Scheda corso CDI

|  |  |
| --- | --- |
| **Titolo** | Come identificare fake news online |
| **Area di formazione** | *Si prega di selezionare una o più delle seguenti opzioni:*   |  |  | | --- | --- | | Sicurezza Online | *X* | | Alfabetizzazione Culturale e Mediatica |  | | Transazioni Economiche |  | | Protezione di dati personali |  | | Identità digitale e reputazione online |  | |
| **Parole chiave (meta tag)** | sicurezza online, sicurezza online, contesto culturale, fake news, informazioni mancanti |
| **Promosso da** | Community Development Institute, CDI |
| **Lingua** | **ITALIANO** |
| **Obiettivi / finalità / risultati di apprendimento** | |
| Alla fine di questo modulo acquisirai conoscenze relative al riconoscimento delle fake news, nonché della sicurezza online con particolare riferimento al contesto culturale.  Il modulo è formato da quattro unità che forniscono informazioni relative all'argomento e suddivise in sezioni. Le unità sono supportati da esempi concreti per una migliore comprensione dei contenuti, foto esplicative e link utili per approfondire l’argomento.  Il modulo prevede una dettagliata introduzione al tema e saranno identificati  I possibili pericoli riguardo la sicurezza online come ad esempio malware, phishing, attacchi per reperire password ecc.  Gli utenti saranno in grado di:   * Comprendere il significato di sicurezza online * Fare la differenza tra fake news, disinformazione e * Conoscere strategie per migliorare la propria sicurezza online | |
| **Descrizione** | |
| Le tecnologie digitali hanno rivoluzionato ogni aspetto della nostra vita. Hanno avuto un impatto sulle catene di valore di tutte le industrie culturali e creative, non solo per quanto riguarda il processo creativo e la sua esecuzione, ma anche per quanto riguarda la realizzazione di un'opera o di un prodotto artistico e la sua promozione, distribuzione, marketing e vendita.  Questa unità di apprendimento insegnerà ai tardivi digitali a individuare potenziali truffe che potrebbero incontrare sul web mentre usano o cercano risorse culturali. Questa unità fornirà esempi specifici di truffe comuni legate alle risorse culturali, come la vendita di biglietti falsi, tentativi di phishing dopo aver ordinato online, ecc. Fornirà anche i punti chiave per identificare risorse culturali sicure online.  Nell'attuale era tecnologica, le fake news fanno parte della circolazione quotidiana e dell'informazione online. Il modulo prevede un’attenta analisi del significato di fake news e cosa gli utenti possono fare per riconoscerle ed evitarle.  Nello specifico il modulo fornisce informazioni e contenuti riguardo alla capacità degli utenti di proteggersi online. Suggerimenti e trucchi saranno forniti insieme a esempi e foto utili. | |
| **Contenuti organizzati su 3 livelli** | |
| **INTRODUZIONE**  Le tecnologie digitali hanno rivoluzionato ogni aspetto della nostra vita. Hanno avuto un impatto sulle catene del valore di tutte le industrie culturali e creative non solo per quanto riguarda il processo creativo e la sua esecuzione, ma anche per quanto riguarda la realizzazione di un'opera o di un prodotto artistico e la sua promozione, distribuzione, marketing e vendita. Mentre il passaggio al digitale continua, sempre più artisti, registi, produttori, musicisti e così via stanno distribuendo i loro prodotti in modo digitale. Alla fine di questo modulo acquisirai conoscenze e abilità di riconoscimento delle fake news e acquisirai maggiore attenzione nella sicurezza online nel contesto culturale.  In un mondo in cui un attacco hacker avviene circa ogni 39 secondi, la sicurezza online non può più essere presa alla leggera. Altrimenti, tutti i vostri dati personali potrebbero essere in pericolo.  Ma cos'è la sicurezza online, per essere precisi? Che tipo di minacce ci sono sul web e cosa si può fare per proteggersi da esse? Una minaccia alla sicurezza online si riferisce a qualsiasi possibile attacco maligno che cerca di accedere illegalmente ai dati, interrompere le operazioni digitali o danneggiare le informazioni. Ora, più che mai i contenuti culturali sono ampiamente accessibili e aperti alle minacce online, fake news con il rischio di danneggiare l'esperienza di una persona mentre gode e si informa su uno spettacolo o un evento culturale.  **Unità 1: Cosa si intende per Online Security?**  **Sezione 1.1 online Security and online safety**  L’internet security consiste in una serie di tattiche di sicurezza per proteggere le attività e le transazioni condotte online su Internet. Queste tattiche hanno lo scopo di salvaguardare gli utenti da minacce come l'hacking di sistemi informatici, indirizzi e-mail o siti web. La sicurezza di Internet è un aspetto specifico di concetti più ampi come la cybersecurity e la sicurezza informatica, essendo focalizzata sulle specifiche minacce e vulnerabilità dell'accesso online e dell'uso di Internet.  **L’Online safety** protegge le persone che usano internet dai danni attraverso la consapevolezza, l'educazione, l'informazione e la tecnologia. Sicurezza online significa essere consapevoli della natura delle possibili minacce che si possono incontrare mentre si è impegnati in attività attraverso Internet, queste potrebbero essere minacce alla sicurezza, proteggere e gestire i propri dati personali online, ed evitare contenuti dannosi o illegali.  **Sezione 1.2 Sicurezza online nei contenuti culturali**  Le tecnologie digitali hanno rivoluzionato ogni aspetto della nostra vita, e la cultura non fa eccezione. Hanno avuto un impatto sulle catene del valore di tutte le industrie culturali e creative, non solo per quanto riguarda il processo creativo e la sua esecuzione, ma anche per quanto riguarda la realizzazione di un'opera o di un prodotto artistico e la sua promozione, distribuzione, marketing e vendita. Alcuni processi di produzione sono esclusivamente digitali e la tecnologia ha un enorme potenziale per rendere la cultura accessibile a tutti, democratizzando sia il consumo che il coinvolgimento nella creazione culturale.  Allo stesso tempo, le istituzioni culturali, come i musei, gli archivi, le biblioteche e le emittenti cinematografiche, televisive e musicali hanno digitalizzato le loro collezioni nel tentativo di preservarle e renderle più ampiamente disponibili. A volte, la digitalizzazione è un passo necessario, come nel caso dei film analogici, che non possono più essere proiettati nella loro forma originale, dato che i cinema sono dotati solo di tecnologia digitale.  Un'abbondanza di contenuti culturali digitali è disponibile online gratuitamente, a pagamento o illegalmente. Una tale disponibilità e abbondanza di contenuti culturali e i vari modi di consultarli online portano nuove sfide e opportunità per disturbare la sicurezza online di una persona con vari mezzi. Quindi è importante in questa era digitale essere informati e conoscere le minacce alla vostra sicurezza online e come proteggersi quando si accede a contenuti culturali online.    **Unità 2: Le maggiori minacce alla tua sicurezza online**  **Sezione 2.1 Tipi di minacce alla sicurezza online**  Una minaccia alla sicurezza online si riferisce a qualsiasi possibile attacco maligno che cerca di accedere illegalmente ai dati, interrompere le operazioni digitali o danneggiare le informazioni.  Ci sono decine di minacce alla sicurezza online su Internet, quindi abbiamo deciso di concentrarci su quelle più pericolose e comuni.  **Malware**:  Il malware è un software maligno come spyware, ransomware, virus e worm. Il malware si attiva quando un utente clicca su un link o un allegato dannoso, che porta all'installazione di un software pericoloso che il malware, una volta attivato, può:   * Bloccare l'accesso a componenti chiave del lavoro (ransomware) * Installare ulteriori software dannosi * Ottenere segretamente informazioni trasmettendo dati dal disco rigido (spyware) * Distruggere singole parti, rendendo il sistema inutilizzabile     **Uomo nel mezzo, MITM:**  Una minaccia man-in-the-middle (MITM) si verifica quando attori malintenzionati si inseriscono in una transazione a due parti. Dopo aver interrotto la transazione, possono filtrare e rubare i dati. La minaccia MITM si realizza spesso quando un visitatore utilizza una rete Wi-Fi pubblica non protetta. Gli attori maligni si inseriscono tra il visitatore e la rete, e poi usano il malware menzionato prima per installare software e usare i dati in maniera maligna.  **Phishing:**  Gli attacchi di phishing utilizzano una comunicazione falsa, come un'e-mail, per indurre il destinatario ad aprirla ed eseguire le istruzioni all'interno, come fornire un numero di carta di credito. L'obiettivo è quello di rubare dati sensibili come la carta di credito e le informazioni di accesso o di installare malware sulla macchina della vittima.  **Phishing Attack:**  Con la password giusta, un attore malintenzionato ha accesso a una grande quantità di informazioni. L'ingegneria sociale è un tipo di attacco alle password che viene definito come "una strategia che si basa molto sull'interazione umana e spesso implica ingannare le persone a violare le pratiche di sicurezza standard".  **Unità 3: Identificare informazioni mancanti, disinformazione, disinformazione e fake news nel contesto culturale**  Ora più che mai i contenuti culturali sono ampiamente accessibili e aperti alle minacce online, la diffusione di informazioni mancanti, disinformazione, disinformazione e fake news potrebbe danneggiare l'esperienza di una persona mentre si gode e si informa su un evento o uno spazio culturale.  **Sezione 3.1 Cosa si intende per fake news, misinformazione e disinformazione?**  **Le fake news** sono informazioni create di proposito, sensazionali, cariche di emozioni, fuorvianti o totalmente inventate.  Ci sono due tipi di notizie false:  1. Storie che non sono vere. Queste sono storie interamente inventate progettate per far credere alla gente qualcosa di falso, per comprare un certo prodotto o per visitare un certo sito web.  2. Storie che hanno un po' di verità, ma non sono accurate al 100%. Di nuovo, questo può essere deliberato, per convincere i lettori di un certo punto di vista, o può essere il risultato di un errore innocente.    La misinformazione è un'informazione fuorviante, imprecisa o completamente falsa che viene diffusa senza l'esplicita intenzione di ingannare. Tuttavia, è destinata ad essere percepita dai destinatari come un'informazione seria e concreta.  Gli esempi di misinformazione abbondano. L'ascesa dei social media, che permette a quasi tutti di condividere i propri pensieri, è una delle cause principali della crescente diffusione della misinformazione. Ma fanno lo stesso anche i media tradizionali, comprese alcune delle più grandi compagnie di notizie, come Fox News o RT. Tali punti vendita lavorano spesso con la misinformazione per suscitare rabbia o paura tra i loro spettatori. Anche i canali di notizie credibili diffondono misinformazione, per esempio quando mandano in onda una notizia falsa senza verificarla adeguatamente, o quando fanno apparire ospiti nei talk show che diffondono misinformazione.  La disinformazione è un'informazione falsa diffusa con l'intenzione di ingannare le persone. La persona che diffonde la "notizia" sa che è falsa e vuole ingannare il suo pubblico. A differenza della misinformazione, la disinformazione non consiste nell'educare in buona fede, ma con l'intento malevolo di dividere e suscitare paura.  **Sezione 3.2 Come riconoscere le fake news, la disinformazione e le informazioni mancanti nel contesto culturale**  Per individuare le fake news, la misinformazione, la disinformazione e le informazioni mancanti, devi porti alcune domande come ad esempio:   * **Chi l'ha scritto?** Controlla il nome dell'autore. Il nome è disponibile o manca? La maggior parte degli autori che dedicano tempo ad un articolo ben studiato avranno probabilmente il loro nome attaccato ad esso. * **Quali sono le loro qualifiche?** Se il nome dell'autore è elencato, scopri chi è la persona e quali sono le sue credenziali. * **Controlla la sezione "Chi siamo**". Nella parte superiore o inferiore del sito web, dovrebbe esserci una sezione chiamata "Chi siamo". Questa sezione delinea lo scopo del sito web. * **L'articolo ti informa su tutti i lati dell'argomento?** Gli articoli di notizie dovrebbero fornire fatti da vari punti di vista. * **Il contenuto corrisponde al titolo dell'articolo?** Un titolo dovrebbe darti un'idea di ciò che l'intero articolo tratta, ma può anche essere usato per convincerti a credere a qualcosa prima di leggere l'articolo. * **Quando è stato pubblicato questo articolo?** Gli articoli più vecchi potrebbero non contenere fatti aggiornati e potrebbero avere link non funzionanti. * **L'articolo è stato riproposto o aggiornato?** Il contenuto riproposto o aggiornato tende ad avere un disclaimer all'inizio o alla fine dell'articolo. * Quanto è importante la data? La data ti dà un'indicazione di quando l'articolo è stato pubblicato. * **L'indirizzo web (URL) è corretto?** Digitare l'indirizzo web sbagliato ti indirizza ad una pagina web che non avevi intenzione di visitare. Potrebbe condurti ad una pagina con le suddette minacce alla sicurezza online. * **L'ho trovato sui social media?** Le piattaforme dei social media non sono organizzazioni di notizie. Sono piattaforme che permettono alle persone di creare e/o condividere contenuti. * **L'ho trovato su un blog/sito web?** I blog contengono contenuti scritti in modo informale e gestiti da un individuo o da un piccolo gruppo.     **Unità 4: Proteggersi dalle minacce alla sicurezza online**  **Sezione 4.1 Proteggersi mentre si è online**  Ecco alcune cose che puoi fare per proteggerti mentre sei online:  **1. Non usare reti WiFi non protette.**  È meglio evitare qualsiasi rete WiFi che non ti chieda una password, e usare invece il tuo piano dati mobile.  **2. Utilizzare un potente software antivirus**  Il software antivirus è la tua migliore scommessa per mantenere il tuo dispositivo al sicuro dalle infezioni da malware di cui abbiamo parlato. Non lasciare che il nome ti confonda: un programma antivirus combatte i virus, ma mira soprattutto al malware (un virus è un tipo di malware). Assicurati di tenere il programma aggiornato e di eseguire frequenti scansioni, soprattutto dopo aver scaricato nuovi file.  **3. Usa sempre una VPN online**  Una VPN (Virtual Private Network) è un servizio online che puoi usare per nascondere il tuo vero indirizzo IP e criptare le tue comunicazioni online. È uno dei modi migliori per migliorare la tua sicurezza online e nascondere le tue impronte digitali. Finché vengono utilizzati i metodi di crittografia appropriati, nessuno sarà in grado di monitorare il tuo traffico online per vedere cosa stai facendo su Internet.  **4. Evitare i tentativi di phishing**  Se ricevi e-mail o messaggi che affermano di provenire da qualcuno vicino a te, dalla tua banca o dalla polizia e ti chiedono di scaricare allegati sospetti, accedere a link abbreviati o condividere informazioni sensibili, ignorali. Mettiti invece in contatto con il presunto mittente per scoprire la verità. Prova a cercare su Google parti del messaggio che hai ricevuto tra le virgolette. Se si tratta di una truffa di phishing, è probabile che tu ottenga risultati di altre persone che parlano di aver ricevuto lo stesso messaggio.    **5. Non tenere acceso il Bluetooth**  Anche se il Bluetooth ha i suoi usi, tenerlo sempre acceso è un bel rischio. Nel 2017 è stato scoperto un nuovo metodo di hacking Bluetooth che ha colpito milioni di dispositivi permettendo agli hacker di usare la minaccia MITM Man in the Middle per ottenere le informazioni del tuo dispositivo.Tutto sommato, è meglio andare sul sicuro e spegnere il Bluetooth quando non lo stai usando per mantenere intatta la tua sicurezza online.  **6. Disattivare i servizi di localizzazione sui vostri dispositivi mobili**  I servizi di localizzazione possono essere davvero utili, ma possono anche essere molto rischiosi, c'è il fatto che alcune applicazioni potrebbero perdere la tua posizione. Se ciò accade, non significa che sarete in pericolo immediato. Tuttavia, la vostra sicurezza online sarà minacciata.  **7. Usa i blocchi degli script nei tuoi browser**  Gli script blocker sono estensioni del browser che puoi usare per assicurarti che i siti web a cui accedi non eseguano in background script e plugin non autorizzati che possono compromettere la tua sicurezza su Internet. Non dimenticare che alcuni script possono essere così pericolosi da prendere il controllo del tuo browser, mentre altri possono eseguire reindirizzamenti di phishing o annunci, o persino estrarre criptovalute utilizzando la tua CPU.  **8. Mantenere il sistema operativo aggiornato**  Non installare gli aggiornamenti più recenti sul tuo sistema operativo può danneggiare seriamente la tua sicurezza online. Perché i malintenzionati possono usare potenziali vulnerabilità a loro vantaggio - vulnerabilità che potrebbero essere state risolte con l'ultimo aggiornamento.  **9. Considera l'uso di app di messaggistica e di e-mail criptate**  Se vuoi davvero assicurarti che le tue comunicazioni online siano sicure, puoi provare a usare le diverse app di messaggistica. Queste dispongono di una crittografia davvero potente.  Per quanto riguarda le e-mail, vale lo stesso, cerca online le diverse app e il tipo di sicurezza che offrono.  **10. Usa password forti**  Avere password potenti per i tuoi account è estremamente importante, ma trovarne una davvero buona è più facile a dirsi che a farsi.  Se hai bisogno di aiuto, ecco le idee principali:  1. Usa spazi se possibile.  2. Usare solo password lunghe. Non limitatevi a una sola parola.  3. Non usare parole del dizionario come password.  4. Usa sia lettere maiuscole che minuscole, e mischiale a caso.  5. Usa simboli (come $, %, o \*)  6. Includi numeri  7. Prova a rendere la tua password una frase intera.  8. Inverti alcune parole che usi nella password (invece di "sedia" usa "resadi").  9. Inoltre, cerca di non usare la stessa password per tutti i tuoi account. È meglio usare password diverse, o almeno variazioni della tua password principale.  **4.2 Consigli per la sicurezza online in un contesto culturale**  Grazie a internet, ci sono diversi modi per i consumatori di ottenere biglietti per un prossimo evento. Il lato negativo è che ci sono anche molte trappole che i consumatori devono evitare. Cliccare sul link sbagliato o fidarsi del sito web sbagliato potrebbe portare a un biglietto falso e alla perdita di fondi.  Ecco alcuni consigli su come essere sicuri online, con un esempio specifico di acquisto di biglietti online per un evento culturale:  - **Acquista direttamente sul luogo dell'evento, quando possibile**. Molti venditori ufficiali di biglietti offrono ora anche opzioni di vendita secondaria. Non cliccare da e-mail o annunci online; un trucco comune per la truffa dei biglietti è quello di creare un indirizzo web che sia simile a quello di una società nota.  - **Considera la tua fonte**. Conosci la differenza tra un broker di biglietti professionale (un rivenditore legittimo e accreditato), un bagarino (un venditore di biglietti non regolamentato e senza licenza) e un truffatore che vende biglietti fasulli.  - **Studia la politica di rimborso.** Dovresti acquistare biglietti solo da un rivenditore di biglietti che fornisce dettagli chiari sui termini della transazione. I venditori dovrebbero rivelare all'acquirente, prima dell'acquisto, la posizione dei posti rappresentati dai biglietti, a voce o con riferimento ad una tabella dei posti; e, se i biglietti non sono disponibili per un accesso immediato all'acquirente, rivelare quando i biglietti saranno spediti o disponibili per il ritiro.  - **Usa metodi di pagamento che hanno una protezione**. Usa sempre una carta di credito, in modo da avere qualche ricorso se i biglietti non sono come promesso. Le carte di debito, il bonifico bancario o le transazioni in contanti sono rischiose; se i biglietti sono fraudolenti, molto probabilmente non sarai in grado di recuperare i tuoi soldi.    - **Diffida delle pubblicità**. Quando cerchi sul web i biglietti online, spesso appaiono annunci di biglietti economici. Usa il buon senso; alcuni di questi annunci saranno truffe di biglietti, specialmente se i prezzi sono bassi.  - **Se non sei sicuro, verifica i biglietti**. Fai una visita all'arena dove si terrà l'evento. Presenta il tuo biglietto al servizio clienti e loro potranno verificare se il tuo biglietto è legittimo e mostrarti come capire se un biglietto è falso.  **CONCLUSIONE**  La sicurezza online rappresentano le regole che segui, le azioni che intraprendi e i processi che avvengono per assicurarti di essere al sicuro su Internet. Con le minacce alla sicurezza (malware, truffe, phishing, hacking, ecc.) che diventano sempre più comuni al giorno d'oggi, la sicurezza online è diventata più importante che mai.  Questo accade mentre usufruisci di risorse culturali.  Di solito, il modo migliore per assicurarsi di essere al sicuro online è quello di utilizzare un forte programma antivirus, una VPN affidabile, password potenti, script blocker ecc.  Le fake news si riferiscono alle falsità deliberate, o alle storie che contengono un po' di verità ma che non sono completamente accurate, per caso o per progetto.  Alcune persone sostengono anche che le storie veritiere sono "fake news", solo perché non sono d'accordo con loro. Questo può portare a ignorare pericolosamente consigli vitali.  Le notizie false possono avere un impatto negativo sugli aspetti sociali e culturali della società, quindi è fondamentale sapere come separare le notizie vere da quelle false e riconoscere quando mancano delle informazioni, la disinformazione o la disinformazione. È possibile farlo seguendo questi sei passi:  1. Sviluppare una mentalità critica.  2. Controllare la fonte.  3. Vedere chi altro sta riportando la storia.  4. Esaminare le prove.  5. Non prendere le immagini al valore nominale.  6. Controllare che "suoni bene". | |
| **Lista dei contenuti** | |
| * I contenuti culturali sono spesso presi di mira da mail intenzionati e piene di minacce online, di diffusione di disinformazione, e fake news che possono danneggiare l'esperienza di una persona mentre gode e si informa su uno spettacolo o evento culturale. * La sicurezza su internet consiste in una serie di tattiche di sicurezza per proteggere le attività e le transazioni condotte online su internet. * Una minaccia alla sicurezza online si riferisce a qualsiasi possibile attacco maligno che cerca di accedere illegalmente ai dati, interrompere le operazioni digitali e/o danneggiare le informazioni. * La sicurezza online consiste nell'essere consapevoli della natura delle possibili minacce che si possono incontrare mentre si svolge un'attività su internet, queste potrebbero essere minacce alla sicurezza, ai propri dati personali online. La sicurezza online protegge le persone che compiono azioni online attraverso la consapevolezza, l'educazione, l'informazione e la tecnologia. * Ci sono decine di minacce alla sicurezza online su Internet, questo modulo si concentra su quelle più pericolose e comuni, come: Malware; Man in the Middle MITM; Phishing; Attacchi con password, ecc. * Le fake news possono avere un impatto negativo sugli aspetti sociali e culturali della società, quindi è fondamentale sapere come separare le notizie vere da quelle false e riconoscere le informazioni dalla disinformazione. | |
| **5 vocaboli chiave** | |
| **1)Sicurezza Informatica**  Consiste nel difendere computer, server, dispositivi mobili, sistemi elettronici, reti e dati dagli attacchi dannosi. È anche conosciuta come sicurezza informatica o sicurezza delle informazioni elettroniche.  **2) Sicurezza online**  La sicurezza Online, è la pratica volta a proteggere le informazioni digitali, i dispositivi e le risorse personali. compresi le informazioni personali, gli account, i file, le fotografie, e persino il denaro.  **3) Contesto culturale**  Il contesto culturale è legato alla società in cui gli individui sono cresciuti e a come la cultura influenza il comportamento. Incorpora valori che vengono appresi e atteggiamenti che sono condivisi tra gruppi di persone. Include credenze, significati, costumi, idee, linguaggio, norme.  Si riferisce al significato simbolico, alla dimensione artistica e ai valori culturali che hanno origine o esprimono le identità culturali.  **4) Fake news**  Notizie false, spesso di natura sensazionale, create per essere ampiamente condivise o distribuite allo scopo di generare entrate, o promuovere o screditare un personaggio pubblico, un movimento politico, un'azienda, ecc.  **5) Informazioni mancanti**  è un'informazione incompleta o imprecisa che mira a distrarre da un'informazione accurata, causare confusione o cambiare il contesto di una frase, azione, attività, ecc. | |
| **Bibliografia e altre referenze** | |
| * <https://www.mindtools.com/pages/article/fake-news.htm> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.researchgate.net/publication/336951206_Fake_news_Acceptance_by_demographics_and_culture_on_social_media> * <https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf> * <https://www.nature.com/articles/s41586-021-03344-2> * <https://www.kdd.org/exploration_files/8._CR.10.Misinformation_in_social_media_-_Final.pdf> * <https://academicguides.waldenu.edu/library/fakenews/examples> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690570> * <https://en.wikipedia.org/wiki/Fake_news> * <https://call-for-papers.sas.upenn.edu/cfp/2021/06/28/if-its-on-the-internet-it-must-be-true-the-socio-cultural-impact-of-fake-news> * <https://www.frontiersin.org/research-topics/23019/the-psychology-of-fake-news-on-social-media-who-falls-for-it-who-shares-it-why-and-can-we-help-users>   <https://researchguides.austincc.edu/c.php?g=612891&p=4258046> | |
| **Cinque domande di autovalutazione a scelta multipla** | 1) Ricevi una e-mail che ti chiede di accedere al loro link con una password per qualche motivo di sicurezza. Cosa faresti?  A. Niente, ignoro il messaggio  B. Farò come richiesto, visto che si tratta di una ragione di sicurezza  C. Contatterò un esperto Informatico per avere maggiori informazioni  **Risposta corretta: A**  2) Sei su un sito che vende biglietti gratuiti per un evento culturale vicino a te. Sono gratuiti, e chiedono solo alcune delle tue informazioni personali. Cosa faresti?  A. Compro i biglietti e inserisco le mie informazioni personali  B. Controllerò il sito per vedere se è affidabile  C. Condivido il sito in modo che anche altri possano ottenere i biglietti  **Risposta corretta: B**  3) Hai visitato un tour virtuale di un noto luogo culturale. Hai notato che in uno dei siti mancano delle informazioni. Cosa fai?  A. Riempio io stesso il lotto vuoto  B. Informo la guida virtuale per questo possibile errore  C. nulla  **Correct answer: B**  5) Tieni al sicuro le tue informazioni personali quando usi i social network?  A. Sì  B. No  C. Non saprei  **Risposta corretta: Opzionale, tutte le risposte sono corrette** |
| **Materiale correlato** |  |
| **PPT correlato** |  |
| **Link di riferimento** |  |
| **Video YouTube (se presente)** | <https://youtu.be/vPAW5j_L4-c>  <https://www.youtube.com/watch?v=0yL-k5nB65o> |