Scheda corso IWS

|  |  |
| --- | --- |
| **Titolo** | **Identità digitale e reputazione online** |
| **Area di formazione** | *Per favore selezionare una o più opzioni:*   |  |  | | --- | --- | | Sicurezza Online |  | | Alfabetizzazione Culturale e dei Media |  | | Transazioni Economiche |  | | Protezione di dati personali |  | | Identità digitale e reputazione online | X | |
| **Parole Chiave (meta tag)** | **Identità digitale, reputazione online, internet, frodi online, truffe, social networks** |
| **Promosso da** | **Internet Web Solutions** |
| **Lingua** | **Italiano** |
| **Obiettivi / finalità / risultati di apprendimento** | |
| **Alla fine di questo modulo sarai in grado di:**  **Sapere ciò che serve a proposito di identià digitale e reputazione virtuale.**  **Questa unità si concentrerà su:**  **Unità 3.1. Dottor Jekyll e Mister Hyde (chi sei e chi sono gli altri in internet: come saperlo e proteggerti)**  Sezione 3.1.1 Introduzione  Section 3.1.2. Furto di identità: cosa succede se qualcuno ruba la tua identità online?  Sezione 3.2.3. Furto di Account: cosa accade se qualcuno utilizza il tuo account? Alcuni trucchi per evitarlo.  Sezione 3.2.4. Altri trucchi | |
| **Descrizione** | |
| Questa unità fornirà elementi utili per capire cosa fare e non fare su internet per proteggere la propria identità digitale, come ad esempio non utilizzare computer pubblici, impostare una password forte e complessa, assicurarsi di utilizzare una connessione sicura, sfruttare l’autenticazione in due tempi e altro ancora. Questa unità tratterà anche i modi sicuri di utilizzare i social media e cosa è meglio non rivelare online. | |
| **Contenuti organizzati su tre livelli** | |
| **UNITÀ 3.1 DOTTOR JEKYLL E MISTER HYDE (CHI SEI E CHI SONO GLI ALTRI IN INTERNET: COME SAPERLO E PROTEGGERTI)**  **Sezione 3.1.1 Introduzione**  Su Internet sei tutto ciò che pubblichi e tutto ciò che commenti con gli altri utenti.  Tutto ciò che pubblichi online può essere visto da altri utenti.  Anche se le tue impostazioni sulla privacy permettono "solo agli amici" (o simili) di vedere i tuoi contenuti, una persona che vuole vedere il tuo post trova il modo di farlo.  Credendo che stando dietro uno schermo le persone non possano vederti, potresti comportarti diversamente da chi sei in realtà.  A differenza della vita reale, qualsiasi cosa pubblichi su Internet ha visibilità mondiale.  Ciò significa che persone da tutto il mondo possono scoprire cose di te e, allo stesso modo, puoi scoprire cose di persone da tutto il mondo.  In internet un truffatore può identificare molte più persone e scegliere la sua vittima con maggiore attenzione: questo e altri fattori rendono le truffe online sempre più comuni.  **Sezione 3.1.2. Furto d’identità: cosa succede se qualcuno ruba la tua identità digitale?**  Una persona che accede illegalmente al tuo account può eseguire molte azioni dannose.  Nella migliore delle ipotesi, possono impersonarti per pubblicare post compromettenti o illegali.  Nel peggiore dei casi, possono impersonarti e parlare con i tuoi conoscenti o familiari, Il furto d’identità non danneggia solo te!  Qualcuno che abbia avuto accesso ai tuoi dati bancari potrebbe iniziare a fare acquisti o transazioni online e rubare denaro.  Se ciò dovesse accadere, prova a parlare con il supporto della piattaforma in cui è stato rubato il tuo account, cambia le password, avvisa le persone interessate e, se il ladro è stato in grado di effettuare un acquisto, avvisa anche la tua banca.  **Sezione 3.2.3 Furto di account: cosa succeed se qualcuno usa un tuo account?**  Ci sono alcune cose che puoi fare per evitare il furto dell'account:  Non salvare le password su nessun dispositivo, prova a ricordarle.  Prova a utilizzare password diverse per siti diversi. Se qualcuno scopre la tua password per una piattaforma, non sarà in grado di accedere ad altri siti.  Non utilizzare il tuo nome, nome utente o altre informazioni personali sulla piattaforma, renderebbe più facile scoprire la tua password.  Utilizza password più lunghe di 8 caratteri e usa un numero o un carattere speciale per evitare attacchi di forza bruta per scoprire la tua password.  Non condividere mai la tua password online, anche se una persona ti dice di essere un moderatore, un amministratore o uno staff di supporto di un sito.  **Sezione 3.2.4. Qualche trucco per evitarlo**  Prima di tutto, devi anche stare attento a ciò che pubblichi sui social media.  Cerca di pubblicare il minor numero possibile di informazioni su di te, in particolare informazioni sensibili, dettagli identificativi o coordinate bancarie.  Informazioni importanti che NON dovresti condividere pubblicamente potrebbero essere:   * Luogo in cui vivi * Indirizzo email * Numero di telefono * Contenuti multimediali compromettenti * Documenti personali * Informazioni sulle tue transazioni bancarie * Informazioni sullo stipendio * Password di qualsiasi tipo   Evita di accedere agli account dal computer di altre persone, in particolare su computer pubblici.  Molte piattaforme supportano l'autenticazione in due passaggi, ad es. usando il tuo numero di telefono: usalo quando ne hai l'opportunità.  Ciò che va online, rimane online per sempre. Quello che pubblichi, quello che dici, come ti comporti, sarà a disposizione di tutti, inclusi: possibili futuri datori di lavoro, la tua famiglia, i tuoi figli e i tuoi amici. E non solo ora, anche in futuro! | |
| **Lista dei contenuti** | |
| * Cerca di pubblicare il minor numero possibile di informazioni su di te, in particolare informazioni sensibili, dettagli identificativi o coordinate bancarie. * Ciò che va online, rimane online per sempre. Quello che pubblichi, quello che dici, come ti comporti, sarà disponibile per tutti, inclusi: possibili futuri datori di lavoro, la tua famiglia, i tuoi figli e i tuoi amici. E non solo ora, anche in futuro. * Usa password più lunghe di 8 caratteri e usa un numero o un carattere speciale per evitare attacchi di forza bruta per scoprire la tua password. | |
| **5 vocaboli chiave** | |
| **Identità digitale:** L'identità digitale è ora spesso utilizzata in modi che richiedono che i dati sulle persone archiviati nei sistemi informatici siano collegati alle loro identità civili o nazionali.  **Reputazione in linea:** È la reputazione di un'azienda, persona, prodotto, servizio o qualsiasi altro elemento su Internet e piattaforme digitali.  **Autenticazione in due passaggi:** È un metodo di autenticazione elettronica in cui a un utente viene concesso l'accesso a un sito Web o a un'applicazione solo dopo aver presentato con successo due o più elementi di prova (o fattori) a un meccanismo di autenticazione.  **Furto d'identità:** La pratica fraudolenta di utilizzare il nome e le informazioni personali di un'altra persona al fine di ottenere credito, prestiti, ecc.  **Truffatore:** Un truffatore può ricercare molte più persone e scegliere la sua vittima con maggiore attenzione. Questo e altri fattori rendono le truffe online sempre più comuni. | |
| **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) Su Internet:**  A. Solo le persone che conosci possono trovarti  B. Solo i truffatori possono trovarti  C. Persone in tutto il mondo possono trovarti  **Risposta giusta: C**  **2) A cosa serve un furto di identità?**  A. Ad accedere solo alle tue coordinate bancarie  B. Ad entrare a casa tua e rubarti il laptop  C. Ad accedere al tuo account ed esegue azionidannose  **Risposta giusta: C**  **3) Quali sono le informazioni personali che consigliamo di non pubblicare su Internet?**  A. La tua misura di scarpe  B. Il tuo numero di telefono  C. Il tuo profilo Facebook  **Risposta giusta: B**  **4) Password e sicurezza. Quale delle seguenti affermazioni è vera?**  A. È meglio non salvare la password su nessun dispositivo  B. Utilizzare una password inferiore a 8 caratteri  C. Usa il tuo numero di telefono come password  **Risposta giusta: A**  **5) Perché è così importante evitare di accedere ai propri account attraverso i computer di altre persone?**  A. Perché è scortese  B. Per proteggere la tua password  C. Per proteggere la tua identità digitale  **Risposta giusta: C** |
| **Materiale correlato** |  |
| **PPT corretlato** | [**SOS creativity\_Modulo 3\_**](file:///\\10.50.100.21\interni\09TS\Utenti\umechf\IAL%20FVG_Progettazione\SOS%20Creativity\PPTs\SOS%20creativity%20Module%203%20Digital%20Identity%20and%20Online%20Reputation.pptx) **Identità digitale e reputazione online** |
| **Link di riferimento** |  |
| **Video YouTube (se presente)** |  |