Scheda corso E-Seniors

|  |  |
| --- | --- |
| **Titolo** | **Argomento: Informazione e comunicazione attraverso i social media**  **Unità 3. Minacce e sfide sui social media: COSA FARE e NON FARE** |
| **Area di formazione** | *Si prega di selezionare una o più delle seguenti opzioni:*   |  |  | | --- | --- | | Sicurezza Online |  | | Alfabetizzazione Culturale e Mediatica | *X* | | Transazioni Economiche |  | | Protezione di dati personali |  | | Identità digitale e reputazione online |  | |
| **Parole chiave (meta tag)** | **Social media, comunicazione, sicurezza** |
| **Promosso da** | **E-Seniors** |
| **Lingua** | **Italiano** |
| **Obiettivi / finalità / risultati di apprendimento** | |
| Questo modulo mira a sviluppare le conoscenze e le competenze degli utenti su come utilizzare i social media per la comunicazione e la promozione della cultura e della creatività. Gli utenti senior acquisiranno familiarità con gli strumenti dei social media, le risorse culturali sui social media che permettono loro di navigare facilmente e scoprire opportunità culturali e di comunicazione. | |
| **Descrizione** | |
| Il corso è organizzato su 3 livelli: ogni modulo è diviso in unità. I titoli delle unità danno un'idea più dettagliata del contenuto del modulo. I moduli sono riuniti sotto un tema comune:  **Argomento: Informazione e comunicazione attraverso i social media**  **Module 3. Minacce e sfide sui social media: COSA FARE e NON FARE**  **Unit 3.1:** Minacce e sfide  **Unit 3.2:** 10 regole da adottare per la sicurezza sui social network. | |
| **Contenuti organizzati su 3 livelli** | |
| **Module 3: Minacce e sfide sui social media: COSA FARE e NON FARE**  Ci sono molte minacce e sfide legate alla navigazione in internet, sia sul computer che sullo smartphone. I social network non fanno eccezione. Ci sono diversi rischi legati all'uso dei social network. Tuttavia, se si prendono delle precauzioni, non è difficile navigare con un rischio minimo.  **Unit 3.1:** Minacce e sfide  **Phishing:** è un metodo di inganno digitale in cui un aggressore invia un messaggio fraudolento progettato per truffare una persona. Questi messaggi sono progettati per indurti a rivelare informazioni personali fingendo di provenire da una fonte affidabile. I messaggi possono provenire da persone che sostengono di essere un tuo amico o un'azienda conosciuta. Non condividere mai informazioni riservate e non cliccare mai su un link web dall'aspetto sospetto.  **Psychological hacking:** La “manipolazione psicologica” è il processo per ottenere informazioni confidenziali da una persona attraverso l'inganno. Il truffatore può iniziare una conversazione sucose che hanno letto sul tuo profilo, come ad esempio dove lavori, ecc. Poi cerca di farti rivelare informazioni personali, in modo simile al phishing.  **Malware:** Il malware è un software pericoloso progettato per infiltrarsi nei dispositivi. Circola sui social network come link con titoli accattivanti. Una volta che il malware si è infiltrato, può inviare messaggi ai contatti, accedere a informazioni personali o danneggiare il dispositivo. Bisogna fare attenzione quando si è tentati di cliccare su un link da una fonte sconosciuta.  **Hate speech:** I discorsi che incitano all'odio sono comuni sui social network perché i loro autori possono rimanere anonimi. Può capitare di ricevere discorsi carichi di odio, a volte senza alcun nesso, quindi è importante distaccarsene e non esitare a segnalarli come contenuti indesiderati e nocivi.  **Cyberbullying:** è il bullismo che ha luogo su dispositivi digitali come telefoni cellulari, computer e tablet. Il cyberbullismo può avvenire attraverso SMS, testi e applicazioni, oppure online nei social media, nei forum o nei giochi dove le persone possono visualizzare, partecipare o condividere contenuti. Il cyberbullismo comprende l'invio, la pubblicazione o la condivisione di contenuti negativi, dannosi, falsi o meschini su qualcun altro. Può includere la condivisione di informazioni personali o private su qualcun altro causando imbarazzo o umiliazione. Alcune forme di cyberbullismo si spingono fino a comportamenti illegali o criminali.  **Ageismo online:** con il termine ageismo ci si riferisce agli stereotipi (come pensiamo), ai pregiudizi (come ci sentiamo) e alla discriminazione (come ci comportiamo) verso gli altri o verso se stessi in base all'età. L'ageismo colpisce tutti. I bambini già a 4 anni diventano consapevoli degli stereotipi sull'età usati nella loro cultura. Da quell'età in poi interiorizzano e usano questi stereotipi per guidare i loro sentimenti e comportamenti verso persone di età diverse. Anche per percepire e capire se stessi, il che può risultare in un ageismo guidato da sé stessi a qualsiasi età. L'ageismo interseca ed esaspera altre forme di svantaggio, comprese quelle legate al sesso, alla razza e alla disabilità.   * **A cosa fare attenzione per evitare le truffe su Facebook:** * Persone che non conosci personalmente che ti chiedono soldi o i tuoi dati bancari. * Pagine non verificate che affermano di rappresentare una grande organizzazione o una figura pubblica. * Persone che ti chiedono di continuare la conversazione fuori da Facebook, in un ambiente meno pubblico o meno sicuro, come un indirizzo email separato. * Persone che ti chiedono di inviare i tuoi dati bancari per ricevere una ricompensa. * Chiunque affermi di essere un vostro amico o parente in difficoltà. * Persone che mentono su dove vivono. * Messaggi o pubblicazioni che contengono errori di ortografia e grammatica. * Persone o account che ti reindirizzano a una pagina per richiedere un premio   **Unit 3.2: 10 regole da adottare per la sicurezza sui social network:**  1- **Proteggi l'accesso ai tuoi profili:** Usate password forti e diverse da un account all'altro. Le applicazioni di gestione delle password possono aiutarvi a salvare facilmente le vostre password. Ad esempio **https://keepassxc.org/**  2- **Controlla le impostazioni della tua privacy**: di default, le impostazioni della privacy sono spesso aperte (su informazioni personali come nome, numero di telefono, indirizzo e-mail). Questi dati possono essere accessibili a tutti gli iscritti ai social network. È possibile limitare questa visibilità regolando la configurazione dell'account per mantenere il controllo di ciò che gli altri utenti vedono.  3- **Controlla i tuoi post:** I tuoi post possono sfuggire di mano ed essere ripubblicati o interpretati più di quanto tu voglia. Non pubblicare informazioni personali o sensibili.  4- **Fai attenzione alle persone con cui parli:** I tuoi amici potrebbero condividere contenuti maliziosi senza saperlo, o potrebbero essere stati loro stessi hackerati. Non inviare mai denaro senza verificare l'identità della persona, non inviare video privati, non fidarti di concorsi, vincite inaspettate o "grandi offerte" che possono nascondere truffe.  5-  **Controlla le applicazioni usate da soggetti terzi:** Alcune applicazioni propongono di interagire con uno dei vostri account di social network. Richiedono autorizzazioni che devono essere esaminate con attenzione, poiché alcune di esse potrebbero poi ottenere l'accesso ai vostri dati. Fate attenzione a non installare applicazioni che sospettate siano dannose.  6- **Evita i computer e le reti pubbliche:** Usare un computer con accesso libero o una connessione Wi-Fi pubblica è rischioso, perché potrebbero essere compromessi o sotto il controllo di criminali informatici. Evita di inserire informazioni sensibili o di usarli se possibile.  7- **Controlla regolarmente gli accessi al tuo account:** La maggior parte dei social network ti permette di vedere le connessioni o le sessioni degli account attivi. Controlla queste informazioni regolarmente per assicurarti che un altro dispositivo non sia collegato a uno dei tuoi account. Se lo è, scollegalo e cambia la tua password.  8- **Diffida dalle notizie false:** Alcune informazioni pubblicate possono essere false, deliberatamente o meno. Prima di considerare o trasmettere qualsiasi informazione, verificatene l'autenticità.  9- **Controlla le credenziali del tuo account:** Alcuni siti web propongono di registrarti con il tuo account di social network. Questo evita la necessità di creare una password, per esempio, ma può fornire dati personali al sito o permettere a un criminale informatico che ha violato il tuo social network di accedere al tuo account anche da quel sito.  10- **Elimina il tuo account se non lo usi più:** Per evitare tutti i rischi descritti sopra, per assicurarsi che il suo account non sia utilizzato a tua insaputa, cancella il tuo account quando non ne hai più bisogno. | |
| **Lista dei contenuti** | |
| * Le minacce e le sfide più frequenti nell'uso dei social media sono quelle di difendersi da phishing, malware, hate speech, ecc; * È possibile evitare le minacce e i rischi dei social media seguendo le raccomandazioni e i consigli indicati in questo modulo di formazione | |
| **5 vocaboli chiave** | |
| **Social media safety:** La sicurezza sui social media si riferisce a tutte le misure che l'utente dovrebbe adottare per evitare rischi, truffe e attacchi al proprio account personale.  **Hate speech:** I discorsi pieni di odio sono parole pronunciate che risultano offensive, insultanti e/o minacciose per un individuo o un gruppo sulla base di un particolare carattersitica della persona o delle persone prese di mira.  **Psychological hacking:** La manipolazione psicologica è il processo per ottenere informazioni riservate da una persona attraverso l'inganno.  **Cyberbullismo:** è il bullismo che ha luogo su dispositivi digitali come telefoni cellulari, computer e tablet  **Ageismo online**: L'ageismo si riferisce agli stereotipi (come pensiamo), al pregiudizio (come ci sentiamo) e alla discriminazione (come ci comportiamo) verso gli altri o se stessi in base all'età. L'ageismo colpisce tutti. | |
| **Bibliografia e altre referenze** | |
| [**https://understandthesocialmedia.com/**](https://understandthesocialmedia.com/)  [**https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf**](https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf) | |
| **Cinque domande di autovalutazione a scelta multipla** | **1) È sicuro usare i computer pubblici**   1. **Vero** 2. **Falso**   **Corretto: B**  **2) Cos’è Malware?**   1. **Software malizioso progettato per infiltrarsi nei dispositivi** 2. **Frode d'identità** 3. **Discorso d’odio**   **Corretto: A**  **3) Cos’è un “hate speech”?**   1. **Sono parole pronunciate che risultano offensive, insultanti e/o minacciose per un individuo o un gruppo sulla base di un particolare attributo della persona o delle persone prese di mira.** 2. **È il processo per ottenere informazioni riservate da una persona attraverso l'inganno.** 3. **È un'informazione maliziosa progettata per infiltrarsi nei dispositivi e attaccare gli esseri umani.**   **Corretto: A**  **4) Social media safety:**   1. **Si riferisce a tutte le misure che le aziende adottano per difendersi dalle frodi online.** 2. **Si riferisce a tutte le misure che l'utente dovrebbe adottare per evitare rischi, truffe e attacchi al proprio account personale.** 3. **Si riferisce agli strumenti che i social media hanno progettato per gli utenti.**   **Corretto: B**  **5) Cosa fare se vi imbattete in un hate speech online?**   1. **Cerca di evitare gli aggressori** 2. **Cerca di denunciare gli aggressori** 3. **Tutti i casi di cui sopra sono corretti**   **Corretto: C** |
| **Materiale correlato** | **Come identificare ed evitare le truffe tipiche sui social media:** [**https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/**](https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/)  **Come evitare le frodi sui social media:** [**https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html**](https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html)  **Cyberbullismo e Hate Speech:** [**https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf**](https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf) |
| **PPT correlato** |  |
| **Link di riferimento** | **https://www.stopbullying.gov/cyberbullying/what-is-it** |
| **Video YouTube (se presente)** | **Cos'è il social media? In linguaggio semplice:**  [**https://www.youtube.com/watch?v=jQ8J3IHhn8A**](https://www.youtube.com/watch?v=jQ8J3IHhn8A)  **Un incredibile esperto di lettura della mente rivela il suo "dono”:** [**https://www.youtube.com/watch?v=F7pYHN9iC9I**](https://www.youtube.com/watch?v=F7pYHN9iC9I) |