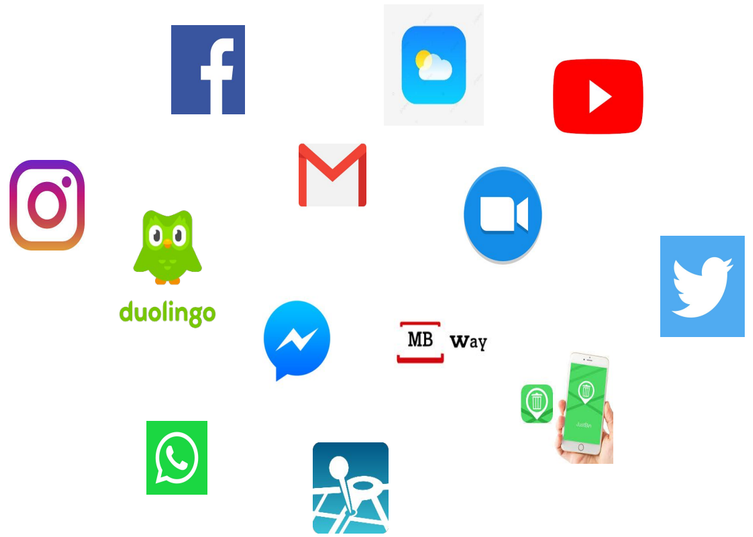
Le app servono per svolgere funzioni e facilitare le attività.

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l’utilizzo di Internet

Applicazioni (App)

Le app, parola che deriva dall’inglese "applicazioni", sono strumenti per il cellulare (simili ai programmi per computer). Nella sua definizione tecnica, un'applicazione è un software che di solito comporta l'elaborazione di dati. Questo tipo di programma deve soddisfare alcuni requisiti, tra gli altri: svolgere compiti, indipendentemente dalla complessità, elaborare dati in informazioni, organizzare e facilitare attività.



DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Applicazioni (app)

Le app possono essere utili in diversi modi. Possono aiutarti a risolvere semplici problemi nella vita di tutti i giorni, come fare una somma usando l'app della calcolatrice o pagare una bolletta tramite l'applicazione della banca. Possono anche fungere da fonte di ricerca, ad esempio per aiutarti a scoprire di più sul tuo artista preferito, trovare un ristorante in una città che stai visitando o metterti in contatto diretto con le persone o i negozi e i servizi che utilizzi di più.

La stragrande maggioranza delle app è gratuita, il che significa che non devi pagare per scaricarle e utilizzarle. Ma ci sono anche app che vengono vendute, come giochi, riviste, musica, libri, programmi avanzati, ecc. Alcune app vengono preinstallate, mentre altre sono disponibili su Apple Store o Play Store.

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Installa solo applicazioni affidabili, presenti negli store ufficiali. Non tutte le applicazioni sono sicure, potrebbero contenere software dannosi.

Se l'offerta sembra troppo bella per essere vera, sii sospettoso. Se sai che un'app o un servizio di solito è a pagamento e trovi una versione gratuita, tieni presente che questa versione potrebbe contenere virus.

ATTIVITÀ

- Lezione 3

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Cosa sono i malware, i virus, i vermi informatici e i trojan?

- Il malware è un software che danneggia i dispositivi rubando dati personali. Spesso, il malware è sviluppato da hacker* che utilizzano i nostri dati per fare soldi.

- Esistono molti tipi di malware:

Virus: i virus si attaccano ai file puliti e si diffondono rapidamente. Possono danneggiare le funzioni centrali di un sistema o distruggere file.

* specialisti informatici che utilizzano le loro conoscenze per commettere crimini nel mondo digitale.

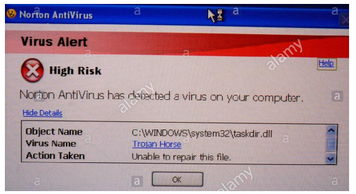
DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Cosa sono i malware, i virus, i vermi informatici e i trojan?

Vermi informatici: *attaccano il funzionamento generale dei dispositivi, localmente o tramite Internet.*

Trojan/cavallo di troia: finge di essere un software affidabile, nascosto nel software originale danneggiato. Di solito "apre le porte" ad altri malware.



ATTIVITÀ

Lezione 4

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Cosa è il cyberbullismo?

- **Il cyberbullismo** è un atto di aggressione intenzionale compiuto attraverso risorse digitali, da un individuo o da un gruppo, nei confronti di una vittima cui non è facile difendersi. Ripetutamente, l'aggressore invia o pubblica contenuti personali su qualcun altro, agendo in modo crudele, volgare, minaccioso, imbarazzante e dannoso (Patchin & Hinduja, 2006).

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Cosa sono i crimini informatici?

- Il crimine su Internet o cybercrime, come è comunemente noto, è una condotta illegale che si verifica attraverso l'uso di computer e Internet (Rosa, 2002, pp. 53-57).

- I crimini più comuni sono la pirateria, la pornografia infantile, i crimini contro l'onore, lo spionaggio e altri (Guimarães Neto, 2003, p. 69).

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

Se sei vittima di cyberbullismo:

- mantieni la calma e analizza la situazione con freddezza;
- cerca sostegno psicologico, se necessario;
- come prevenzione evita di pubblicare informazioni personali o foto su Internet;
- valuta la possibilità di sospendere o eliminare temporaneamente i tuoi profili e bloccare i contatti. Ricorda: tutto ciò che si fa su Internet lascia tracce. Pertanto, dovresti raccogliere quante più informazioni possibili su tutti i comportamenti aggressivi, i profili degli aggressori, i collegamenti a post offensivi e qualsiasi tipo di contenuto che provochi imbarazzo perché così sarai in grado di prendere le misure legali appropriate, persino sporgere denuncia. La maggior parte dei casi di cyberbullismo può essere risolta semplicemente mediando i conflitti o rimuovendo i contenuti che danneggiano qualcuno.

DIGITALISE ME

Argomento 1: La terminologia e i concetti di base per l'utilizzo di Internet

I principali social network dispongono già di strumenti per la segnalazione e la rimozione di contenuti che rientrano in questa categoria di reati..

Durante la navigazione in Internet, potrebbero apparire delle finestre con domande e richieste di informazioni personali. In caso di dubbio o sospetto, non cliccare, non rispondere e non accedere.

ATTIVITÀ

- Lezione 5

DIGITALISE ME

ARGOMENTO 2
Proteggere i dispositivi

Argomento 2: Proteggere i dispositivi

INTRODUZIONE

L'obiettivo principale di questa lezione è fornire informazioni sulla protezione dei dispositivi e dei contenuti digitali, nonché comprendere i rischi e le minacce negli ambienti digitali. La protezione dei dispositivi è fondamentale per garantire la sicurezza delle persone e delle organizzazioni salvaguardando dati, le informazioni messe a disposizione e/o condivise e anche le proprietà.

Cosa impariamo:

- l'importanza di proteggere i propri dispositivi;
- diversi passaggi da eseguire per proteggere un dispositivo.

DIGITALISE ME

Argomento 2: Proteggere i dispositivi

Perché è importante imparare a proteggere i propri dispositivi?

Come attivare/disattivare un firewall:
hthttps://www.youtube.com/watch?v=7PaQnhsiwos (IT)
https://www.youtube.com/watch?v=dlBgoVMXIWo (Eng)

Come aggiornare un dispositivo:
https://www.youtube.com/watch?v=f2Iq5cxxU_Y (IT – windows per PC)
https://www.youtube.com/watch?v=H1XSCaDuMAY (IT – smartphone)
https://www.youtube.com/watch?v=53jhGJgh51k (Eng – windows to PC)
https://www.youtube.com/watch?v=uzu4Jp7UFpI (Eng - smartphones)

Come installare/disinstallare un programma:
https://www.youtube.com/watch?v=_yM6rBr_8sE (IT)
https://www.youtube.com/watch?v=nbFWKuLujq4 (Eng)

DIGITALISE ME

Argomento 2: Proteggere i dispositivi

Quali misure devono essere prese per proteggere un dispositivo?

- Controllo appropriato e implementazione delle pratiche di gestione della sicurezza per mantenere e far funzionare un server web sicuro.

- Una gestione adeguata del dispositivo è essenziale per il suo funzionamento e perché si possa usare in sicurezza. Si consigliano le seguenti pratiche e controlli:

- configurazione del server e controllo delle modifiche e degli aggiornamenti;

- valutazione e gestione del rischio;

- configurazioni software che soddisfano la politica di sicurezza del sistema;

- certificazione delle applicazioni.

DIGITALISE ME

Argomento 2: Proteggere i dispositivi

- Imposta password e crea sequenze di blocco schermo per assicurarti che il tuo dispositivo non venga utilizzato da altri.

- Aggiorna il sistema operativo e i programmi antivirus/antispyware su tutti i tuoi dispositivi. Mantieni attivo il firewall.

ATTIVITÀ

- Lezione 6

DIGITALISE ME

ARGOMENTO 3:
La protezione dei dati personali e della privacy

Argomento 3: La protezione dei dati personali e della privacy

INTRODUZIONE

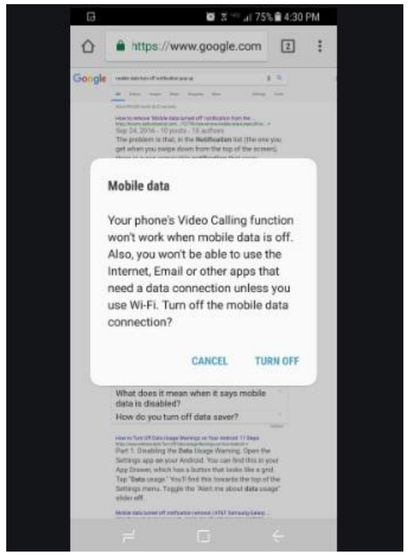
L'obiettivo principale di questa lezione è fornire informazioni su come proteggere i dati personali e la privacy negli ambienti digitali.

Le questioni che verranno trattate includono:

1. L'importanza di proteggere i dati personali.
2. Vari comportamenti da seguire per essere sicuri.
3. L'importanza di tutelare la propria privacy negli ambienti digitali.
4. Vari comportamenti a tutela della propria privacy.

DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy



Il diritto alla protezione dei dati (personali) deriva dal diritto al rispetto della vita privata..

- I dati personali includono il nome, l'indirizzo e altri dati identificativi come codice fiscale, partita iva, numero di passaporto, numero di carta di identità o anche il numero di un cliente, nonché numero di telefono, indirizzo e-mail, il timbro della voce per consentire l'accesso a un conto corrente bancario, e altri dati che, in quanto associati a una persona, ne consentono l'identificazione.

- La direttiva 95/46/CE del 24 ottobre 1995 stabilisce il concetto di dato personale all'articolo 2, lettera a), come "qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"); una persona identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più fattori specifici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".

DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy

- A volte forniamo informazioni non conoscendo per che scopo saranno utilizzate. Non ci chiediamo perché questi o quei dati siano necessari, ad esempio, nel caso della raccolta dei dati per la carta fedeltà di un esercizio commerciale o anche per un questionario di soddisfazione. Possono sembrare innocui o a volte irragionevoli. Questi dati rappresentano un vero e proprio mercato per l'e-commerce e gli utenti devono essere protetti da pratiche abusive.

- Qualsiasi manovra fatta per raccogliere dati personali dai consumatori porta risorse innegabili a coloro che riescono ad abusare di queste informazioni.

- Molte informazioni critiche finiscono per essere accessibili, più o meno direttamente e/o immediatamente, online. Al giorno d'oggi possiamo accedere non solo alle nostre informazioni personali sui social network, ma anche al nostro conto bancario, per esempio. L'accesso è possibile a noi, ma anche a persone o programmi che riescano a passare attraverso le nostre misure di sicurezza informatica e difesa informatica e possono mettere in pericolo non solo noi stessi, ma anche tutti coloro con cui siamo in rete (Martins, 2012) .

DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy

Le più importanti regole di sicurezza e cosa non fare online

- Condividi le informazioni personali in modo limitato.
- Mantieni attive le tue impostazioni sulla privacy.
- Mantieni aggiornato il tuo programma antivirus.
- Tieni aggiornati software, programmi e applicazioni.
- Pratica la navigazione sicura.
- Assicurati che la tua connessione Internet sia sicura.
- Fai attenzione a ciò che scarichi (scarica programmi e app solo da fonti attendibili).
- **Scegli password complesse (e non riutilizzarle).**
- Apri le e-mail con attenzione (+ Diffida di download).
- Tieni d'occhio le notizie che riguardano la sicurezza informatica.
- Effettua acquisti online da siti sicuri.
- Fai attenzione a ciò che pubblichi.
- Fai attenzione a chi incontri online.

DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy

Un modo per garantire la tua privacy è creare **password complesse**. C'è anche la possibilità di utilizzare altri mezzi per garantire la doppia autenticazione.

Elabora una password complessa

I criteri per le password incoraggiano a utilizzare le password più sicure possibili senza la necessità o la tentazione di riutilizzare le password o di annotarle. Ciò significa che le password devono essere casuali, complesse e lunghe (almeno 8 caratteri e di tipo diverso, preferibilmente). In ogni caso devi cambiare la password regolarmente e non comunicarla a nessuno.

DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy

Come creare una password sicura:

- Usa password di almeno otto (8) caratteri o più (più lunghe è meglio).
- Utilizza una combinazione di lettere maiuscole, minuscole, numeri e caratteri speciali (ad esempio: !, @, &, %, +) in tutte le password.
- Evita di usare nomi di persone o animali domestici; è anche meglio evitare di utilizzare date chiave (compleanni, anniversari, ecc.). E non scegliere mai una password come "12345678".
- Una password complessa dovrebbe apparire come una serie di caratteri casuali.

DIGITALISE ME

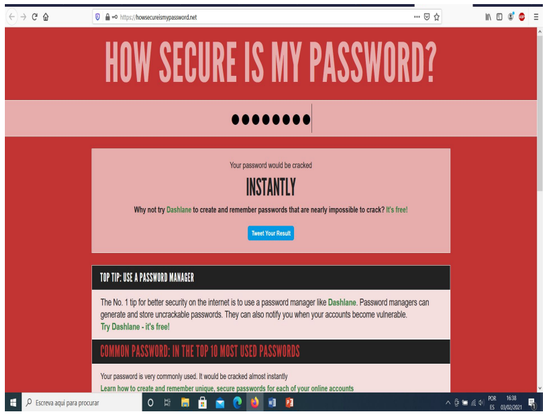
Argomento 3: La protezione dei dati personali e della privacy

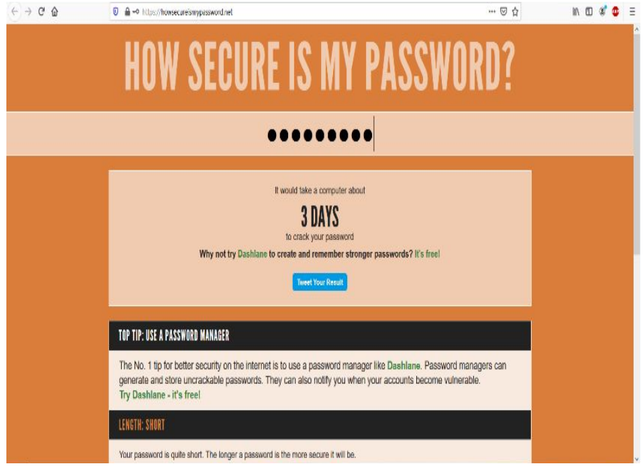
Come creare una password sicura:

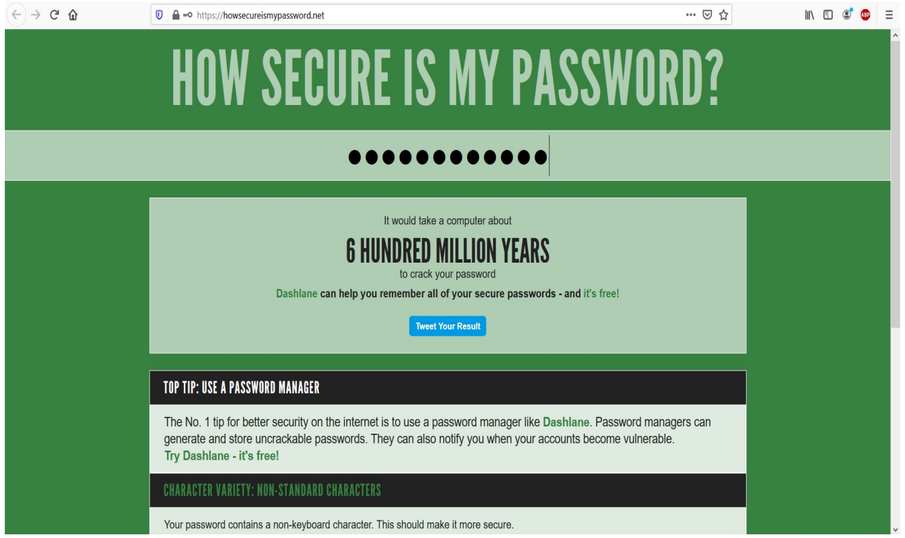
- Verifica la sicurezza della tua password!

Alcuni siti lo fanno in automatico. Altrimenti, esistono siti appositi, come questo:
https://howsecureismypassword.net/

Provaci!







DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy

Come creare una password sicura:

- Mantieni private le tue password: non condividere mai una password con nessun altro.
- Non scrivere le tue password.
- Sul web, se pensi che la tua password possa essere stata compromessa, cambiala subito e poi controlla se gli altri tuoi account sono stati utilizzati in modo improprio.

Andare oltre: metodi di autenticazione a due fattori

Questi metodi, che richiedono di provare attraverso due strumenti che tu sia chi affermi di essere, sono più sicuri rispetto all'utilizzo di password statiche per l'autenticazione. Un esempio comune è un token di sicurezza personale che visualizza diversi codici di accesso da utilizzare insieme a una password. Tuttavia, sappiamo che i sistemi a due fattori potrebbero non essere sempre possibili o pratici!

ATTIVITÀ

- Lezione 7

DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy

Cose che non dovresti mai, mai condividere sui social media

- Programmi di viaggio/ dettagli esatti della tua prossima vacanza.
- La tua posizione personale (anche immagini georeferenziate).
- Immagini delle tue carte di credito/acquisti costosi.
- Video dei tuoi amici che hai girato senza avere il permesso.
- Contenuti che i tuoi amici dovrebbero condividere solo se lo vogliono. (Quando un tuo amico ti dice che si sta per sposare o che aspetta un bambino, non lasciarti trascinare dall'impazienza di condividerlo con gli altri).
- Immagini personali inadeguate.
- Informazioni bancarie.
- Lamentele sul tuo capo.

Argomento 3: La protezione dei dati personali e della privacy

C'è una regola che dovresti seguire sui social media: non pubblicare mai nulla che non vorresti che il mondo intero veda.

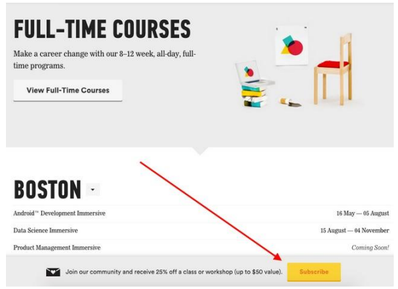
Se pubblichi qualcosa oggi e te ne penti tra due anni, potresti essere in grado di eliminarlo dal tuo account, ma non potrà mai essere completamente cancellato da Internet.

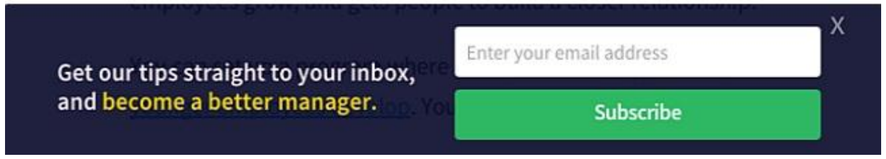
Una buona regola generale è chiedersi se ciò che si sta per pubblicare potrebbe essere esposto in qualsiasi luogo pubblico, in qualsiasi parte del mondo, senza sentirsi in imbarazzo. Se la risposta è no, allora è meglio non pubblicare.

DIGITALISE ME

Argomento 3: La protezione dei dati personali e della privacy

A volte, durante la navigazione in Internet, possono apparire delle finestre che chiedono i tuoi dati personali. Fai attenzione a questo tipo di richieste!





ATTIVITÀ

- Lezione 8

DIGITALISE ME

ARGOMENTO 4:
La tutela della salute e del benessere

Argomento 4: La tutela della salute e del benessere

INTRODUZIONE

L'obiettivo principale di questa lezione è fornire informazioni su come evitare rischi per la salute e minacce al benessere fisico e psicologico nell'utilizzo delle tecnologie digitali, nonché su come proteggere se stessi e gli altri da possibili pericoli negli ambienti digitali.

Nel corso della lezione impareremo a capire che *ogni cosa che facciamo online comporta delle conseguenze, ed è quindi importante essere responsabili quando si naviga in Internet per evitare i rischi che derivano da un uso improprio.*

DIGITALISE ME

Argomento 4: La tutela della salute e del benessere

Le tecnologie digitali hanno contribuito a migliorare la qualità della vita, ma comportano anche alcuni rischi, come la dipendenza tecnologica. Gli studi dimostrano l'importanza di prevenire questa situazione e di sensibilizzare gli operatori sanitari, gli educatori e i genitori.

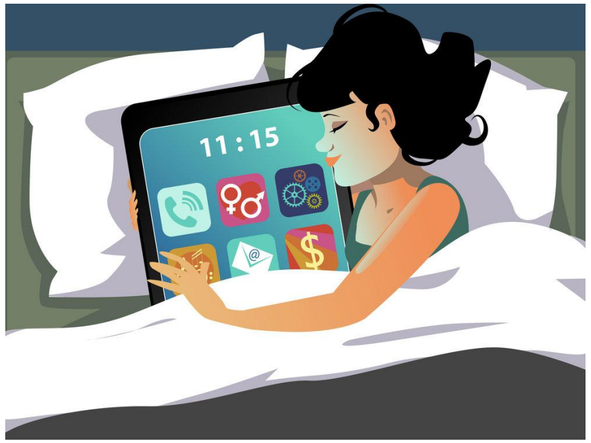
Una dipendenza dalle tecnologie digitali ampiamente discussa è un nuovo tipo di dipendenza emerso nel 21° secolo che riguarda **l'abuso** di telefoni cellulari, social network e Internet.

La dipendenza dalle tecnologie digitali è definita da disturbi psicologici e comportamentali, che non comportano l'uso di sostanze, ma sono di natura impulsivo-compulsiva e che portano l'utente a rimanere continuamente o sempre più impigliato nelle ICT, indipendentemente dalle conseguenze negative che possono avere per il suo benessere fisico, sociale, spirituale, mentale o finanziario. (Dott. José Romero, Psichiatra).

DIGITALISE ME

Argomento 4: La tutela della salute e del benessere

Uno studio condotto in Portogallo (uno dei paesi di realizzazione del progetto Digitalise me) ha rivelato che il 73,3% dei giovani di età compresa tra i 14 ei 25 anni presenta sintomi indicativi di dipendenza da Internet. Di questi, il 13% aveva gravi livelli di dipendenza e il 52,1% degli intervistati si considerava "dipendente da Internet". Un altro studio sottolinea che circa il 25% dei bambini e dei giovani in Portogallo dipende clinicamente dall'uso di Internet e dei social network.



DIGITALISE ME

Argomento 4: La tutela della salute e del benessere

Non esiste un'unica **causa della dipendenza da Internet.**
Diversi fattori possono svolgere un ruolo, tra cui:-

- condizioni di salute mentale sottostanti, tra cui ansia e depressione;
- genetica;
- fattori ambientali.

Le cause che possono **portare a una dipendenza**, sono, tra le altre:

- ❑ Troppa navigazione online.
- ❑ Eccessivo uso dei social network.
- ❑ Tempo eccessivo speso in attività online come giochi, compravendita di azioni, gioco d'azzardo.

DIGITALISE ME

Argomento 4: La tutela della salute e del benessere

Le cause che possono portare un individuo a diventare dipendente dalle nuove tecnologie possono essere suddivise in: fattori individuali, familiari e sociali. C'è una frequente associazione di alcune patologie psichiatriche con queste dipendenze dalle nuove tecnologie, per esempio con il disturbo da iperattività e deficit di attenzione, con la depressione, il disturbo bipolare e altri disturbi dell'umore, con ansia, fobia sociale, uso/abuso di sostanze e con il disturbo ossessivo-compulsivo, insonnia, ostilità e aggressività, tendenza al suicidio e alla schizofrenia.

News dal mondo:

https://www.ictedmagazine.com/index.php/edi2-10/86-aspetti-neurobiologici-della-dipendenza-da-internet (IT)

https://portaldasaude.scmp.pt/pt-pt/noticias/a-dependencia-nas-tecnologias-de-informacao-e-comunicacao- (PT)

https://www.theguardian.com/technology/2018/mar/18/dangers-of-digital-dependency (Eng)

DIGITALISE ME

Argomento 4: La tutela della salute e del benessere

Mantenere l’equilibrio

I contatti online possono essere un'ancora di salvezza. Ma è anche importante stabilire dei limiti sul tempo trascorso davanti a uno schermo e bilanciarlo con altre modalità di relazione, comunicazione, apprendimento e lavoro.

Prendi in considerazione l’idea di leggere un libro, fare un po' di esercizio o lavoretti o completare un puzzle.

È fortemente consigliabile ottenere il giusto equilibrio tra la tua vita online e offline.

ATTIVITÀ

- Lezione 9

DIGITALISE ME

Bibliografia

· ACM Computing Surveys, Vol. 52, No. 5, Article 88. Publication date: September 2019.

· ACM Reference format: Ori Or-Meir, Nir Nissim, Yuval Elovici, and Lior Rokach. 2019. Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. ACM Comput. Surv. 52, 5, Article 88 (September 2019), 48 pages.

· Cavelty, 2018b, pp. 8-9; Christou, 2018, pp. 13-14; Carrapiço e Barrinha, 2017, pp. 1260-1261

· Emm, David. 2008. Changing threats, changing solutions: A history of viruses and antivirus. Viruslist.com. 1.1

. FIREWALLa. Firewall - Segurança nas Redes. 2007 Available at :

http://www.gta.ufrj.br/grad/07_1/firewall/index_files/Page350.htm. Acesso em: 28 de Janeiro de 2010. Pearson

· Gashi, Ilir, Stankovic, Vladimir, Leita, Corrado, & Thonnard, Olivier. 2009. An experimental study of diversity with off-the-shelf antivirus engines. 4–11. 2.1

DIGITALISE ME

Bibliografia

· Koepsell, David R. (2002). The ontology of cyberspace: philosophy, law, and the future of intellectual property. Chigaco: Open Court.

· KUROSE James F., ROSS, Keith W. (2010), Redes de Computadores e a Internet 5a. Edição. 2010. Editora

· Kurose, J. F. e Ross, K. W. (2010). Redes de computadores e a Internet: uma abordagem top-down. Addison Wesley, São Paulo, 5. Ed

· Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. Youth Violence and Juvenile Justice, 4, 148- 169.

· Richardson, R. 2008. CSI computer crime and security survey. Computer security institute. 1.1, 2.2.1

· SOARES, Luiz Fernando Gomes. Redes de computadores: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995

· Stallings, W. (2008). Criptografia e segurança de redes. Pearson Prentice Hall, São Paulo, 4 ed.

· Vieites. Álvaro Gómez. TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS. Available at:

https://bdigital.ufp.pt/bitstream/10284/6089/1/DM_Thiago%20Machado.pdf (consulted at February 15, 2017).

DIGITALISE ME

Bibliografia

· https://repositorio.unesp.br/bitstream/handle/11449/89341/gonsalespanes_g_me_sjrp.pdf?sequence=1&isAllowed=y (consulted at November 9, 2020)

· https://repositorio.ul.pt/bitstream/10451/4321/1/ulfc055737_tm_Carlos_Miguel_Silva.pdf (consulted at November 9, 2020)

· https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=1&sid=10d47551-9469-48e8-9d1d-3e1649102039%40pdc-v-sessmgr02 (consulted at November 9, 2020)

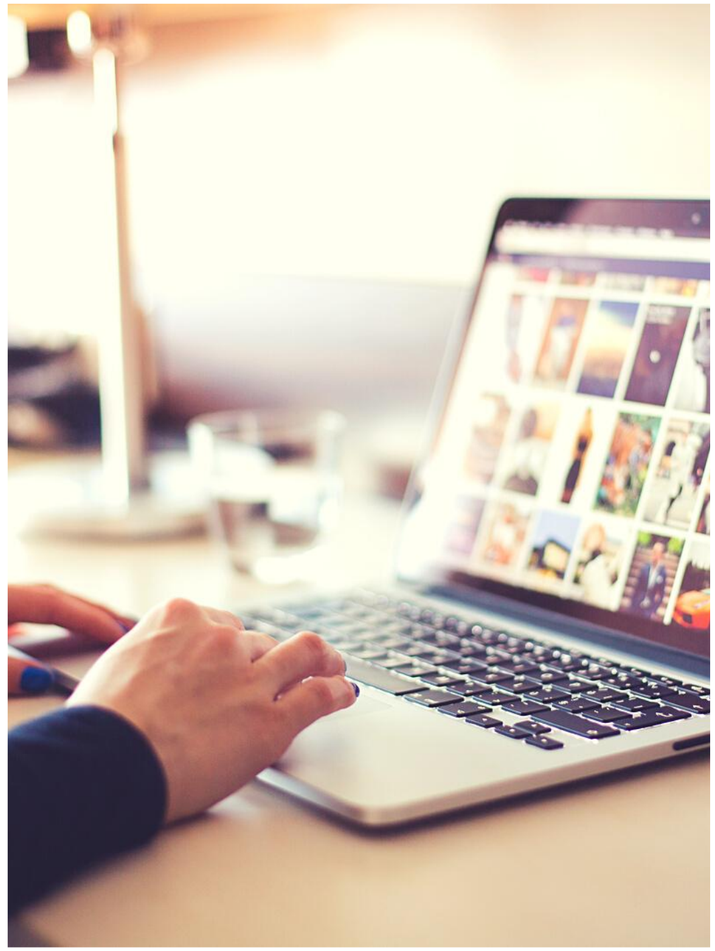
· https://www.avg.com/pt/signal/what-is-malware (consulted at November 10, 2020)·

· vhttps://repositorio.ual.pt/bitstream/11144/1861/1/PDF%20-%20A%20PROTE%c3%87%c3%83O%20DE%20DADOS%20PESSOAIS%20E%20PRIVACIDADE%20DO%20UTILIZADOR%20NO%20%c3%82MBITO%20DAS%20COMUNICA%c3%87%c3%95ES%20ELETR%c3%93NICAS%20%28F%29.pdf (consulted at November11, 2020)

DIGITALISE ME

Glossario (1)

TERM	DEFINITION
SOFTWARE ANTIVIRUS **(SLIDE 10)**	Gli antivirus sono applicazioni che rilevano programmi dannosi e sono in grado di rimuoverli o di metterli in quarantena.
APPLICAZIONI **(SLIDE 12)**	Programma o insieme di programmi che permettono di svolgere attività sul computer o sul telefono cellulare/tablet.
CYBERBULLISMO **(SLIDE 18)**	Il cyberbullismo è un (ripetuto) atto intenzionalmente aggressivo compiuto attraverso risorse elettroniche, da un individuo o da un gruppo, nei confronti di una vittima che non è in grado di difendersi facilmente.
CRIMINE INFORMATICO **(SLIDE 19)**	È un comportamento illegale condotto attraverso l'uso di computer e Internet.
FIREWALL **(SLIDE 8)**	È una barriera difensiva. La sua funzione è fondamentalmente quella di bloccare il traffico dati indesiderato o dannoso e consentire quello non dannoso.
MALWARE (VIRUS, VERMI INFORMATICI, TROJAN) **(SLIDE 16)**	Il malware è un software che danneggia i dispositivi rubando dati personali. Spesso, il malware viene sviluppato da hacker che utilizzano i nostri dati per fare soldi.



Contatti

http://www.digitaliseme.eu/en

https://www.facebook.com/digitaliseme.project/

DIGITALISE ME