**Scheda di formazione**

|  |  |  |
| --- | --- | --- |
| **Titolo** | Cybersecurity and strumenti digitali per le PMI. Essere preparati per prevenire e risolvere gli attacchi Cyber | |
| **Parole chiave (meta tag)** | Cybersecurity, Sicurezza, Cybercrime, Cyber-attack, | |
| **Fornito da** | ITSFA | |
| **Lingua** | Inglese | |
| **Area** | Comunicazione digitale e online |  |
| Impegno di squadra e di persone da remoto |  |
| Equilibrio lavoro-vita |  |
| Benessere personale |  |
| “Come aumentare la produttività del tuo team da remoto?” |  |
| Remote project management |  |
| Agile Management by Objectives |  |
| Autoefficacia “Smart” |  |
| Leadership e Motivazione ai tempi dello Smart Work |  |
| Telelavoro: una selezione di strumenti digitali per gestire il tuo business | **X** |
| **Obiettivi / fini / risultati dell’apprendimento** | | |
| In questo corso acquisirai una conoscenza di base della Cybersecurity, a livello aziendale e anche a livello di utente/dipendente. Imparerete le definizioni dei principali rischi informatici che possono mettere in pericolo la vostra sicurezza e la vostra sicurezza aziendale; e imparerete i principali strumenti per prevenire i crimini informatici con una guida di base di cybersecurity, che vi aiuterà a sapere quali sono le misure di base da seguire per proteggere la vostra PMI da queste minacce, e quindi per essere in grado di lavorare in remoto in modo più sicuro. | | |
| **Descrizione** | | |
| A causa della pandemia Covid-19, le PMI, per le loro caratteristiche intrinseche, sono diventate il bersaglio dei criminali informatici. I nuovi modi di lavorare portati dalla pandemia, il telelavoro, il telelavoro; in altre parole, il cosiddetto Smart working, hanno reso necessario per le PMI acquisire conoscenze che le aiutino a sopravvivere saltando sul carro della digitalizzazione e a non rimanere indietro. Uno dei bisogni formativi fondamentali guidati da questa situazione è la cybersecurity.  Con questo corso, le PMI saranno in grado di ottenere una conoscenza di base della cybersecurity, e quindi avere gli strumenti per prevenire i rischi informatici che mettono in pericolo la sopravvivenza delle loro imprese, in un mondo che si muove senza controllo verso la digitalizzazione. | | |
| **Contenuti in 3 livelli** | | |
| 2. Cybersecurity and strumenti digitali per le PMI. Essere preparati per prevenire e risolvere gli attacchi Cyber  2.1 Sicurezza a livello business  -Cos’è la Cyber Security?  A causa della digitalizzazione, la Cybersecurity per le PMI è una questione cruciale oggi. I cyber-attacchi prendono sempre più di mira le piccole e medie imprese che non sono protette come le grandi aziende.  La Cybersecurity è un insieme di pratiche per difendere i sistemi informatici e il software dal crimine informatico. Il crimine informatico è qualsiasi attività criminale che si svolge nel mondo digitale, coinvolgendo un computer, un dispositivo in rete o una rete, e destinato a raggiungere un certo scopo o beneficio, che può essere di diversi tipi. La cybersecurity copre molte aree: sicurezza della rete, sicurezza delle app, sicurezza delle informazioni, sicurezza degli utenti, ecc. Vediamo alcuni concetti per considerare la cybersecurity a livello aziendale, per finire alla fine del corso con una guida di base della Cybersecurity.  -Ransomware  Il ransomware è un tipo di software maligno che cripta le informazioni su diversi dispositivi. Utilizzando questo metodo, i criminali informatici estorcono denaro alle loro vittime, chiedendo un riscatto in cambio di riottenere l'accesso ai loro dati.  Ransomware, è un tipo di malware che impedisce agli utenti di accedere al loro sistema o ai loro file personali e richiede il pagamento di un riscatto al fine di recuperare l'accesso ad essi.  -Malware  Malware significa software maligno. Una delle minacce informatiche più comuni, il malware è un software che un criminale informatico o un hacker ha creato per interrompere o danneggiare il computer di un utente legittimo. Spesso diffuso tramite un allegato e-mail non richiesto o un download dall'aspetto legittimo, il malware può essere usato dai criminali informatici per fare soldi o in attacchi informatici motivati politicamente. Ci sono molti tipi diversi di malware, come virus, Trojan, Spyware, Ransomware, Adware, botnet.  -Antivirus  Un antivirus è un programma che rileva i malware, li blocca e li elimina per evitare di infettare il dispositivo. Esistono diversi tipi di antivirus, per scegliere quello più adatto a te o alla tua azienda, dovrai prendere in considerazione le specifiche del dispositivo da proteggere e alcuni criteri da prendere in considerazione.  • Compatibile con il tuo sistema operativo  • Protezione del tuo dispositivo, senza rallentare la sua velocità, capacità o prestazioni.  • Aggiornamenti frequenti. Altrimenti, potremmo essere esposti a nuove minacce.  • Versatilità. Il nostro antivirus deve essere versatile come il malware..  • Capacità di agire. Oltre a riconoscere la minaccia, deve sradicarla e pulirla dal nostro dispositivo.  -Anti malware  Qual è la differenza tra antivirus e anti-malware?  Entrambi si riferiscono a un software progettato per rilevare, proteggere e rimuovere il software dannoso. Nonostante ciò che il nome potrebbe suggerire, il software antivirus protegge da più di un semplice virus; semplicemente usa un nome un po' antiquato per descrivere ciò che fa. Il software anti-malware è anche progettato per proteggere contro i virus, e semplicemente usa un nome più moderno che comprende tutti i tipi di software maligno, compresi i virus.  Sapendo questo, l'anti-malware può prevenire il verificarsi di un'infezione virale e rimuovere i file infetti. Tuttavia, l'anti-malware non è necessariamente in grado di ripristinare i file che un virus ha modificato o sostituito.  - Patches di Sicurezza. Vulnerabilità  È una parte importante della sicurezza informatica negli affari, perché aiuta a evitare lacune di vulnerabilità nei sistemi dell'azienda, aggiornando tutte le loro attrezzature e dispositivi. Questo include applicazioni per computer e sistemi operativi, firmware di apparecchiature elettroniche e software anti-malware. Le patch e gli aggiornamenti sono creati dagli stessi sviluppatori del software e servono a migliorare le sue prestazioni correggendo i bug di sicurezza e aggiungendo nuove funzionalità.  - Proteggere i Business Data: nozioni base di backup  Molto semplicemente, un backup dei dati non è altro che una copia dei file sul vostro computer o dispositivo. E, come evidenziato dalle molte minacce descritte sopra, mantenere un backup dei vostri importanti file e dati aziendali è essenziale per una serie di motivi importanti.  Qualsiasi backup è meglio di nessun backup, tuttavia, non tutti i dispositivi e le tecnologie di backup sono uguali o offrono gli stessi livelli di protezione. Per una protezione ottimale, è meglio salvaguardare i vostri dati usando la regola 3-2-1, che è la seguente:  • Tieni almeno tre (3) copie dei dati (così un singolo evento non distruggerà tutte le copie);  • Memorizzare i dati in almeno due (2) formati diversi (cioè disco, nastro, cloud, ecc.);  • Conservare una (1) copia fuori sede per proteggersi da incendi, inondazioni, furti e altri disastri fisici.  Proteggere le reti Wireless  L'uso di una rete wireless ti dà la comodità di poter lavorare e usare il tuo computer praticamente ovunque, e di connetterti ad altri computer in rete o accedere a Internet. Tuttavia, se la tua rete wireless non è sicura, ci sono rischi significativi. Per esempio, un hacker potrebbe intercettare qualsiasi dato che invii o ricevi, accedere ai tuoi file condivisi, dirottare la tua connessione a Internet ed esaurire la tua larghezza di banda o il tuo limite di download.  • Quando compri un router Wi-Fi, ha un nome e una password predefiniti. Questi sono molto facili da violare, quindi dovresti cambiarli. Inoltre, il router ha una password di amministratore che ti permette di cambiare e gestire le impostazioni del router. Proprio come il nome e la password del router, dovresti cambiare anche questa password.  • Per proteggere le informazioni che invii attraverso la rete Wi-Fi, puoi criptare la tua rete aggiornando il software del router. Cerca le impostazioni WPA3 o WPA2, che offrono la crittografia più forte.  Formazione dei dipendenti  I dipendenti possono rendere la vostra azienda vulnerabile agli attacchi, o aiutare a prevenirli. Numerosi studi dimostrano che una grande quantità di perdita di dati proviene dai dipendenti interni che, nella maggior parte dei casi per disattenzione o disinformazione, danno ai criminali informatici l'accesso alle loro reti.  Ci sono molti scenari che potrebbero risultare in attacchi in cui le vie d'accesso sono i dipendenti. Per esempio, un dipendente che perde un tablet di lavoro, dando via le sue credenziali di accesso, o aprendo e-mail fraudolente, che distribuiscono virus sulla rete.  Per proteggersi dalle minacce interne, è di fondamentale importanza investire in una formazione di qualità sulla cybersecurity per i dipendenti, che dia loro gli strumenti necessari per agire di fronte a varie situazioni e rischi.  Politiche. Politica di Sicurezza informatica. Cos’è una politica cyber security?  Per prevenire il crimine informatico, è importante non solo formare i vostri dipendenti nella prevenzione del crimine informatico, ma anche creare una politica di sicurezza informatica aziendale. Questo aiuterà a delineare chiaramente le linee guida per il trasferimento di dati aziendali, l'accesso a sistemi privati e l'utilizzo di dispositivi aziendali. Quando preparate la vostra politica, assicuratevi che guidi i vostri dipendenti su:  • Il tipo di informazioni aziendali che possono essere condivise e dove  • Uso accettabile dei dispositivi e dei materiali online  • Manipolazione e conservazione di materiale sensibile  Un modello completo di politica di cybersecurity includerà le seguenti parti di base:  • Introduzione  • Obiettivo  • Ambito  • Dati Confidenziali  Sicurezza dei dispositivi:  • Uso aziendale  • Uso personale  • Sicurezza e-mail  • Trasferimenti di dati  • Azione disciplinari  2.2 Cybersecurity a livello di utenti / dipendenti  La formazione degli utenti finali è importante perché affronta il fattore più imprevedibile della sicurezza informatica: le persone. Se non si seguono buone pratiche di sicurezza, chiunque può accidentalmente introdurre un virus in un sistema altrimenti sicuro. Insegnare agli utenti a prestare attenzione ai fattori di rischio è fondamentale per la sicurezza di qualsiasi organizzazione.  Proteggere i dati sui tuoi dispositivi  Dati personali e dati sensibili. Sono la stessa cosa?  Cosa sono i dati personali?  I dati personali sono qualsiasi informazione che qualcuno può usare per identificare, con un certo grado di precisione, una persona vivente. Per esempio, l'indirizzo e-mail di un dipendente di un'azienda è considerato un dato personale, perché indica che quella persona lavora per l'azienda. Anche un indirizzo fisico o un numero di telefono sono dati personali, perché queste informazioni possono essere usate per contattare la persona.  Tutto ciò che può affermare la vostra presenza fisica da qualche parte è anche considerato dato personale. Per esempio, le registrazioni delle telecamere di sicurezza sono dati personali, così come le impronte digitali.  Alcuni esempi possono essere:  • Un nome e un cognome  • Un indirizzo di casa  • Un indirizzo e-mail  • Un numero di carta d’identità  • Dati di localizzazione  • Un indirizzo IP (Internet Protocol)  • L'identificatore pubblicitario del suo telefono  Cosa sono i dati sensibili?  I dati personali sensibili sono un insieme specifico di "categorie speciali" che detengono una protezione legale più forte, e devono essere trattati con maggiore sicurezza, previa approvazione specifica del soggetto a cui si riferiscono quei dati. Questo include informazioni relative a:  • Origine etnica o razziale;  • Opinioni politiche;  • Credenze religiose o filosofiche  • Iscrizione al sindacato;  • Dati generici  • Dati biometrici (laddove elaborati per identificare in modo univoco qualcuno).  I dati personali sensibili devono essere conservati separatamente dagli altri dati personali, preferibilmente in un cassetto o schedario chiuso a chiave. Come per i dati personali in generale, dovrebbero essere conservati su computer portatili o dispositivi portatili solo se il file è stato criptato e/o sotto pseudonimo.  Sicurezza fisica  La sicurezza informatica inizia con una forte sicurezza fisica. Questo include l'archiviazione sicura dei documenti, chiudendoli a chiave in una stanza o in un armadio, limitando l'accesso fisico ai dati sensibili, cancellando correttamente le informazioni e distruggendo i documenti di dati sensibili quando non sono più necessari. Consentire l'accesso alle informazioni personali e finanziarie solo al personale che ne ha veramente bisogno.  • Ricorda ai tuoi dipendenti di non lasciare mai incustoditi i documenti di dati sensibili sul posto di lavoro o in luoghi pubblici. Le carenze nella sicurezza fisica possono esporre i dati aziendali sensibili al furto di identità, con conseguenze potenzialmente gravi.  A tutti può verificarsi a causa di violazioni della sicurezza fisica, come la perdita di un computer portatile, il furto di un telefono cellulare o lo smarrimento di un flash drive. Come tali, hanno meno probabilità di provocare una violazione dei dati se le informazioni su questi dispositivi sono protette.  Alcuni esempi utili:  Richiedere password complesse: Richiedete password lunghe, complesse e uniche. E assicurati che queste password siano conservate in modo sicuro. Considerare l'utilizzo di un gestore di password.  Utilizzare l'autenticazione a più fattori: Richiedi l'autenticazione a più fattori per accedere alle aree della tua rete con informazioni sensibili. Questo richiede ulteriori passaggi oltre al login con una password, come un codice temporaneo su uno smartphone.  Limitare i tentativi di login: Limitare il numero di tentativi di login errati consentiti per sbloccare i dispositivi. Questo aiuterà a proteggere dagli intrusi.  Crittografare: Crittografare i dispositivi portatili, compresi i computer portatili e le chiavette, che contengono informazioni sensibili. Crittografare tutti i dati sensibili che si inviano al di fuori dell'azienda, ad esempio a un commercialista o a un avvocato.   * Sicurezza delle e-mail   Nel caso in cui l'utente/dipendente utilizzi dispositivi personali per accedere ai sistemi dell'azienda, o per uso personale, devono essere prese alcune misure di sicurezza per quanto riguarda l'uso della posta elettronica, in quanto può essere anche una porta d'ingresso per azioni criminali. Nel caso in cui i dipendenti debbano utilizzare i loro dispositivi personali per accedere ai sistemi aziendali, i dipendenti dovrebbero riferire queste informazioni alla direzione per la registrazione.  Per assicurare la protezione dei sistemi aziendali, tutti gli impiegati dovrebbero:  • Assicurarsi che tutti i dispositivi personali utilizzati per accedere ai sistemi aziendali siano protetti da password (minimo 8 caratteri).  • Installare un software antivirus completo  • Aggiornare regolarmente il software antivirus  • Bloccare tutti i dispositivi, se lasciati incustoditi  • Assicurarsi che i dispositivi siano sempre protetti  • Usare sempre reti sicure e private  Proteggere i sistemi di posta elettronica è una priorità assoluta, in quanto le e-mail possono portare a furti di dati, truffe e portare software maligno come worm e bug. Pertanto, si consiglia agli utenti/dipendenti di:  Verifica la legittimità di ogni e-mail, compreso l'indirizzo e-mail e il nome del mittente.  - Evita di aprire e-mail sospette, allegati e di cliccare su link.  - Cercare errori grammaticali significativi.  - Evitare titoli e link che incoraggino a cliccare.  - Contatta il dipartimento IT per qualsiasi e-mail sospetta. Verifica la legittimità di ogni e-mail, compreso l'indirizzo e-mail e il nome del mittente.  Phishing  Conosciuto anche come frode elettronica. Conoscere un po' meglio le frodi più comuni e pericolose ci aiuterà ad evitare di caderci.  Attraverso questi metodi, "phishing" e "smishing", l'aggressore cerca di ottenere informazioni private come password o carte di credito. In questo attacco, alla vittima vengono chiesti dati vulnerabili, come password o codici di accesso, via e-mail, fingendo di essere il sito web o l'entità legittima, in modo che la vittima fornisca i dati richiesti dall'aggressore.  Smishing  Questa minaccia è simile al phishing, l'unica differenza è che viene inviata via SMS ai telefoni. L'hacker invia un messaggio ai nostri telefoni, aprire il messaggio non è pericoloso. Il pericolo sta nel cliccare sul link, è allora che inizia l'attacco.  2. 3 I più comuni rischi informatici di cui essere consapevoli. La guida di base della Cybersecurity  Dopo aver familiarizzato con i concetti di cui sopra, diamo un'occhiata ai rischi più frequenti affrontati dalle PMI, secondo gli studi basati sull'indagine dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA), con phishing e attacchi basati sul web in cima alla lista.  1) Attacchi Phishing  Questo tipo di attacco è diventato estremamente popolare a causa del lavoro a distanza. Un clic incauto su un link è tutto ciò che serve a un criminale informatico per ottenere l'accesso a informazioni aziendali sensibili.  2) Attacchi dal web  I criminali informatici utilizzeranno quasi tutte le vulnerabilità - all'interno di un sistema operativo (OS) o di un'applicazione - per effettuare un attacco. Tuttavia, la maggior parte dei criminali informatici sviluppa minacce web che prendono deliberatamente di mira alcuni dei sistemi operativi e delle applicazioni più comuni.  3) Attacchi di General malware  Molte PMI sottovalutano la possibilità di attacchi informatici a causa delle loro dimensioni. Tuttavia, questo è proprio quello che gli hacker stanno cercando, in quanto possono rapidamente trarre profitto da una minaccia ransomware alle PMI meno sicure.  4) Insiders cattivi  Questo tipo di minaccia si riferisce all'esistenza di persone all'interno di un'organizzazione (sia dipendenti interni che fornitori esterni, tra gli altri) che per negligenza, ignoranza e/o malafede, compiono un'"azione" che colpisce la sicurezza di processi, sistemi o strutture di un ambiente operativo industriale o di un'infrastruttura critica.  5) Attacchi di negazione del servizio  Lo scopo di questi attacchi è quello di interrompere il sito web di un'azienda in modo che sia inaccessibile, cosa che viene fatta per vari motivi dal criminale informatico. Un sito web bloccato può portare a perdite di entrate, violazioni di dati, sfiducia dei clienti e paralisi dell'attività dell'azienda.  La guida di base della sicurezza informatica  1. Determina le tue vulnerabilità  La prima cosa da fare è identificare le vostre vulnerabilità, in modo da sapere quali dati proteggere. Fatevi domande come: Quali sono i dati più importanti che la mia azienda conserva? Dove memorizzate questi dati? Una volta che avete le risposte, potete iniziare a valutare i rischi.  2. Proteggi i tuoi dispositivi  I dispositivi di lavoro sono cruciali per le prestazioni della vostra azienda. La loro connessione internet li rende vulnerabili agli attacchi informatici. Ecco alcuni consigli per proteggerli.  A. Aggiorna il software  B. Proteggi I tuoi dispositive dai virus  C. Installa un Firewall  D. Precauzioni speciali per computer e altri dispositivi mobili  3. Proteggi i tuoi dati  Indipendentemente dal tipo di attività che si svolge, i dati sono una parte essenziale di essa. I dati possono essere danneggiati in mille modi diversi, uno dei quali è attraverso attacchi informatici. Ecco alcuni consigli utili su come proteggere i vostri dati.  A. Implementare una procedura per il backup dei dati critici  B. Crittografare le informazioni aziendali riservate che si archiviano nel cloud  C. Proteggere le password  D. Impostare i permessi  E. Proteggere le vostre reti wireless  F. Navigare in Internet in modo sicuro  G. Proteggere le informazioni riservate create dai lavoratori remoti  H. Proteggere i dati dei clienti  4. Diffondi la sicurezza informatica sul posto di lavoro  Le misure di sicurezza menzionate in questa guida di base possono aiutarvi a ridurre significativamente il rischio di un attacco informatico. Ma questo non servirà a nulla se i dipendenti della vostra azienda non hanno la consapevolezza e la formazione necessarie per essere in grado di contribuire alla loro prevenzione. Includete questo tipo di formazione nella vostra azienda, e non dimenticate di creare una politica di cybersecurity aziendale che tutti i membri del team possano seguire. | | |
| **Contenuti elencati** | | |
| 2. Cybersecurity e strumenti digitali per le PMI. Essere preparati a prevenire e risolvere Cyber-attacchi  2.1 Sicurezza a livello business  2.2 Sicurezza informatica a livello di utente/dipendente  2.3 I più comuni rischi informatici di cui essere consapevoli. La guida di base della Cybersecurity | | |
| **5 novità del glossario** | | |
| Cybersecurity: è un insieme di pratiche per difendere i sistemi informatici e il software dal crimine informatico. La cybersecurity copre molte aree: sicurezza delle reti, sicurezza delle app, sicurezza delle informazioni, sicurezza degli utenti, ecc.  Cybercrime: è qualsiasi attività criminale che si svolge nel mondo digitale, che coinvolge un computer, un dispositivo in rete o una rete, e che mira a raggiungere un certo scopo o beneficio, che può essere di diversi tipi.  Ransomware: è un tipo di software maligno che cripta le informazioni su diversi dispositivi. Usando questo metodo, i criminali informatici estorcono denaro alle loro vittime chiedendo un riscatto in cambio di riottenere l'accesso ai loro dati.  Malware: significa software maligno. Una delle minacce informatiche più comuni, il malware è un software che un criminale informatico o un hacker ha creato per interrompere o danneggiare il computer di un utente legittimo. Ci sono molti tipi diversi di malware, come: Virus, Trojan, Spyware, Ransomware, Adware, Botnets.  Backup: molto semplicemente, un backup dei dati non è altro che una copia dei file sul vostro computer o dispositivo. E, come evidenziato dalle molte minacce descritte sopra, mantenere un backup dei vostri importanti file e dati aziendali è essenziale per una serie di importanti ragioni. | | |  |
| **Bibliografia e Ulteriori Referenze** | | | SWIFTSME\_Course 2\_Cybersecurity and digital tools for SMEs. Be prepared to prevent and solve Cyber-attacks\_EN |
| <https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes>  <https://www.kaspersky.com/resource-center/preemptive-safety/protecting-wireless-networks>  <https://www.pandasecurity.com/es/mediacenter/seguridad/parches-brechas-datos/>  <https://searchsecurity.techtarget.com/definition/cybercrime>  <https://es.malwarebytes.com/antivirus/>  <https://ciberseguridad.com/normativa/espana/medidas/actualizaciones/>  <https://www.betterteam.com/cyber-security-policy>  <https://business.gov.au/online/cyber-security/create-a-cyber-security-policy>  <https://www.daemon4.com/empresa/noticias/las-principales-amenazas-de-ciberseguridad-para-pymes/>  <https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data>  <https://www.bbva.com/es/phishing-y-smishing-que-son-y-como-evitarlos/>  <https://www.acronis.com/en-us/articles/data-backup-for-business/>  <https://www.ciberseguridadlogitek.com/la-amenaza-del-malicious-insider-en-los-entornos-de-operacion-industrial-y-de-infraestructuras-criticas/>  <https://usa.kaspersky.com/resource-center/threats/web>  <https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/>  <https://es.vpnmentor.com/blog/la-guia-completa-de-ciberseguridad-para-pequenas-y-medianas-empresas/>  <https://www.ncsc.gov.uk/collection/small-business-guide>  <https://insights.ascentor.co.uk/blog/2019/11/12-practical-cyber-security-tips-for-smes>  <https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf>  <https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security>  <https://ciberseguridadbidaidea.com/ciberseguridad/6-principales-amenazas-de-una-empresa-en-ciberseguridad/>  <https://www.widefense.com/recursos/ciberseguridad/pequenas-empresas/>  <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>  <https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices>  <https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware>  <https://internetpasoapaso.com/antimalware/>  <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited>  <https://me-en.kaspersky.com/blog/how-to-set-up-wifi-router/4390/>  <https://blog.walkme.com/5-employee-training-fails/>  <https://almamate.in/importance-of-selecting-the-best-salesforce-institute-in-noida/>  <https://cmitsolutions.com/blog/6-ways-protect-data-devices-digital-identity/>  <http://www.rbntechnologies.com/products.html>  <https://memoori.com/physicalsecurity-2016-rounded_v1/>  <https://www.djcs.com.ve/djcsnews/1901-automationedge-password-reset>  <https://www.datacenterknowledge.com/security/managing-encryption-data-centers-hard-and-it-will-get-harder>  <https://nakedsecurity.sophos.com/es/2016/08/09/email-how-secure-is-yours-survey/>  <https://www.valoradata.com/blog/que-es-el-phishing/>  <https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/>  <https://www.keepnetlabs.com/7-ways-to-prevent-phishing-attacks-in-2021/>  <https://www.teceze.com/what-is-vmdr-vulnerability-management>  <https://cypheradda.blogspot.com/2019/05/5-cybersecurity-tips-for-workplace.html>  <https://molinaoposiciones.com/2021/03/22/por-fin-fecha-definitiva-de-auxilio/>  <https://unaaldia.hispasec.com/2021/04/malware-en-plantillas-empresariales-de-descarga-gratuita.html> | | |  |
| **5 domande a risposta multipla per autoanalisi** | | |  |
| 1) Cosa sono i dati personali?  **a) I dati personali sono qualsiasi informazione che qualcuno può usare per identificare, con un certo grado di precisione, una persona vivente. Per esempio, l'indirizzo e-mail di un dipendente di una società è considerato un dato personale, perché indica che quella persona lavora per la società.**  b) I dati personali sono un insieme specifico di "categorie speciali" che detengono una protezione legale più forte, e devono essere trattati con maggiore sicurezza, previa approvazione specifica del soggetto a cui quei dati si riferiscono.  2) Selezionare la risposta corretta relativa al concetto di Security Patches.  **a) È una parte importante della cyber-sicurezza nel business in quanto aiuta a evitare lacune di vulnerabilità nei sistemi dell'azienda, aggiornando tutte le loro attrezzature e dispositivi. Questo include applicazioni per computer e sistemi operativi, firmware di apparecchiature elettroniche e software anti-malware.**  b) È una parte importante della cyber-sicurezza che include l'archiviazione sicura dei documenti, chiudendoli a chiave in una stanza o in un armadio, limitando l'accesso fisico ai dati sensibili, cancellando le informazioni correttamente e distruggendo i documenti di dati sensibili quando non sono più necessari.  3) Per quanto riguarda la Cybersecurity a livello utente, perché è importante una formazione per l'utente finale?  a) Non è così importante, poiché l'utente finale è solo quello colpito dal crimine informatico e non ha altra scelta che installare un buon antivirus.  b) **La formazione dell'utente finale è importante perché affronta il fattore più imprevedibile della sicurezza informatica: le persone.**  4) Qual è la differenza tra antivirus e anti-malware?  a) Entrambi si riferiscono a un software progettato per rilevare, proteggere e rimuovere il software dannoso.  b) Un anti-malware può rilevare il software dannoso, un antivirus è specificamente progettato per rimuovere solo la minaccia dal computer    5) Seleziona l'opzione corretta sulla protezione delle reti wireless.  **a) Se la tua rete wireless non è sicura, ci sono rischi significativi. Per esempio, un hacker potrebbe intercettare tutti i dati che invii o ricevi, accedere ai tuoi file condivisi, dirottare la tua connessione Internet ed esaurire la tua larghezza di banda o il limite di download.**  **b) Quando compri un router Wi-Fi, ha un nome e una password predefiniti. Questi sono molto facili da violare, quindi dovresti cambiarli. Inoltre, il router ha una password di amministratore che ti permette di cambiare e gestire le impostazioni del router, dovresti cambiare anche questa password.** | | |  |
| **Materiale relativo** |  | |
| **PPT Correlata** | SWIFTSME\_Course 2\_Cybersecurity and digital tools for SMEs. Be prepared to prevent and solve Cyber-attacks\_EN | |
| **Link di Referenza** |  | |
| **Video YouTube (se presente)** |  | |