Scheda di formazione

|  |  |  |
| --- | --- | --- |
| **Titolo** | | Sicurezza informatica in ufficio (di casa) |
| **Parole chiave (meta tag)** | | cybersecurity, sicurezza, malware, phishing, informazioni sensibili |
| **Fornito da** | | Soluzioni Web per Internet |
| **Lingua** | | Inglese |
| **Area di formazione (X se applicabile)** | | |
|  | Innovazione e servitizzazione | |
| **X** | Trasformazione digitale | |
|  | Localizzazione | |
|  | Sostenibilità | |
| **ESCO competenze e abilità** | | |
| * Capacità e competenze trasversali   + Competenze sociali ed emotive   + Pensiero critico   + Pensiero analitico   + Risoluzione di problemi   + Autogestione   + Gestione aziendale   + Adattabilità   + Resilienza   + Creatività   + Networking   + Iniziativa   + Flessibilità   + Apertura   + Comprensione della complessità   + Cooperazione   + Empatia   + Innovazione   + Leadership * Competenze | | |

|  |
| --- |
| * Competenze tecnologiche * Marketing di prodotto * Marketing digitale * Competenze digitali * Comunicazione * Cooperazione * Intelligenza emotiva * Conoscenza   + Gestione aziendale   + Apprendimento e formazione online   + Pubblicità   + Cloud computing   + Grandi dati   + Commercio elettronico   + Intelligenza artificiale   + IoT   + Alfabetizzazione digitale   + Cybersecurity   + Estrazione e analisi dei dati   + Sostenibilità   + Benessere   + Cambiamento climatico   + Gestione dei social media |
| **Teaser** |
| "Sapevate che l'85% delle PMI europee considera la cybersecurity una preoccupazione fondamentale per la propria attività?" |
| **Obiettivi / finalità / risultati di apprendimento** |
| In questo modulo imparerete cos'è la cybersecurity, familiarizzerete con la terminologia più comunemente usata in questo campo e scoprirete gli attacchi informatici più comuni quando si lavora da casa e dall'ufficio. In questo modo, sarete in grado di prevenire i principali rischi informatici e di navigare in sicurezza, non solo quando lavorate da casa ma anche quando svolgete le attività quotidiane su Internet, aumentando così le vostre competenze e conoscenze sulla sicurezza informatica. |
| **Descrizione** |
| La maggior parte delle PMI europee considera la cybersecurity una preoccupazione aziendale fondamentale. Tuttavia, in un contesto post-pandemico, non tutte le aziende hanno implementato nuove misure di sicurezza per combattere i rischi derivanti dal lavoro a distanza, a causa della mancanza di consapevolezza e di competenze in materia di cybersecurity. Questo modulo consentirà al personale e agli imprenditori delle PMI di migliorare le proprie competenze e conoscenze in materia di cybersecurity, al fine di aumentare le proprie competenze digitali e la propria resilienza informatica. |
| **Lista di controllo dei vantaggi per gli imprenditori** |
| * L'implementazione di strategie di cybersecurity nelle PMI riduce il rischio di perdite e fughe di informazioni, mantenendo l'integrità dei dati. * Mantenendo la riservatezza delle informazioni sui clienti, la reputazione e l'immagine aziendale dell'azienda vengono rafforzate anche agli occhi del pubblico. |

|  |
| --- |
| ✓ La cybersecurity aumenta la resilienza e la capacità di recupero delle aziende, con backup che consentono di riprendere l'attività dopo un incidente imprevisto.  ✓ Riducendo la perdita di informazioni dovuta ad attacchi informatici o a problemi interni, si ottiene anche un aumento della produttività.  ✓ La sicurezza informatica è uno strumento essenziale per i datori di lavoro e i dipendenti, non solo nella vita lavorativa ma anche in quella personale, grazie alla sensibilizzazione e alla prevenzione dei rischi informatici (ad esempio, negli acquisti online). |
| **Contenuti disposti su 3 livelli** |
| **Modulo: Cybersicurezza nell'ufficio (domestico)**  **Unità 1: Fondamenti di cybersicurezza**  **Sezione 1.1: Cos'è la cybersecurity?**  Il termine "**cybersecurity**" è nato negli anni '70 per la necessità delle aziende di **proteggere i propri sistemi informatici** da attacchi malevoli che potrebbero comprometterne il corretto funzionamento attraverso l'uso improprio delle informazioni.  La cybersecurity comprende l'applicazione di strumenti, tecnologie, politiche, controlli e procedure per proteggere o recuperare reti, sistemi, dispositivi e applicazioni da **attacchi informatici** volti ad accedere, distruggere o alterare informazioni sensibili, interrompere i flussi di lavoro o estorcere denaro a organizzazioni o individui.  Secondo un rapporto del 2021 dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA), su un totale di 249 PMI europee intervistate, **l'85% considera la cybersecurity una preoccupazione fondamentale per la propria attività**. In un contesto post-pandemia, il 45% delle PMI ha implementato nuove tecnologie in risposta alla pandemia, ma il 90% non ha incluso nuove misure di sicurezza.  Lo stesso rapporto, che fornisce informazioni preziose sulla sicurezza informatica delle PMI europee, **mostra i principali incidenti di sicurezza informatica** subiti dalle PMI europee in base alla loro origine, come illustrato nel grafico. |





|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Gli attacchi più comuni alle PMI europee** | | | | | |  |
| Dispositivo compromesso/rubato  Ingegneria sociale  Negazione del servizio  Insider malintenzionati Malware generale Attacchi basati sul web  Phishing |  |  |  |  |  |
| 0% 10% 20% 30% 40% 50% | | | | | |
| Fonte: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>(elaborazione propria)  **Sezione 1.2: Definizioni principali**  Sicurezza generale:   * **Backup**: una copia di file e programmi che viene memorizzata su altri dispositivi o altri supporti, al fine di recuperare le informazioni in caso di guasto, perdita o furto. * **Informazioni sensibili**: informazioni contenenti dati privati o confidenziali, come dati personali o bancari. * **Software**: il software è un programma per computer progettato per eseguire compiti specifici, ad esempio un browser, un gioco, ecc. È l'opposto dell'"hardware", che è costituito dai componenti fisici del dispositivo, come la scheda madre o il processore. * **Crittografia**: è un processo che converte un documento o un file in informazioni illeggibili per chi non possiede la chiave per decifrarlo. Serve a proteggere le informazioni da persone che non dovrebbero avervi accesso. * **HTTP / HTTPS**: uno dei protocolli più utilizzati per la navigazione in Internet. HTTPS (HyperText Transfer Protocol Secure) è la versione sicura e garantisce che le informazioni trasmesse tra il dispositivo e il sito web siano criptate e protette. * **Firewall**: quando si naviga in rete e si accede a un sito web, comunica con il computer per stabilire la connessione. Il firewall analizza questo tipo di connessione per impedire l'accesso a quelle che potrebbero costituire un rischio.   Threats:   * **Ingegneria sociale**: l'ingegneria sociale non richiede elevate competenze informatiche, in quanto comporta la manipolazione delle persone attraverso tecniche psicologiche e abilità sociali, ed è spesso utilizzata per ottenere informazioni sensibili, come password o dati bancari. Le tecniche di phishing si basano sull'ingegneria sociale. | | | | | | | |

|  |
| --- |
| * **Phishing**: la tecnica di fingere di essere un'altra persona o un'entità tramite e-mail, inducendo l'utente a compiere un'azione su una pagina fraudolenta al fine di ottenere password o scaricare un file infetto. * **Smishing**: SMS + phishing. Simile al phishing, questa tecnica utilizza gli SMS per lo stesso scopo. * **Vishing**: voce + phishing. In questo caso, l'aggressore finge di essere un'altra persona durante una telefonata, spesso spacciandosi per il supporto tecnico del dispositivo o della compagnia telefonica. * **Attacchi basati sul Web**: questi attacchi complessi agiscono quando si utilizza Internet, sfruttando il software dannoso per infettare i dispositivi che non dispongono della sicurezza necessaria o sono obsoleti.   Tipi di malware:   * **Malware**: il malware è un software dannoso che può assumere varie forme (come codice eseguibile, script, ecc.) e può eseguire azioni quali la crittografia o l'eliminazione di dati sensibili, l'alterazione delle funzioni di base del dispositivo, lo spionaggio delle attività dell'utente e altro ancora. Antimalware è un software che ha la funzione di rilevare, proteggere e rimuovere questo tipo di software dannoso. * **Virus informatico**: questo tipo di malware mira ad alterare il funzionamento del dispositivo e richiede l'interazione dell'utente per diffondersi ad altri file e sistemi. * **Worm informatico**: è in grado di replicarsi e spostarsi da un dispositivo infetto ad altri attraverso la rete. Spesso proviene da unità USB infette, allegati di posta elettronica o persino siti web. * **Trojan**: questo tipo di malware entra nel sistema come un file o un software innocuo ed esegue azioni indesiderate in background, come l'eliminazione di file o il download di altro malware. * **Spyware**: come suggerisce il nome, questo tipo di malware spia il dispositivo infetto, raccogliendo informazioni sulle attività dell'utente. Di solito proviene da siti web di spam o di download fraudolenti. * **Adware**: malware che tiene traccia del browser e della cronologia dei download dell'utente per visualizzare annunci o banner indesiderati su cui l'utente deve cliccare. Di solito infettano i dispositivi tramite siti web infetti o siti web di download fraudolenti. * **Ransomware**: un pericoloso tipo di malware che cripta i file sul disco rigido del dispositivo e limita l'accesso all'utente, chiedendo un riscatto, solitamente in criptovalute, in cambio della decriptazione dei file. Un caso noto è quello di [**WannaCry**](https://www.europol.europa.eu/wannacry-ransomware).   **Unità 2: Cybersecurity...**  **Sezione 2.1: ...sul posto di lavoro**  **La cybersecurity è una responsabilità di tutti in un'azienda**, sia del management che dei dipendenti, quindi deve anche essere parte della cultura lavorativa dell'azienda.  Sia in ufficio che a casa, è assolutamente necessario rispettare una serie di **misure di base** **nell'ambito di un piano di cybersecurity** per il corretto funzionamento dell'azienda.  Di seguito è riportato un piano di **cybersecurity di base** da seguire per mantenere l'integrità delle informazioni aziendali: |

|  |
| --- |
| 1. **Informare sulle politiche di cybersecurity dell'azienda**. Ogni azienda ha esigenze uniche, quindi le politiche di cybersecurity devono essere sviluppate e seguite da tutti i dipendenti e i manager per creare una cultura della cybersecurity. 2. **Aggiornare il software dei dispositivi**. Mantenere aggiornate tutte le applicazioni e i sistemi operativi previene le vulnerabilità. 3. **Impostare un firewall**. Un firewall fornisce una protezione aggiuntiva durante la navigazione in Internet. 4. **Eseguire regolarmente dei backup**. In caso di perdita di dati, i backup aiutano a ripristinare rapidamente la normalità. 5. **Proteggere le reti wifi**. Le reti wifi utilizzate nelle attività quotidiane devono essere configurate correttamente per essere sufficientemente sicure nei confronti di terzi. 6. **Installare un software anti-malware**. Per proteggersi da eventuali attacchi. 7. **Sviluppare un piano d'azione per i dispositivi mobili**. La sicurezza informatica non riguarda solo i computer, ma anche i dispositivi mobili come smartphone e tablet, che devono essere protetti. 8. **Implementare procedure per la protezione delle informazioni**. È necessario stabilire le procedure da seguire in caso di incidenti di cybersecurity. 9. **Utilizzare password forti**. Devono combinare numeri, lettere e caratteri speciali. Un modo per verificare se le password sono sicure è il sito web <https://password.kaspersky.com/>. 10. **Limitare le autorizzazioni per l'installazione di software**. I dipendenti devono avere un accesso limitato quando installano un nuovo software, per evitare l'installazione di applicazioni fraudolente che potrebbero infettare i dispositivi di rete.   **Sezione 2.2: ...nel lavoro da remoto**  **Quando si lavora da remoto, la cybersecurity è ancora più importante**, poiché quando si lavora da casa non c'è lo stesso controllo sulle procedure e sulle politiche di cybersecurity dell'azienda, le reti sono meno sicure, possono esserci errori di configurazione, mancanza di formazione, ecc.  Per questo motivo è necessario prendere in considerazione nuove misure per garantire il raggiungimento dei seguenti **obiettivi di cybersecurity per l'accesso remoto** alle informazioni:   * **Disponibilità**. Gli utenti autorizzati devono poter accedere alle informazioni quando necessario. * **Riservatezza**. Deve essere garantito che solo gli utenti autorizzati possano accedere alle informazioni. * **Autenticità**. Si deve garantire che gli utenti autorizzati (che hanno accesso alle informazioni) siano quelli che dichiarano di essere. * **Tracciabilità**. Deve essere possibile rintracciare gli accessi impropri o non autorizzati alle informazioni. * **Integrità**. Deve essere garantita l'accuratezza e la completezza delle informazioni e dei relativi metodi di elaborazione. |

|  |
| --- |
| Oltre al piano di cybersecurity già citato, si raccomanda l'uso di una **VPN (Virtual Private Network**). Questa tecnologia di rete consente una connessione sicura tra la rete locale e Internet, in modo da **garantire l'integrità e la riservatezza delle informazioni**.  Inoltre, le **applicazioni di accesso al desktop remoto** consentono ai telelavoratori di controllare a distanza i computer che si trovano fisicamente in ufficio, come ad esempio lo strumento TeamViewer.  **Anche le soluzioni cloud e gli strumenti** di collaborazione sono strumenti importanti per la cybersecurity nel lavoro a distanza, **consentendo l'accesso alle informazioni in modo rapido e coordinato.**  Alcuni esempi di strumenti per il lavoro a distanza sono:  **VPN:**   * **hide.me**. Questo servizio VPN permette di navigare in modo privato, senza restrizioni geografiche. Conta più di 2000 server e 75 località. <https://hide.me/> * **PrivadoVPN**. Con sede in Svizzera, la sua versione gratuita permette di proteggere fino a 10 GB di dati al mese. <https://privadovpn.com/>   **Desktop remoto:**   * **AnyDesk**. Si tratta di un altro software di desktop remoto disponibile gratuitamente per uso personale. Questo tipo di strumento consente di accedere alle informazioni da qualsiasi luogo, migliorando la comunicazione interna. <https://anydesk.com/> * **TeamViewer.** Questo strumento si concentra maggiormente sull'accesso remoto alle informazioni, in quanto consente di accedere a qualsiasi dispositivo da qualsiasi luogo. Consente la condivisione sicura dei file e l'accesso ad altri dispositivi ed è gratuito per uso personale.. <https://www.teamviewer.com/>   **Soluzioni cloud:**   * **Dropbox** Il piano gratuito offre 2 GB di spazio di archiviazione, mentre i piani a pagamento arrivano fino a 3 TB di spazio di archiviazione. <https://www.dropbox.com/> * **MEGA**. Questa piattaforma include 20 GB gratuiti e ha piani a pagamento per i privati fino a 16 TB e per le aziende fino a 10 PB, il che la rende una delle soluzioni con la maggiore capacità. <https://mega.io/>   **Strumenti di collaborazione:**   * **Slack**. Questa piattaforma di messaggistica istantanea consente l'integrazione con altri strumenti e semplifica la comunicazione di gruppo. La versione gratuita consente di accedere alla cronologia degli ultimi 10.000 messaggi del team, di effettuare videochiamate con i colleghi e di integrarsi con 10 applicazioni. <https://slack.com/> * **Trello**. Questo strumento funziona con il sistema di schede Kanban e consente di includere note, file, scadenze e altri elementi. È facile da gestire trascinando le schede ed è disponibile in diverse lingue. Questo strumento è gratuito fino a 10 schede per team. <https://trello.com/>   **Unità 3: Raccomandazioni per imprenditori e personale** |

|  |
| --- |
| **Unità 3: Raccomandazioni per imprenditori e personale**   * Assicuratevi che la vostra azienda disponga di un piano di **cybersecurity adeguato** alle esigenze e alle potenziali vulnerabilità della vostra attività. * Stabilire politiche e procedure per la **gestione sicura delle informazioni**, ad esempio, nessun dispositivo personale, distruzione sicura dei documenti. * **Formate i vostri dipendenti sulla sicurezza informatica** in modo che possano rispettare le politiche e le procedure. * **Migliorate le vostre competenze digitali e di cybersicurezza**; ricordate che gestite informazioni molto sensibili. * Anche le raccomandazioni per il **personale sono condivise**!    **Sezione 3.2: Raccomandazioni per il personale**   * La sicurezza informatica inizia con la **sicurezza fisica delle informazioni**: mantieni il tuo desktop libero da informazioni riservate, post-it con password, e-mail, ecc. * Non collegare **dispositivi USB** provenienti da persone non fidate, perché potrebbero infettare il computer. * **Crittografare le informazioni sensibili prima di inviarle**, ad esempio attraverso un file compresso protetto da password. * Ricordatevi di **svuotare regolarmente il cestino del compute**r. * Eseguite regolarmente dei **backup**. * Al di fuori dell'azienda, **tenete sotto controllo i vostri dispositivi mobili**. * Se possibile, **evitate di collegarvi a reti wifi aperte** con i dispositivi di lavoro. Se è necessario, utilizzate una VPN per la sicurezza. * **Bloccate il computer** quando siete lontani dalla scrivania * **Utilizzare password sicure**. Potete verificare la sicurezza delle vostre password su siti web dedicati al controllo delle password, come ad esempio <https://password.kaspersky.com/>. * **Utilizzate sempre le stesse password**, perché sareste più vulnerabili in caso di fuga di notizie. * **Non scaricate allegati da mittenti sconosciuti**, diffidate dei **messaggi sospetti e segnalate eventuali incidenti** ai vostri superiori e * Segnalate qualsiasi incidente ai vostri supervisori. |
| **Contents in bullet points** |
| * La cybersecurity è nata dall'esigenza delle aziende di proteggere i propri sistemi informatici da attacchi malevoli. * Gli incidenti di cybersecurity più comuni subiti dalle PMI europee sono legati al phishing. * La cybersecurity è una responsabilità di tutti all'interno di un'azienda ed è necessario avere un piano di cybersecurity che sia seguito correttamente da manager, direttori e dipendenti. * Nel lavoro a distanza, la cybersecurity è integrata dall'uso di strumenti TIC che consentono di raggiungere i cinque obiettivi della cybersecurity nell'accesso alle informazioni. * Il datore di lavoro deve assicurarsi che esista un piano di cybersecurity e che i dipendenti abbiano le competenze necessarie per rispettarlo. * I lavoratori devono impegnarsi a gestire in modo sicuro le informazioni nel corso del loro lavoro. |

|  |
| --- |
| **5 voci di glossario** |
| **Cybersecurity**. L'applicazione di strumenti, tecnologie, politiche, controlli e procedure per la protezione o il ripristino di reti, sistemi, dispositivi e applicazioni da attacchi informatici volti ad accedere, distruggere o alterare informazioni sensibili, interrompere i flussi di lavoro o estorcere denaro a organizzazioni o individui.  **Phishing.** Tecnica che consiste nel fingere di essere un'altra persona o un'entità tramite e-mail, inducendo l'utente a compiere un'azione su una pagina fraudolenta per ottenere password o scaricare un file infetto. Simili sono il vishing (voice + phishing) o lo smishing (SMS + phishing).  **Malware.** Software dannoso che può presentarsi in diverse forme (come codice eseguibile, script, ecc.) e può eseguire azioni quali la crittografia o l'eliminazione di dati sensibili, l'alterazione delle funzioni di base del dispositivo, lo spionaggio dell'attività dell'utente, tra le altre cose. Anche virus, worm, adware, trojan, spyware e ransomware sono malware.  **Backup.** Copia di file e programmi memorizzati su altri dispositivi o altri supporti, al fine di recuperare le informazioni in caso di guasto, perdita o furto.  **Informazioni sensibili**. Informazioni contenenti dati privati o riservati, come ad esempio dati personali o bancari. |
| **Bibliografia e ulteriori riferimenti** |
| [https://www.redseguridad.com/especialidades-tic/como-definir-la-ciberseguridad-en-un-](https://www.redseguridad.com/especialidades-tic/como-definir-la-ciberseguridad-en-un-entorno-laboral-hibrido_20210928.html) [entorno-laboral-hibrido\_20210928.html](https://www.redseguridad.com/especialidades-tic/como-definir-la-ciberseguridad-en-un-entorno-laboral-hibrido_20210928.html)  [https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-web-based-](https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-web-based-attacks-ebook-en-es.pdf) [attacks-ebook-en-es.pdf](https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-web-based-attacks-ebook-en-es.pdf)  <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes> <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>  [https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad\_en\_el\_teletrabaj](https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf) [o.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf)  <https://www.microfocus.com/en-us/what-is/cyber-security>  [https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-](https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-debes-conocer) [debes-conocer](https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-debes-conocer)  <https://es.linkedin.com/pulse/recomendaciones-de-ciberseguridad-en-el-puesto-trabajo-pizarro>  [https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-](https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html) [evitar-ataques-de-este-tipo\_20210410.html](https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html)  <https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/> |

|  |  |
| --- | --- |
| <https://uniserveit.com/blog/10-step-cybersecurity-plan-for-your-small-business>  [https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-](https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes) [europes-smes](https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes)  <https://www.europol.europa.eu/wannacry-ransomware> | |
| **Cinque domande di autovalutazione a scelta multipla**  Al termine del meccanismo di convalida, gli utenti potranno generare un certificato di partecipazione e un certificato di completamento personalizzati. | **Domanda 1. Cosa si intende per "cybersecurity"?**  Opzione a: Strumenti per proteggere i dispositivi dagli attacchi di malware.  Opzione b: Procedure progettate per proteggere le informazioni sensibili da attacchi dannosi.  Opzione c: La protezione dei sistemi informatici aziendali.  Opzione d: Tutte le risposte sono corrette.  **Opzione corretta: d**  **Domanda 2. Cosa si dovrebbe fare per prevenire il phishing?**  Opzione a: Diffidare delle e-mail non richieste per cambiare la password.  Opzione b: Cliccare sui link contenuti nelle e-mail.  Opzione c: Scaricare gli allegati delle e-mail di spam.  Opzione d: Rispondere a telefonate da numeri sconosciuti.  **Opzione corretta: a**  **Domanda 3. Qual è l'attacco più comune alle PMI europee?**  Opzione a: Denial of service.  Opzione b: Ransomware.  Opzione c: Phishing.  Opzione d: Nessuna è corretta**.**  **Opzione corretta: c**  **Domanda 4. Quali dei seguenti sono obiettivi di cybersecurity per l'accesso remoto alle informazioni?**  Opzione a: Disponibilità, riservatezza.  Opzione b: tracciabilità, pubblicità.  Opzione c: Riservatezza, corruzione.  Opzione d: Integrità, misurabilità.  **Opzione corretta: a**  **Domanda 5. Cosa fareste con una chiavetta USB trovata sulla scrivania di un ufficio?**  Opzione a: La collegherei al mio computer per vedere cosa contiene e restituirla al proprietario.  Opzione b: cercherei di trovare il proprietario senza collegarla a nessun computer.  Opzione c: Denunciarlo alla polizia.  Opzione d: Buttarlo via.  **Opzione corretta: b** |

|  |  |
| --- | --- |
|  |  |
| **Materiale correlato** | RESTART\_PR3\_COU\_03\_IWS\_Cybersecurity\_EN.pptx |
| **Link di riferimento** | - |
| **Video in formato YouTube**  **formato (se presente)** | <https://www.youtube.com/watch?v=PSrnvEEDpuY> |