Scheda corso IWS

|  |  |
| --- | --- |
| **Titolo** | **Sicurezza online e creatività: che cosa succede?** |
| **Area di formazione** | *Per favore selezionare una o più opzioni:*   |  |  | | --- | --- | | Sicurezza Online | *X* | | Alfabetizzazione Culturale e dei Media | *X* | | Transazioni Economiche |  | | Protezione di dati personali |  | | Identità digitale e reputazione online |  | |
| **Parole chiave (meta tag)** | **Truffe, frodi, trucchi per la sicurezza online, Internet** |
| **Promosso da** | **Internet Web Solutions** |
| **Lingua** | **Italiano** |
| **Obiettivi / finalità / risultati di apprendimento** | |
| **Al termine di questo modulo, sarai in grado di conoscere la sicurezza online nel mondo della cultura online. Questa unità si concentrerà su:**  **Unità 2.1 Truffe più comuni online: esempi delle più comuni truffe online, proteggendo le tue informazioni online.**  - Sezione 2.1.1. introduzione  - Sezione 2.1.2. Annunci di lavoro  - Sezione 2.1.3. Truffa bancaria  - Sezione 2.1.4. Acquisti online  - Sezione 2.1.5. Prodotti di terze parti  - Sezione 2.1.6. Eredità tramite whatsapp  - Sezione 2.1.7. Uomini/Donne affascinanti innamorati/e di te  - Sezione 2.1.8. SMS truffa dalla tua banca  - Sezione 2.1.9. Truffa della lotteria  - Sezione 2.1.10. Falsi enti di beneficenza  **Unità 2.2. Sicurezza online nel mondo culturale, come evitare truffe specifiche del mondo culturale (biglietti falsi, hacking o phishing)**  - Sezione 2.2.1 Come si comportano i truffatori  - Sezione 2.2.2. Passi per proteggerti  **- Unità 2.3. Suggerimenti per la sicurezza online**  - Sezione 2.3.1. Come impostare una password sicura | |
| **Descrizione** | |
| Questo corso è rivolto a persone adulte che stanno imparando le basi di Internet. Il modulo svilupperà concetti fondamentali per gli utenti anziani al fine di renderli capaci di valutare i sistemi di sicurezza online e di proteggere le proprie informazioni, rendendoli consapevoli delle potenziali truffe e frodi che potrebbero incontrare sul web durante l'utilizzo o la ricerca di risorse culturali. Questa unità di apprendimento insegnerà agli anziani come identificare le truffe finanziarie online più comuni e come proteggere le loro informazioni finanziarie e i loro conti. | |
| **Contenuti organizzati su 3 livelli** | |
| **Modulo 2: SICUREZZA E CREATIVITÀ ONLINE: CHE COSA SUCCEDE?**  **Unità 2.1 Truffe più comuni online: esempi delle più comuni truffe online, per proteggere le tue informazioni online.**  **Sezione 2.1.1. introduzione**  Le frodi su Internet stanno diventando sempre più comuni a causa del numero crescente di persone che utilizzano Internet quotidianamente.  Queste truffe non vogliono solo i tuoi soldi, ma vogliono anche le tue informazioni, e queste ultime sono più difficili da identificare.  Il funzionamento di base delle truffe non è cambiato, offrono prodotti o servizi in cambio di una somma di denaro "troppo bella per essere vera" o in cambio di qualche domanda per ottenere informazioni.  Possono anche offrire prestiti o offerte di lavoro come mezzo per farti abboccare.  **Sezione 2.1.2. Truffe con offerte di lavoro**  Ad esempio, un annuncio di lavoro propone uno stipendio a tempo pieno solo con orari giornalieri part-time e non richiede alcuna esperienza precedente. Lo stipendio è troppo alto e questo potrebbe essere considerato un primo indizio che l'annuncio potrebbe essere una truffa.  Prima di compilare il form o fornire informazioni è sempre bene verificare:  - l'autenticità del sito web dove è pubblicato l'annuncio  - la qualità delle immagini o dei commenti in caso di vendita di prodotti  - la società che pubblica l'annuncio  - le indennità di lavoro offerte  **Sezione 2.1.3. Truffe Bancarie**  Altri tentativi di frode possono consistere nel farsi passare per un'entità come la tua Banca o un sito che frequenti, inviandoti un link sospetto magari con la scusa di una grande offerta o di qualcosa che non va.  Se pensi che la comunicazione possa essere importante, come nel caso della tua Banca, chiamali invece di cliccare sul link.  **Sezione 2.1.4. Shopping Online**  Lo shopping online sta diventando sempre più comune, quindi ecco alcuni suggerimenti per farlo in modo sicuro.  - Il sito web deve avere una connessione crittografata sicura, il protocollo web deve essere https.  - Assicurati di essere su un sito Web affidabile. Un sito Web con prezzi anormalmente bassi, tutti i prezzi uguali, nessuna recensione o immagini di prodotti sospette indicano che il sito Web è una truffa.  **Sezione 2.1.5. Podotti venduti da terzi**  Alcuni siti Web vendono prodotti di terze parti. In questi casi è doveroso indagare sull'azienda da cui proviene il prodotto.  È un buon segno se il sito è chiaro nella visualizzazione delle informazioni sui costi e sulla spedizione, accetta diverse forme di pagamento e invia una fattura di acquisto.  Se ritieni che il sito sia autentico e fai un acquisto, non salvare mai i dati della tua carta di credito: questo impedirà a qualcuno di accedere in seguito dal tuo dispositivo ed effettuare acquisti indesiderati.  Controlla periodicamente il tuo saldo e, se noti movimenti sospetti, segnalali rapidamente alla tua banca.  Se il prodotto non arriva, prova a contattare la piattaforma o il venditore da cui hai effettuato l’acquisto.  **Sezione 2.1.6. Eredità via whatsapp**  Su WhatsApp una persona ti scrive affermando di essere molto anziana, senza eredi, e propone a te di ereditare la sua fortuna.  Qualcun altro potrebbe scriverti per suggerirti un trucco per investire senza rischi, promettendoti di guadagnare 100.000€ in un solo mese.  **Sezione 2.1.7. Uomini/Donne affascinanti innamorati/e di te**  Una persona con una fotografia attraente che non conosci affatto ti contatta e ti parla di argomenti suggestivi.  Sii cauto con chiunque incontri online dall'estero.  Scopri i segni di una truffa relazionale: cosa bisogna guardare.  Non inviare mai denaro.  Se hai già dato loro dei soldi, non andare all'estero per cercare di riaverli indietro.  Conferma sempre la loro identità e legittimità prima di andare all'estero per incontrarli.  **Sezione 2.1.8. SMS truffa dalla tua Banca**  Un SMS arriva sul tuo cellulare dalla tua presunta banca dicendo che c'è un errore con il tuo conto e devi compilare un modulo.  Una persona finge di essere un moderatore di un social network e ti chiede di fornirgli la tua password per risolvere un problema.  Su un sito Web di offerte di lavoro di terze parti, offrono il doppio di uno stipendio normale.  Quando provi a effettuare un acquisto da un individuo, quest’ultimo ti chiede di pagarlo in anticipo oppure non è in grado di darti alcuna informazione sulla spedizione.  **Sezione 2.1.9. Truffe della lotteria**  Una truffa della lotteria è un tipo di frode a pagamento anticipato che inizia con una e-mail, una telefonata o una notifica inaspettata (a volte contenente un assegno di grandi dimensioni) nella quale ti viene annunciato che "Hai vinto!" una grossa somma di denaro in una lotteria.  Al destinatario del messaggio - il vero obiettivo della truffa - viene solitamente detto di mantenere segreto l'avviso "a causa di un errore di alcuni nomi e numeri" e di contattare un "agente di reclamo".  Dopo aver contattato l'agente, al bersaglio della truffa verrà chiesto di pagare delle "spese di elaborazione" o delle "spese di trasferimento" in modo che le vincite possano essere distribuite, ma non riceverà mai alcun pagamento della lotteria.  **Sezione 2.1.10. Finte donazioni**  I truffatori possono impersonare veri enti di beneficenza e chiedere donazioni, oppure contattarti affermando di raccogliere denaro dopo disastri naturali o eventi importanti.  Gli enti di beneficenza falsi cercheranno di sfruttare la tua generosità e compassione per i bisognosi, e i truffatori ruberanno i tuoi soldi fingendosi un vero ente di beneficenza. Non solo queste truffe ti costano denaro, ma deviano anche le donazioni tanto necessarie ai veri enti di beneficenza e alle loro cause legittime.  Approcci di finta beneficenza si verificano tutto l'anno e spesso assumono la forma di una risposta a disastri o emergenze reali, come inondazioni, cicloni, terremoti e incendi boschivi.  **Unità 2.2. SICUREZZA ONLINE NEL MONDO DELLA CULTURA: COME EVITARE LE TRUFFE TIPICHE DEL SETTORE CULTURALE (BIGLIETTI FALSI, HACKING O PHISHING).**  **Sezione 2.2.1. Come agiscono i truffatori**  I truffatori possono:  - creare siti Web falsi  - utilizzare siti Web autentici per pubblicare annunci falsi  - offrire falsi ingressi VIP e pacchetti di biglietti per concerti e musei  Per evitare una truffa sui biglietti:  > fai una scelta ponderata quando guardi il sito web del rivenditore  > utilizza un sito Web affidabile  Ci sono rivenditori di biglietti legali, ma se un affare sembra troppo bello per essere vero, probabilmente non lo è.  **Sezione 2.2.2. Le mosse giuste per proteggerti**  Usa il buon senso prima di divulgare informazioni sensibili.  Non fidarti mai dei messaggi allarmanti.  Non aprire gli allegati in queste e-mail sospette o strane, in particolare gli allegati Word, Excel, PowerPoint o PDF.  Usa un sito web affidabile  **Unità 2.3. TRUCCHI PER LA SICUREZZA ONLINE**  Quando hai un account di social network, usalo solo per parlare con persone che conosci nella vita reale e per pubblicare opinioni o immagini (meglio senza dati sensibili).  Sii sempre consapevole di rispettare i termini di utilizzo del sito e di non commettere illeciti.  **Sezione 2.3.1. Come impostare una password sicura**  Sii sempre consapevole di rispettare i termini e condizioni di utilizzo del sito e di non trasgredire le regole.  Non credere a immagini sconosciute: non fare affidamento su immagini come chat e screenshot.  Non fare clic su allegati sconosciuti.  Controlla la fonte dei tuoi messaggi.  Non condividere mai i tuoi dati personali.  Attenzione a possibili truffe.  Proteggi i tuoi dati finanziari.  Evita di condividere i dettagli di base.  Utilizzare password o PIN con caratteri come &, \*. \_\_, minuscolo e MAIUSCOLA. | |
| **Lista dei contenuti** | |
| * Utilizzare password o PIN con caratteri come &, \*. \_\_, minuscolo e MAIUSCOLA. * Una volta che hai un account di social network, puoi usarlo solo per parlare con persone che conosci nella vita reale e pubblicare opinioni o immagini (meglio senza dati sensibili). * Approcci di finta beneficenza si verificano tutto l'anno e spesso prendono la forma di una risposta a disastri o emergenze reali, come inondazioni, cicloni, terremoti e incendi boschivi. * Una truffa della lotteria è un tipo di frode a pagamento anticipato che inizia con una e-mail, una telefonata o una notifica inaspettata (a volte contenente un assegno di grandi dimensioni) che spiega: "Hai vinto!" una grossa somma di denaro in una lotteria. | |
| **5 vocaboli chiave** | |
| **Truffa della lotteria:** Una truffa della lotteria è un tipo di frode a pagamento anticipato che inizia con una e-mail, una telefonata o una notifica inaspettata (a volte contenente un assegno di grandi dimensioni) che spiega: "Hai vinto!" una grossa somma di denaro in una lotteria.  **Finta carità:** tipo di frode che si verifica quando le organizzazioni di beneficenza sollecitano fondi dal pubblico per scopi filantropici, come cercare cure per malattie o aiutare le famiglie degli agenti di polizia uccisi.  **Prodotti di terze parti:** si riferisce a qualsiasi prodotto e/o servizio di terzi offerto da o tramite l'intermediario della Banca.  **Truffa:** Una truffa o un trucco di fiducia è un tentativo di frodare una persona o un gruppo guadagnando la loro fiducia.  **Phishing:** Il phishing è un tipo di ingegneria sociale in cui un utente malintenzionato invia un messaggio fraudolento (contraffatto, falso o ingannevole) progettato per indurre una vittima a rivelare informazioni riservate o per diffondere un software dannoso. | |
| **Bibliografia e altre referenze** | |
| [**https://www.careercast.com/career-news/10-ways-build-your-online-identity**](https://www.careercast.com/career-news/10-ways-build-your-online-identity)  [**https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/**](https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/)  [**https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php**](https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php)[**https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html**](https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html)  [**https://whatis.techtarget.com/definition/digital-identity**](https://whatis.techtarget.com/definition/digital-identity)  [**https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html**](https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html)[**https://www.techopedia.com/definition/23915/digital-identity**](https://www.techopedia.com/definition/23915/digital-identity)  [**https://www.techopedia.com/definition/1327/domain-name**](https://www.techopedia.com/definition/1327/domain-name) | |
| **Cinque domande di autovalutazione a scelta multipla** | **1) Quali sono i segnali di allerta per identificare una frode bancaria?**  A. Un collegamento sospetto ricevuto tramite e-mail  B. Un'e-mail ufficiale dalla tua banca  C. Un'e-mail da un'associazione di beneficenza  ***Risposta giusta: A***  **2) Cosa dovresti fare se rimani vittima di una truffa bancaria?**  A) Fornisci le tue informazioni personali  B) Fare clic su allegati sconosciuti  C) Chiamare la banca per verificare il problema  ***Risposta giusta: C***  **3) Come evitare una truffa sui biglietti?**  A) Evita di acquistare biglietti online  B) Acquista solo da rivenditori online ufficiali  C) Utilizzare un sito Web di un rivenditore di biglietti sospetto  ***Risposta giusta***: B  **4) Come sono gli approcci di Finta Beneficienza?**  A) Spesso assumono la forma di una risposta a una reale richiesta di aiuto di un tuo parente accertato.  B) Spesso assumono la forma di una risposta alla reale richiesta di aiuto di un accertato amico di famiglia  C) Spesso assumono la forma di una risposta a disastri o emergenze, come inondazioni, cicloni, terremoti e incendi boschivi.  ***Risposta giusta***: C  **5) Come impostare una password sicura?**  A) Usando il tuo indirizzo  B) Usando il tuo nome completo  C) Usare caratteri come &, \*. \_\_, minuscolo e MAIUSCOLA.  **Risposta giusta: C** |
| **Materiale correlato** |  |
| **PPT correlato** | [**SOS creativity\_Modulo 2 - Sicurezza Online e creatività: cosa succede?**](http://ppts/SOS%20creativity%20Module%202%20Online%20security%20and%20creativity%20what%E2%80%99s%20up.pptx) |
| **Link di riferimento** |  |
| **Video YouTube (se presente)** | Online safety for grown ups, Bristol City Council Skills & Learning - Adult & Community Learning Service [**https://www.youtube.com/watch?v=iCs3aJYXLwo**](https://www.youtube.com/watch?v=iCs3aJYXLwo) |