Scheda di formazione

Titolo	Sicurezza online: Cosa fare e cosa non fare
Parole chiave	Internet, sicurezza, online, offline, password, privacy
Fornito da	Internet Web Solutions
Lingua	Italiano

Area di formazione (X se applicabile)	
	Alfabetizzazione all'informazione
	Comunicazione e collaborazione
X	Sicurezza
	Problem Solving

Obiettivi / Risultati dell'apprendimento

Al termine di questo modulo sarai in grado di:

- Comprendere l'importanza di un comportamento online responsabile
- Identificare i rischi online più comuni
- Riconoscere i vantaggi di Internet
- Imparare le migliori pratiche di sicurezza online
- Sviluppare le competenze digitali

Descrizione

Questo corso offre una panoramica completa su come stare al sicuro quando si usa Internet, fornendo consigli pratici sulle cose da fare e da non fare online, tra cui suggerimenti su connessioni sicure, gestione delle password, impostazioni della privacy per i social media, pratiche di acquisto online sicure e riconoscimento ed evitamento di frodi e truffe. Seguendo queste linee guida, sarai in grado di navigare nel mondo online in modo sicuro e di proteggerti da potenziali minacce.

Indice di contenuto (3 livelli)

Modulo: Sicurezza online: Cosa fare e cosa non fare
Unità 1: Introduzione alla sicurezza online
1.1. Cosa significa essere sicuri online?
1.2. Quali sono i rischi di una navigazione in Internet non sicura?
1.3. Perché non si dovrebbe smettere di navigare in Internet anche con questi rischi?

Unità 2: Cosa fare e cosa non fare online
2.1. Connessioni sicure
2.2. Password
2.3. Privacy e social media

Co-funded by the European Union

2.4. Shopping online
2.5. Truffe e raggiri

Unità 3: Bonus track: Fare e non fare offline
3.1. Dispositivi digitali

Contenuto sviluppato

Modulo: Sicurezza online: Cosa fare e cosa non fare

Unità 1: Introduzione alla sicurezza online

Sezione 1.1: Cosa significa essere sicuri online?

Essere sicuri online significa prendere precauzioni e adottare comportamenti responsabili durante l'utilizzo di Internet. Si tratta di comprendere e gestire **i rischi e le minacce potenziali** associati alle attività online per proteggere le informazioni personali, le risorse finanziarie e il benessere generale.

Il cyberspazio è come un'autostrada: bisogna percorrerlo in sicurezza per evitare incidenti. Proprio come allacciare la cintura di sicurezza, alcune pratiche di base per la sicurezza in Internet possono contribuire a garantire un'esperienza sicura e piacevole.

Essere sicuri online è importante per diversi motivi. Aiuta a **proteggere le informazioni personali** dalle mani sbagliate. I dati personali come il nome, l'indirizzo, il numero di telefono e le informazioni finanziarie possono essere utilizzati per il furto d'identità, la frode o altre attività dannose se accessibili ai criminali informatici. La propria presenza online contribuisce alla propria reputazione, sia personale che professionale.

Se si è al sicuro online, si può **evitare la diffusione di contenuti inappropriati o dannosi** che potrebbero avere un impatto negativo sulla propria immagine e sulle proprie relazioni. La salvaguardia della propria sicurezza online garantisce **la protezione della propria privacy e protegge da frodi e truffe finanziarie**.

Essere sicuri online aiuta anche a **evitare casi di cyberbullismo e molestie.** Implementando le misure di sicurezza, è possibile ridurre il rischio di imbattersi in persone o situazioni dannose che potrebbero causare disagio emotivo o danni. La sicurezza online è fondamentale anche per **proteggere i bambini** e garantire il loro benessere nel mondo digitale.

Sezione 1.2: Quali sono i rischi di una navigazione in Internet non sicura?

Una navigazione in Internet poco sicura comporta dei rischi per le persone anziane. Questi ultimi possono avere meno dimestichezza con le piattaforme e le minacce

Co-funded by the European Union

online, per cui è importante comprendere i rischi specifici che corrono.

Alcuni rischi comuni sono:

- **Phishing e truffe:** Gli anziani sono più esposti alle e-mail di phishing, ai siti web fraudolenti e alle truffe telefoniche, in cui i truffatori li inducono a rivelare informazioni sensibili.
- **Furto di identità:** Una navigazione in Internet poco sicura aumenta il rischio di furto di informazioni personali e di identità, con conseguenti perdite finanziarie e interruzioni della vita.
- **Frodi finanziarie:** Gli anziani vengono presi di mira con falsi programmi di investimento, truffe alla lotteria o acquisti fraudolenti, sfruttando la loro fiducia e vulnerabilità.
- **Malware e virus:** Una navigazione in Internet poco sicura può portare al download involontario di software dannoso che compromette la sicurezza del dispositivo e le informazioni personali.
- **Molestie online e cyberbullismo:** Le persone anziane possono soffrire di stress emotivo e problemi di benessere mentale a causa delle molestie online.
- **Violazioni della privacy:** Pratiche di privacy inadeguate possono esporre informazioni personali, con conseguente furto di identità o sollecitazioni indesiderate.
- **Truffe di assistenza tecnica:** Le persone anziane sono più soggette a truffe in cui i truffatori si fingono rappresentanti dell'assistenza tecnica.
- **Mancanza di alfabetizzazione digitale:** l'insicurezza della navigazione in Internet è aggravata dalla mancanza di alfabetizzazione digitale degli anziani, che li rende più vulnerabili alle minacce e alle truffe.

Gli anziani dovrebbero essere consapevoli di questi rischi e adottare misure proattive per prevenirli, ad esempio cercando aiuto e supporto da persone fidate o segnalando i problemi alle autorità o alle piattaforme competenti.

Sezione 1.3: Perché non si dovrebbe smettere di navigare in Internet anche con questi rischi?

La sicurezza in Internet è importante, ma non deve essere stressante. La consapevolezza è un primo passo importante per proteggersi insieme a un software antivirus affidabile (molti sono gratuiti!).

Nonostante i rischi online, non si dovrebbe smettere completamente di navigare in Internet, perché la rete può avere enormi vantaggi per il benessere e l'inclusione sociale. Internet offre una grande quantità di **informazioni e risorse** che possono essere di grande utilità. Permette di accedere a notizie, materiali educativi, risorse

Co-funded by the European Union

sanitarie, strumenti di comunicazione e vari servizi online.

In termini di **connessione sociale,** Internet permette di rimanere in contatto con la famiglia, gli amici e le comunità, soprattutto quando la mobilità fisica o la distanza rappresentano una barriera. Le piattaforme di social media, le videochiamate e i forum online consentono di mantenere relazioni, condividere esperienze e combattere l'isolamento o la solitudine. Le piattaforme online offrono comodità e i**ndipendenza** a tutte le persone in vari aspetti della vita quotidiana. È possibile fare **acquisti online, accedere a servizi di banking online, fissare appuntamenti e ordinare farmaci,** garantendo una maggiore comodità e **riducendo la necessità di spostamenti fisici o di assistenza.**

La navigazione è anche una fonte di **stimolazione cognitiva e di impegno mentale**, in quanto offre l'opportunità di imparare, giocare, partecipare a hobby o comunità virtuali e rimanere mentalmente attivi, il che può contribuire al benessere generale.

Navigando in Internet e adottando pratiche online sicure, è possibile **sviluppare competenze digitali,** aumentare la fiducia in sé stessi e mantenere un se**nso di empowerment**. Internet offre una grande quantità di **risorse per l'apprendimento**, tra cui corsi online, esercitazioni e piattaforme educative. È possibile esplorare nuovi interessi, apprendere nuove competenze e impegnarsi in opportunità di apprendimento permanente, promuovendo la crescita personale e la stimolazione intellettuale.

Sebbene sia importante essere consapevoli dei rischi online e prendere le dovute precauzioni, **evitare completamente Internet può portare all'isolamento, a un accesso limitato alle risorse e a opportunità mancate.**

Unità 2: Cosa fare e cosa non fare online

Sezione 2.1: Connessioni sicure

Fare:

Utilizzare reti Wi-Fi sicure: Quando possibile, collegarsi a reti Wi-Fi sicure e affidabili. Queste reti richiedono solitamente una password e la crittografia, garantendo un ambiente di navigazione più sicuro. Evitare di accedere ad account sensibili o di effettuare transazioni finanziarie su reti Wi-Fi pubbliche.

Verificare la sicurezza dei siti web: Prima di inserire informazioni sensibili o effettuare transazioni online, assicurarsi che il sito web abbia una connessione sicura. Cercare "https://" nell'indirizzo del sito e il simbolo del lucchetto nella barra degli indirizzi del browser**.**

Mantenere il software aggiornato: Aggiornare regolarmente il sistema operativo del

Co-funded by the European Union

dispositivo, i browser web e il software di sicurezza. Gli aggiornamenti del software spesso includono patch di sicurezza che aiutano a proteggere dalle vulnerabilità note.

Utilizzare la protezione del firewall: Attivare e mantenere un firewall sul proprio computer o router per agire come una barriera contro gli accessi non autorizzati e le potenziali minacce provenienti da Internet.

Non fare:

Non condividere informazioni sensibili: Evitare di inserire informazioni sensibili, come password, dati della carta di credito o numeri di previdenza sociale.

Evitare siti web sospetti: Evitare di visitare siti web sospetti o sconosciuti. Per le attività online, attenersi a siti web affidabili e di fiducia.

Non ignorare gli avvisi del browser: Prestare attenzione agli avvisi e agli avvisi del browser su potenziali rischi per la sicurezza o siti web non attendibili.

Non collegarsi automaticamente alle reti: Disattivare la funzione di connessione automatica sui propri dispositivi, perché potrebbe connettersi automaticamente a reti non protette senza che se ne sia consapevoli.

Sezione 2.2: Password
Fare:

Creare password forti e uniche: Utilizzare password forti e uniche per ogni account online. Dovrebbe includere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali. Evitare di utilizzare informazioni indovinabili come date di nascita o nomi.

Fare password lunghe: Optare per password più lunghe, perché in genere sono più sicure. Puntate a un minimo di 12 caratteri. Considerare l'uso di *passphrase*: una serie di parole o una frase più facile da ricordare ma difficile da indovinare per gli altri. Ad esempio, ‘’IlMioColorePreferitoèIlBlu’’.

Attivare l'autenticazione a due fattori (2FA): Quando possibile, attivare l'autenticazione a due fattori per i propri account online. Questo aggiunge un ulteriore livello di sicurezza richiedendo un secondo passaggio di verifica, come un codice univoco inviato al proprio dispositivo mobile**.**

Aggiornare regolarmente le password: Cambiare le password periodicamente, preferibilmente ogni pochi mesi.

Co-funded by the European Union

Non fare:

Non riutilizzare le password: Non riutilizzare mai la stessa password per più account. Se un account venisse compromesso, potrebbe potenzialmente garantire l'accesso anche ad altri account. Utilizzare password uniche per ogni servizio o piattaforma online.

Evitare le password comuni: Evitare le password comuni o facili, come ''123456'', ''password'' o ''qwerty''. Queste password sono spesso prese di mira dagli hacker e possono essere facilmente decifrate.

Non condividere o scrivere le password: Evitare di condividere le proprie password con altri, compresi parenti e amici. Inoltre, evitare di scrivere le password su appunti fisici o di memorizzarle in file digitali facilmente accessibili.

Non salvare le password nei browser: Evitare di salvare le password nei browser o di utilizzare la funzione ''Ricordami''. Anche se può essere comodo, rappresenta un rischio per la sicurezza se qualcuno ottiene un accesso non autorizzato al proprio dispositivo.

Sezione 2.3: Privacy e social media

Fare:

Esaminare le impostazioni sulla privacy: Familiarizzare con le impostazioni sulla privacy delle piattaforme di social media utilizzate. Regolare le impostazioni per controllare chi può vedere il vostro profilo, i post e le informazioni personali. Considerare la possibilità di limitare l'accesso ad amici e familiari fidati.

Essere selettivi con le richieste di amicizia: Essere cauti quando accettate richieste di amicizia o di connessione da persone sconosciute. Verificare l'identità della persona prima di accettare la sua richiesta.

Pensare prima di condividere: Fare attenzione quando si condividono informazioni personali, foto o aggiornamenti sulle piattaforme di social media. Evitare di condividere pubblicamente dettagli sensibili come l'indirizzo completo, il numero di telefono o le informazioni finanziarie.

Rivedere e aggiornare regolarmente la lista degli amici: Rivedere periodicamente l'elenco degli amici o delle connessioni sulle piattaforme di social media. Rimuovere o togliere l'amicizia a persone di cui non ci si fida più o che non si riconoscono più.

Non fare:

Non cliccare su link sospetti: Diffidare di cliccare sui link condivisi sui social media, soprattutto quelli provenienti da fonti sconosciute o sospette. Questi link possono

Co-funded by the European Union

portare a siti web di phishing o al download di malware. Verificare la fonte prima di fare clic.

Attenzione alle applicazioni di terze parti: Essere selettivi quando si concedono permessi ad applicazioni di terze parti che richiedono l'accesso ai propri account di social media. Esaminare le autorizzazioni richieste e considerare la credibilità dell'applicazione prima di concedere l'accesso.

Evitare di pubblicizzare eventi personali: Evitare di annunciare vacanze imminenti o periodi prolungati di assenza da casa sulle piattaforme dei social media. Ciò potrebbe allertare potenziali ladri o criminali che la vostra casa non è occupata.

Sezione 2.4: Shopping online
Fare:

Acquisti da siti web affidabili: Quando si fanno acquisti, rivolgersi a rivenditori online rinomati e rispettabili. Cercare siti web che abbiano recensioni positive dei clienti e opzioni di pagamento sicure, come carte di credito o piattaforme di pagamento affidabili.

Verificare la sicurezza del sito web: Prima di inserire i dati personali o di pagamento, assicurarsi che il sito web abbia una connessione sicura. Cercare "https://" nell'indirizzo del sito e il simbolo del lucchetto nella barra degli indirizzi del browser.

Tenere traccia delle transazioni: Conservare un registro delle transazioni di acquisto online, comprese le conferme d'ordine, le ricevute e i numeri di tracciamento. In questo modo è possibile monitorare le consegne e risolvere eventuali problemi.

Non fare:

Non condividere informazioni non necessarie: Essere cauti nel condividere informazioni personali non necessarie durante il processo di checkout. I rivenditori di solito richiedono dettagli di base come l'indirizzo di spedizione e le informazioni di pagamento.

Attenzione alle e-mail o ai link di phishing: Diffidare di e-mail o messaggi che affermano di provenire da rivenditori online, soprattutto se chiedono informazioni personali o invitano a cliccare su link sospetti.

Evitare il Wi-Fi non protetto per le transazioni: Quando si fa shopping online, evitare di utilizzare reti Wi-Fi pubbliche o non protette. Queste reti possono essere vulnerabili agli hacker che potrebbero intercettare le vostre informazioni personali e finanziarie.

Non cadere nelle truffe di imitazione: Fare attenzione ai venditori online che si

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

spacciano per marchi affidabili o che utilizzano tattiche ingannevoli per ottenere informazioni personali o finanziarie. Verificare l'autenticità del venditore e del suo sito web prima di effettuare un acquisto.

Sezione 2.5: Truffe e raggiri

Fare:

Essere scettici e vigili: Mantenere un sano scetticismo quando ci si imbatte in e-mail, telefonate o messaggi non richiesti che chiedono informazioni personali o propongono strane offerte. Verificare la legittimità della fonte prima di fornire informazioni o assumere impegni finanziari.

Istruirsi: Rimanere informati sulle comuni truffe online e sulle tattiche di frode che prendono di mira le persone anziane. Familiarizzare con i segnali delle truffe, come le richieste di pagamento con metodi non convenzionali o le pressioni ad agire rapidamente.

Verificare l'identità del contatto: Quando qualcuno afferma di rappresentare un'organizzazione, chiedere le informazioni di contatto ufficiali e confermarne l'autenticità contattando direttamente l'organizzazione utilizzando i dati di contatto verificati.

Consultare persone fidate: Se si riceve una richiesta sospetta o si incontra una situazione sconosciuta online, chiedere consiglio a un familiare, un amico o un professionista fidato.

Ignorare le telefonate non richieste e le ''robocall''. Trattare con scetticismo le telefonate non richieste. Una persona in carne e ossa o una voce registrata dà informazioni false che sembrano importanti e sensibili al tempo. Potrebbero affermare di essere un parente in difficoltà, che la garanzia della vostra auto sta scadendo e che è richiesto un pagamento, potrebbero presentarsi come "assistenza tecnica" e dire che il vostro PC deve essere riparato a pagamento.

Non fare:

Non avere fretta o sentirsi sotto pressione: I truffatori spesso utilizzano tattiche per creare un senso di urgenza o di pressione, costringendo le vittime a prendere decisioni rapide senza un'adeguata considerazione. Prendere tempo, fare ricerche e agire con cautela prima di prendere qualsiasi impegno finanziario.

Non inviare denaro a persone sconosciute: Diffidare delle richieste di denaro o di bonifici da parte di persone che non si conoscono personalmente. Verificare l'identità e la legittimità della persona prima di intraprendere qualsiasi transazione

Co-funded by the European Union

finanziaria.

Non cliccare sui link contenuti in e-mail provenienti da mittenti sconosciuti. Diffidare di messaggi strani o inaspettati, anche se provengono da persone conosciute. Potrebbero contenere link malevoli o di phishing. Se un messaggio ha un aspetto sospetto ma sembra provenire da una persona che si conosce e di cui ci si fida, è bene informarsi prima di cliccare.

Non aprire gli allegati. Non aprire gli allegati che non ti aspetti o che provengono da un contatto sconosciuto, soprattutto se hanno un'estensione .exe o .zip. Se i file sembrano provenire da un amico o da un familiare, chiedere loro di accertarsi che vi abbiano inviato qualcosa. Questa regola di sicurezza vale anche per gli allegati inviati tramite messaggi di testo e social media.

Non cliccare sulle finestre pop-up sul telefono o sul computer. Uno stratagemma comune è lo *scareware*, che utilizza avvisi di sicurezza a comparsa per spaventare l'utente e indurlo a scaricare o pagare per un software falso mascherato da vera protezione per la sicurezza informatica. Ad esempio, viene visualizzato un avviso che informa che il dispositivo è compromesso e deve essere riparato. Quando si chiama l'assistenza, i truffatori possono chiedere l'accesso remoto al computer e richiedere un pagamento. Un'altra tecnica di malware consiste nell'utilizzare gli ingannevoli pulsanti ''Chiudi'' o ''X'', che installano automaticamente un virus quando vi si fa clic.

Unità 3: Bonus track: Fare e non fare offline

Sezione 3.1: Dispositivi digitali
Fare:

Bloccare i dispositivi. Assicurarsi che i dispositivi con accesso a informazioni sensibili si blocchino automaticamente e richiedano una password per essere riattivati. Assicurarsi di configurare il router Wi-Fi di casa e i punti di accesso con nomi utente e password unici e diversi da quelli predefiniti.

Mantenere i dispositivi al sicuro: Assicurarsi che i dispositivi digitali, come smartphone, tablet o computer portatili, siano fisicamente sicuri. Conservarli in un luogo sicuro e protetto quando non vengono utilizzati.

Aggiornare regolarmente il software: Mantenere aggiornati il sistema operativo e le applicazioni sui dispositivi. Gli aggiornamenti del software spesso includono importanti patch di sicurezza che aiutano a proteggere dalle vulnerabilità e a garantire prestazioni ottimali.

Attivare la localizzazione e il blocco a distanza: Attivare le funzioni di localizzazione e blocco remoto sui dispositivi, se disponibili. Ciò consente di localizzare il dispositivo o di bloccarlo a distanza in caso di smarrimento o furto.

Co-funded by the European Union

Smaltire in modo sicuro i vecchi dispositivi: Quando si smaltiscono i vecchi dispositivi digitali, assicurarsi che tutti i dati personali siano completamente cancellati dal dispositivo. Eseguire un reset di fabbrica o utilizzare un software specializzato per cancellare i dati in modo sicuro.

Non fare:

Non lasciare i dispositivi incustoditi: Evitare di lasciare i dispositivi digitali incustoditi in luoghi pubblici, come caffè o mezzi di trasporto pubblici. Tenerli sempre a portata di mano o custoditi in modo sicuro.

Non installare applicazioni non autorizzate: Evitare di scaricare e installare applicazioni da fonti non attendibili. Limitarsi agli app store ufficiali, come Google Play Store o Apple App Store, per ridurre il rischio di scaricare applicazioni dannose o contraffatte.

5 Voci del glossario

Password. La password è una combinazione segreta di caratteri utilizzata per autenticarsi e accedere a un dispositivo o a un account. Si consiglia di impostare una password forte per proteggere le informazioni sensibili.
Social media. I social media si riferiscono a piattaforme e tecnologie online che consentono agli utenti di creare, condividere e scambiare informazioni, idee e contenuti con altri. Queste piattaforme prevedono in genere contenuti generati dagli utenti e facilitano la comunicazione, il networking e l'interazione tra individui o gruppi.
Sicurezza online. La sicurezza online si riferisce alle misure e alle precauzioni adottate per proteggere gli individui e le loro informazioni personali durante l'utilizzo di Internet e le attività online. Comprende pratiche e linee guida che mirano a prevenire vari rischi online come il cyberbullismo, il furto di identità, le frodi, l'hacking e l'esposizione a contenuti inappropriati. La sicurezza online implica la comprensione e l'attuazione di strategie per salvaguardare la privacy, la sicurezza e il benessere durante l'utilizzo delle piattaforme digitali.
Applicazioni dannose. Le app dannose sono applicazioni progettate per danneggiare o compromettere la sicurezza di un dispositivo o dei dati dell'utente. L'installazione di applicazioni da fonti non attendibili aumenta il rischio di scaricare applicazioni dannose che possono rubare informazioni personali o eseguire azioni non autorizzate.
Informazioni sensibili. Per informazioni sensibili si intendono tutti i dati o i dettagli che, se divulgati o consultati da persone non autorizzate, potrebbero rappresentare un rischio per la privacy, la sicurezza o il benessere di un individuo. Sono incluse le informazioni di identificazione personale (PII) come nomi e cognomi, indirizzi, numeri di telefono, numeri di previdenza sociale, informazioni finanziarie, credenziali di accesso e cartelle cliniche. Le informazioni sensibili richiedono una protezione e una gestione particolari per evitare abusi, furti di identità, frodi o altre

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

conseguenze dannose.

5 domande di autovalutazione a scelta multipla

Domanda 1. Di cosa ha bisogno una connessione Wi-Fi per essere sicura?
Opzione a: Richiede che sia privato, con l'uso di password e crittografia
Opzione b: Richiede un utilizzo illimitato dei dati.
Opzione c: Richiede un'alta velocità di Internet.
Opzione d: Richiede che la connessione Wi-Fi sia pubblica.
Opzione corretta: a

Domanda 2. Perché è importante aggiornare regolarmente il software del dispositivo?
Opzione a: Perché aumenta lo spazio di archiviazione del dispositivo
Opzione b: Perché rende l'interfaccia del dispositivo più gradevole.
Opzione c: Perché protegge dalle vulnerabilità e dalle minacce alla sicurezza note.
Opzione d: Perché aumenta la durata della batteria del dispositivo
Opzione corretta: c

Domanda 3. Come si possono identificare potenziali frodi o truffe?
Opzione a: Ignorando gli avvisi di sicurezza.
Opzione b: Condividendo ovunque informazioni personali e finanziarie
Opzione c: Affrontando rapidamente gli impegni finanziari.
Opzione d: Imparando a conoscere le più comuni truffe online e stando attenti.
Opzione corretta: d

Domanda 4. Come si può creare una password forte?
Opzione a: Utilizzare una sola parola in minuscolo, senza numeri o caratteri speciali.
Opzione b: Includere lettere maiuscole e minuscole, numeri e caratteri speciali.
Opzione c: Riutilizzare la stessa password per più account.
Opzione d: Scegliere una password facile da indovinare e condividerla con gli amici per non perderla.
Opzione corretta: b

Domanda 5: Quando si fa shopping online, cosa si deve fare se un sito web non ha una connessione sicura?
Opzione a: Procedere comunque all'acquisto.
Opzione b: È meglio evitare di inserire dati personali o di pagamento su quel sito web ed effettuare l'acquisto su un sito web più affidabile con una connessione sicura.
Opzione c: Chiedere a qualcun altro di utilizzare i propri dati per effettuare l'acquisto su quel sito web.
Opzione d: Effettuare l'acquisto utilizzando una rete Wi-Fi pubblica, non ci saranno problemi a condividere i miei dati con quel sito web.
Opzione corretta: b

Bibliografia e ulteriori riferimenti

Co-funded by the European Union

https://www.enisa.europa.eu/ http://www.eun.org/ https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 https://www.microfocus.com/en-us/what-is/cyber-security https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/ https://www.europol.europa.eu/wannacry-ransomware	
Materiale correlato	BOOMER_OnlineSafety_IWS_ITA.pptx
Link di riferimento	
Video in formato Powtoon	https://youtu.be/n5lkYa10I4M

Co-funded by the European Union