13+

PROTEGGERE LE INFORMAZIONI PERSONALI SULLE PIATTAFORME DIGITALI (IMPOSTAZIONI DI SICUREZZA)

MATERIA: Navigazione sicura online

ARGOMENTO DELLA LEZIONE: Impostazioni di sicurezza

DURATA: 45 minuti (1 Lezione); 1-1.5 ore (Preparazione)

OBIETTIVO/I DI APPRENDIMENTO:

Obiettivo principale della lezione:

Studenti e studentesse impareranno a proteggere le informazioni personali sensibili sulle piattaforme digitali, compresi i dati identificativi, i dati delle carte di credito, le informazioni sanitarie, l'indirizzo di casa, i numeri di telefono e altri identificatori personali, oltre all'uso di password forti.

Competenze che verranno acquisite:

- Studenti e studentesse comprenderanno l'importanza di proteggere vari tipi di informazioni personali online.
- Scopriranno le pratiche migliori per proteggere i dati sensibili, come i documenti d'identità, i dati delle carte di credito, i dati sanitari, gli indirizzi di casa e i numeri di telefono.
- Saranno consapevoli dei potenziali rischi associati a una protezione inadeguata delle informazioni personali e come mitigarli.

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

MATERIALI/RISORSE NECESSARIE:

- Modulo 2 (https://www.digi-civis.eu/e-learning)
- Un dispositivo con accesso a Internet (se disponibile) per dimostrare le impostazioni di sicurezza relative alle informazioni personali.
- Scenari ed esempi già preparati (forniti di seguito) da discutere durante la lezione.
- Quiz con domande (fornito di seguito).

METODI/TECNICHE:

- **Presentazione:** L'insegnante offre una panoramica concisa e coinvolgente degli argomenti chiave, sottolineando l'importanza di proteggere i vari tipi di informazioni personali online.
- **Lavoro di gruppo (analisi di scenari)**: La classe viene divisa in piccoli gruppi per discutere e risolvere scenari specifici relativi alla protezione delle informazioni personali.
- **Quiz:** Un breve quiz per valutare la comprensione dei concetti chiave discussi durante la lezione. Questo aiuta a rafforzare l'apprendimento e a identificare le aree che potrebbero richiedere ulteriori chiarimenti.

PANORAMICA DELLA LEZIONE PREPARAZIONE:

Per l'insegnante:

- Approfondite il Modulo 2 del progetto Digi-Civis che tratta i fondamenti delle impostazioni di sicurezza sulle piattaforme digitali.
- Familiarizzate con le impostazioni di sicurezza specifiche relative alle informazioni personali, come la protezione dei documenti d'identità, la sicurezza delle carte di credito e la salvaguardia delle informazioni sanitarie, degli indirizzi di casa e dei numeri di telefono.
- Stampate e ritagliate gli scenari per l'attività di gruppo.
- Stampate le domande del quiz che serviranno a valutare la comprensione di studenti e studentesse alla fine della lezione.

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

SVOLGIMENTO:

1. Introduzione/Breve Presentazione (15 minuti):

Panoramica dell'argomento: Spiegate i concetti essenziali relativi ai dati identificativi, ai dettagli delle carte di credito, alle date di nascita, alle cartelle cliniche e agli indirizzi di casa.

Spiegazione: Le informazioni sui documenti d'identità comprendono identificatori personali come i numeri di previdenza sociale (SSN), i numeri di patente e i numeri di passaporto. Queste informazioni sono fondamentali per verificare l'identità di una persona e possono essere utilizzate per commettere un furto d'identità se cadono nelle mani sbagliate. Il furto di identità si verifica quando qualcuno utilizza illegalmente le informazioni personali di un'altra persona per ottenere benefici finanziari o altri vantaggi.

Perché è importante: Le informazioni sull'identità sono un obiettivo primario per i criminali informatici perché possono essere utilizzate per aprire conti bancari, richiedere prestiti o commettere frodi.

Buone pratiche:

- Non condividete mai il vostro SSN, il numero della patente di guida o il numero del passaporto se non è assolutamente necessario.
- Conservate le copie fisiche di questi documenti in un luogo sicuro (ad esempio, un cassetto o una cassaforte chiusa a chiave)
- Quando fornite informazioni sui documenti d'identità online, assicuratevi che il sito web sia sicuro (cercare “https” e l'icona di un lucchetto).
- Monitorate regolarmente il vostro Rapporto di Credito per individuare eventuali usi non autorizzati dei dati del vostro documento d'identità.

Spiegazione: I dati della carta di credito comprendono il numero della carta, la data di scadenza, il CVV (Card Verification Value) e l'indirizzo di fatturazione. Queste informazioni sono sensibili perché consentono a terzi di effettuare acquisti o prelevare denaro dal vostro conto.

Perché è importante: la frode con carta di credito è una forma comune di crimine finanziario in cui i ladri utilizzano le informazioni rubate della carta per effettuare acquisti non autorizzati.

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

Buone pratiche:

- Inserite i dati della carta di credito solo su siti web sicuri e affidabili.
- Utilizzate numeri di carta di credito virtuali o portafogli digitali (ad esempio, Apple Pay, Google Pay) per le transazioni online.
- Impostate degli avvisi tramite vostra banca o la società di carte di credito per essere avvisati di qualsiasi attività insolita.
- Controllate regolarmente gli estratti conto per individuare eventuali transazioni non autorizzate.

Spiegazione: Dati personali come date di nascita, indirizzi e-mail e persino nomi utente possono essere utilizzati dai criminali per indovinare le password, rispondere alle domande di sicurezza o costruire un profilo per il furto d'identità.

Perché è importante: Le date di nascita sono spesso utilizzate in combinazione con altri dati per reimpostare le password o verificare le identità.

Buone pratiche:

- Siate cauti nel condividere la vostra data di nascita completa online; considerate di condividere solo il mese e il giorno, se necessario.
- Utilizzate indirizzi e-mail diversi per diversi tipi di account (ad esempio, uno per le operazioni bancarie e un altro per i social media).
- Evitate di usare lo stesso nome utente su più piattaforme per rendere più difficile a qualcuno collegare i vostri account.
- Fate attenzione a quante informazioni personali condividete sui profili social.

Spiegazione: Le informazioni sanitarie comprendono le cartelle cliniche, i dati assicurativi e qualsiasi dato relativo alla salute fisica o mentale di una persona. Con l'aumento dei servizi sanitari online e delle cartelle cliniche elettroniche, la protezione di queste informazioni è diventata sempre più importante.

Perché è importante: Le informazioni sanitarie sono dati altamente sensibili e possono essere utilizzate per il furto d'identità, la frode assicurativa o addirittura il ricatto se divulgate in modo improprio.

Buone pratiche:

- Usate canali di comunicazione sicuri e criptati quando condividete informazioni sanitarie online.

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

- Verificate la sicurezza dei portali sanitari online prima di inserire dati sanitari personali.
- Siate cauti nel condividere informazioni sulla salute sui social media o in forum pubblici.
- Abilitare l'autenticazione a due fattori sui portali sanitari, quando possibile.

Spiegazione: L'indirizzo di casa è un'informazione personale che può rivelare il luogo in cui si vive. Se reso noto online, può comportare vari rischi, tra cui stalking, furti e truffe.

Perché è importante: Conoscere l'indirizzo di casa di qualcuno può permettere ai criminali di prenderlo di mira fisicamente (ad esempio, per un furto) o di usare le informazioni per truffarlo (ad esempio, false truffe di consegna).

Buone pratiche:

- Evitate di condividere l'indirizzo di casa pubblicamente online, ad esempio sui social media o sui forum pubblici.
- Utilizzate una casella postale per le consegne se fate spesso acquisti online o vendete articoli.
- Assicuratevi che tutte le piattaforme che richiedono il vostro indirizzo di casa (ad esempio, negozi online) abbiano impostazioni di privacy efficaci.
- Fate attenzione alle richieste del vostro indirizzo, soprattutto al telefono o via e-mail.

Spiegazione: I numeri di telefono sono spesso utilizzati per scopi di verifica e di contatto. Tuttavia, se non sono adeguatamente protetti, possono anche essere sfruttati per truffe, furti di identità o marketing indesiderato.

Perché è importante: I numeri di telefono possono essere utilizzati negli attacchi di SIM-swap (sostituzione di SIM), in cui un hacker prende il controllo del vostro numero di telefono per accedere ai vostri account online.

Buone pratiche:

- Evitate di condividere pubblicamente il vostro numero di telefono online, soprattutto sui social media.
- Usate le applicazioni di autenticazione a due fattori anziché gli SMS, ove possibile, per ridurre il rischio di scambio di SIM.

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

- Considerate la possibilità di utilizzare un numero di telefono secondario o un numero basato su app per i servizi non essenziali.
- Siate cauti con le chiamate o gli SMS non richiesti che chiedono informazioni personali.

2. Lavoro di gruppo su uno scenario (20 minuti):

Scenario 1: Uno studente riceve un messaggio che afferma di provenire dalla sua banca e che gli chiede di verificare l'indirizzo di casa e il numero di telefono. Cosa deve fare?

Soluzioni possibili (per l'insegnante, da non condividere con la classe)

1. Non rispondere al messaggio di testo.
2. Contattare direttamente la banca utilizzando un numero di telefono noto per verificare se la richiesta è legittima.
3. Segnalare il messaggio sospetto all'ufficio frodi della banca.

Scenario 2: Un utente condivide spesso la sua posizione e le foto della propria casa sui social media. Discutete i rischi connessi e le misure da adottare per proteggere la propria privacy.

Soluzioni possibili (per l'insegnante, da non condividere con la classe)

1. Evitate di condividere dettagli specifici sulla posizione in tempo reale.
2. Regolate le impostazioni sulla privacy per limitare chi può visualizzare i post.
3. Siate cauti nel taggare i luoghi o nel menzionare i dettagli della casa nei post.

Scenario 3: Qualcuno riceve una telefonata non richiesta da una persona che sostiene di essere del suo fornitore di servizi sanitari e che gli chiede il numero di assicurazione sanitaria e altri dati personali. Come si dovrebbe rispondere?

Soluzioni possibili (per l'insegnante, da non condividere con la classe)

1. Non fornite nessuna informazione al telefono.
2. Riattaccate e contattate direttamente l'operatore sanitario utilizzando un numero di telefono verificato.
3. Segnalate la chiamata all'ufficio frodi dell'operatore sanitario.

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

Scenario 4: Una persona elenca l'indirizzo di casa e il numero di telefono sul profilo di un sito online per rendere più conveniente la vendita di articoli. Discutete i potenziali rischi e come ridurli.

Soluzioni possibili (per l'insegnante, da non condividere con la classe)

1. Utilizzate il sistema di messaggistica privata della piattaforma invece di condividere le informazioni di contatto personali.
2. Considerate l'utilizzo di una casella postale o di un numero di telefono temporaneo.
3. Incontrate gli acquirenti in luoghi pubblici invece di fornire l'indirizzo di casa.

Ogni gruppo (3-5 studenti/studentesse) discute lo scenario assegnatogli e presenta alla classe le soluzioni proposte, spiegando le motivazioni alla base di ogni azione.

MAGGIORI INFORMAZIONI PER SAPERNE DI PIÙ:

- Kaspersky, Cose da non fare su Internet: la top 10 delle regole per navigare in sicurezza su Internet
- Online Privacy & Security 101: How To Actually Protect Yourself? https://www.youtube.com/watch?v=qZE45J-MIUg

ALLEGATI:

- Quiz di valutazione

COMPITI A CASA:

Studenti e studentesse devono rivedere e proteggere le informazioni personali che condividono online, tra cui l'indirizzo di casa, il numero di telefono, la data di nascita e altri dati personali. Devono applicare almeno una nuova misura di sicurezza discussa in classe.

Riflessione: Fate loro scrivere un breve paragrafo sulle modifiche apportate e su come ritengono che queste modifiche possano proteggere meglio le loro informazioni personali.

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

VALUTAZIONE:

- Valutate studenti e studentesse in base al loro coinvolgimento nelle discussioni di gruppo e alla qualità delle soluzioni presentate.
- Valutate le risposte al quiz per verificare la comprensione dei concetti chiave.
- Incoraggiateli a condividere una nuova azione che intendono intraprendere per proteggere le loro informazioni personali online, spiegando perché è necessaria.

Quiz (15 minuti):

Quiz scritto:

1. Domanda: Perché è importante non condividere pubblicamente online il proprio indirizzo di casa?

(Risposta: Condividere pubblicamente l'indirizzo di casa può rendervi bersaglio di furti, truffe e visite indesiderate.)

2. Domanda: Cosa dovete fare se ricevete una telefonata sospetta che vi chiede informazioni personali?

(Risposta: Non fornite alcuna informazione; riagganciate e contattate direttamente l'organizzazione utilizzando un metodo di contatto verificato.)

3. In che modo la condivisione del vostro numero di telefono online può mettervi a rischio?

(Risposta: Il numero di telefono può essere utilizzato per furti di identità, attacchi di SIM-swap e marketing indesiderato.)

4. Domanda: Quali sono i rischi della condivisione di informazioni sanitarie su canali non protetti?

(Risposta: Le informazioni sanitarie possono essere intercettate, con conseguenti violazioni della privacy o furti di identità.)

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.