TeleGrow
Enhancing the Teleworking Digital Skills for the Middle aged employees

Moduli di formazione sul telelavoro: La formazione definitiva sul telelavoro per gli operatori della formazione professionale

Modulo 6 - Fondamenti di sicurezza online

27/6/2022

Erasmus+

Progetto finanziato da: **Bando 2020 Round 1 KA2 - Cooperazione per l'innovazione e lo scambio di buone pratiche/ KA226 - Partenariati per la preparazione all'istruzione digitale**

Il sostegno della Commissione Europea per la produzione di questa pubblicazione non costituisce un'approvazione dei contenuti, che riflettono solo le opinioni degli autori. La Commissione Europea non può essere ritenuta responsabile per qualsiasi uso che possa essere fatto delle informazioni in essa contenute.

Indice

1. Introduzione al tema

In questi tempi difficili, tutti cercano di adattarsi alla nuova era del lavoro da casa senza la necessaria conoscenza della quantità di rischi e minacce che comporta, non solo per le persone con più di 50 anni, a cui si rivolge il progetto TeleGrow, ma per i lavoratori di tutte le età. Un rapporto della Commissione europea del 2020 afferma che circa il 40% dei lavoratori dell'UE ha iniziato a lavorare da remoto dopo la pandemia COVID-19, con un aumento di quasi 8 volte rispetto all'anno precedente. Questo rapido aumento del telelavoro rende difficile per le aziende implementare nuove e solide misure di sicurezza, aprendo una finestra per varie pratiche dannose. Con un aumento delle attività di criminalità informatica di oltre il 600% dall'inizio della pandemia, è facile concludere che le persone di età superiore ai 50 anni che hanno avuto poca o nessuna esperienza con il telelavoro sono particolarmente vulnerabili ai pericoli che può comportare. Questi pericoli riguardano il furto d'identità, la violazione dei dati, i software maligni (malware) e i virus, le frodi bancarie e molte altre minacce a cui gli anziani potrebbero non essere ben preparati.

Questo modulo è concepito come una breve introduzione al tema della sicurezza online. Include la descrizione dei pericoli più comuni del telelavoro e dell'uso generale di Internet che i gruppi target del progetto TeleGrow possono incontrare. Questa parte del modulo aiuterà a capire cosa sono lo spam e il phishing, come riconoscerli e quali pericoli possono comportare. Verranno spiegate in modo approfondito anche altre pratiche comuni, come l'hacking, il ransomware o il furto di identità. Il modulo spiegherà anche quali sono le misure da adottare per proteggere la connessione privata a Internet e farà conoscere al discente il Regolamento generale sulla protezione dei dati. Infine, questo modulo del progetto TeleGrow includerà anche una breve serie di esercizi per i discenti, per verificare le conoscenze acquisite nel corso del modulo.

2. Obiettivi di apprendimento

Al termine di questo modulo, il discente è in grado di:

- essere istruiti su spam e phishing e su come riconoscerli
- capire cos'è l'hacking, come funziona il ransomware e come proteggersi dal furto di identità e dalle conseguenze che ne derivano
- sapere quali misure adottare per proteggere la propria connessione a Internet e qual è la differenza tra una password debole e una forte. differenza tra una password debole e una forte
- acquisire conoscenze sul Regolamento generale sulla protezione dei dati e sulle modalità di protezione delle informazioni personali
- essere in grado di stabilire un ambiente di lavoro sicuro da casa con l'uso di attività pratiche alla fine del modulo

3. Contenuti didattici

Capitolo 1 - Spam e Phishing

La parola "spam" si riferisce a tutti i messaggi digitali indesiderati che le persone ricevono e che sono stati inviati a un grande gruppo di destinatari. Questo processo è spesso effettuato da cosiddetti "spambot", che sono programmi automatizzati utilizzati per inviare messaggi di spam agli account di posta elettronica, ai siti di social network o ai forum. Anche se lo spam può sembrare un problema relativamente nuovo, la sua storia risale al 1978, quando Gary Thuerk volle promuovere il suo prodotto inviando e-mail non richieste a migliaia di persone, che presumibilmente generarono circa 12 milioni di dollari di entrate.

L'utilizzo odierno dei messaggi di spam rimane per lo più lo stesso, in quanto viene utilizzato per generare un profitto attraverso la promozione di qualcosa. In genere, i prodotti pubblicizzati sono di qualità discutibile e gli argomenti che i messaggi di spam pubblicizzano sono per lo più i seguenti:

- prodotti farmaceutici
- contenuti per adulti
- servizi finanziari
- gioco d'azzardo online
- criptovalute

Fonte: freepik.com

Nel 2020, circa il 50% di tutte le e-mail ricevute erano spam. Le persone che creano e inviano messaggi di spam sfruttano gli utenti di Internet inesperti e l'apertura di tali e-mail può avere conseguenze molto spiacevoli, come la condivisione di informazioni

private con persone non autorizzate o l'inserimento nelle mailing list di vari venditori, che porteranno ad accumulare ancora più e-mail indesiderate nella casella di posta elettronica di qualcuno. Anche se i numeri possono sembrare schiaccianti, oggi le persone vedono raramente messaggi di spam nelle loro caselle di posta elettronica. Ciò è dovuto al rapido sviluppo dell'area di filtraggio dello spam. Le statistiche rivelate da Google nell'aprile 2020 hanno dimostrato che sono riusciti a bloccare e filtrare il 99,9% delle e-mail di spam. Ciò significa che gli utenti di Internet di oggi, insieme alle persone di età superiore ai 50 anni, sono molto più al sicuro dalla ricezione di questo tipo di messaggi. Questo non significa che il filtraggio funzioni perfettamente; ci sono ancora e-mail di spam che passano e per poterle filtrare da soli, gli utenti di Internet dovrebbero sapere quale tipo di messaggio dovrebbero evitare di aprire. Alcuni dei tipi più comuni di spam sono:

- Spoofing delle e-mail

  Questo tipo di messaggi cerca di imitare il mittente contraffacendo la stessa identica e-mail che ha il mittente e ingannando il destinatario facendogli credere che l'e-mail provenga da una persona o da un sito web di cui si può fidare. Spesso viene richiesta una qualche azione, che può essere la richiesta di pagamento di una fattura insoluta, la convalida/sblocco di un account o la verifica di un acquisto, e viene fornito un link che, una volta cliccato, può essere utilizzato per rubare le informazioni personali del destinatario. Fortunatamente, molti provider di posta elettronica avvertono preventivamente l'utente del rischio di essere "spoofato".

- Truffe con anticipo

  A volte definita "truffa del principe nigeriano", una delle idee alla base di questa truffa è che il mittente promette una grande somma di denaro, ma solo se il destinatario fornisce un piccolo prestito in anticipo. Di solito si dice che questo prestito è necessario per una qualche questione legale che sbloccherà la somma maggiore. L'altro tipo di truffa a pagamento anticipato funziona in modo simile,

ma in questo caso il mittente si finge un amico intimo o un familiare del destinatario che ha bisogno di denaro a causa di una qualche emergenza.

- Pubblicità e spam di malware

Lo spam pubblicitario è semplicemente un messaggio non richiesto che offre un qualche tipo di prodotto. Anche se a volte queste offerte possono essere vere, in molti casi il prodotto non esiste o non funziona. Lo spam malware è un tipo di messaggio che contiene vari tipi di contenuti dannosi nascosti dietro i link o gli allegati presenti nel messaggio. Una volta che la persona scarica e apre il file allegato o scaricato attraverso il link, gli script dannosi vengono eseguiti e infettano il computer con diversi tipi di malware pericolosi.

Fonte: freepik.com

- Phising

Simile allo spoofing delle e-mail, ma più complesso, è il phishing. Questa pratica dannosa viene utilizzata nel contesto di frodi, spionaggio o per organizzare attacchi informatici mirati a varie organizzazioni. Si tratta di contraffare e-mail o telefonate e sostenere di provenire da una fonte legittima per convincere le persone a rivelare le proprie informazioni personali o finanziarie, spesso senza un obiettivo particolare. Anche i messaggi di spear phishing vengono inviati da e-mail contraffatte che sembrano affidabili, ma in questo caso il criminale informatico raccoglie informazioni sulla vittima da diverse fonti, come i post pubblici sui social media, i siti su cui è

registrata l'e-mail della vittima, i profili degli amici della vittima sui social media o le informazioni sui dipendenti sul sito web dell'azienda.

L'hacker può quindi raccogliere tutte le informazioni su quella persona e preparare un messaggio personalizzato, di cui il destinatario può essere vittima. Queste e-mail contengono spesso link dannosi, ma possono anche essere utilizzate per creare una connessione tra il criminale e la vittima, al fine di ottenere fiducia e rubare informazioni sensibili. A volte, gli attacchi di spear phishing prendono di mira i dirigenti di un'azienda per indurli a rivelare le loro informazioni personali o i dati aziendali più importanti, che possono poi essere utilizzati per scopi dannosi. Per essere meno inclini a cadere nei tentativi di phishing, gli utenti di Internet dovrebbero prestare particolare attenzione ed evitare di aprire:

- Email di vincita di un premio importante
- Siti web falsi che assomigliano molto a quelli originali
- Minacce relative alla disattivazione dell'account o alla perdita dell'accesso ad esso
- Messaggi su una falsa infezione da malware
- Email a tema COVID-19
- Falsi parenti che chiedono denaro
- Grammatica scadente e parole sbagliate in e-mail apparentemente formali.

Anche se i filtri per i contenuti dannosi forniti dalla maggior parte dei provider di posta elettronica offrono una forte protezione contro lo spam e il phishing, le persone devono tenere presente che non sono impeccabili e che ci sono alcune contromisure che possono adottare per ridurre ulteriormente le possibilità di furto dei propri dati personali. A tal fine, è consigliabile copiare e incollare il contenuto di un messaggio sospetto in un motore di ricerca (ad esempio, Google), poiché è possibile che sia già stato segnalato come un tentativo di pishing. Un'altra buona pratica è quella di contattare l'azienda che si presume abbia inviato il messaggio sospetto senza cliccare sui link o sugli allegati presenti al suo interno. Una buona idea è anche quella di installare sul computer filtri antispam e barre di strumenti anti-phishing, in quanto

questi strumenti possono proteggere l'utente da messaggi di questo tipo. In un ambiente di lavoro, i dipendenti dovrebbero cercare di confermare verbalmente qualsiasi richiesta inviata loro via e-mail e cambiare regolarmente le proprie password.

Capitolo 2 - Hacking, Ransomware, furto d'identità

A causa del recente aumento del telelavoro e della necessità di rimanere a casa e sbrigare molte commissioni online a causa della pandemia COVID-19, il mondo sta assistendo anche a un enorme aumento dei crimini informatici. Questi possono essere definiti come qualsiasi attività illegale svolta utilizzando un computer e sono spesso associati a persone chiamate "hacker" o "criminali informatici", che possono essere suddivisi in molte categorie diverse a seconda di ciò che vogliono ottenere e di quanto sono abili.

Fonte: freepik.com

L'hacking è il processo di identificazione delle falle di sicurezza di un sistema informatico o di una rete al fine di ottenere l'accesso a dati personali o aziendali. L'uso di un algoritmo di decifrazione delle password per accedere a un sistema informatico è un esempio di hacking informatico. Sebbene sia spesso considerata una pratica dannosa, a volte è legale e utilizzata con buone intenzioni, principalmente per migliorare la sicurezza online e proteggere i dati preziosi all'interno di una determinata organizzazione. Tale pratica è chiamata "hacking etico". L'hacking abituale copre un ampio spettro di pratiche malevole, a partire dal rallentamento dei computer altrui, passando per il furto di informazioni relative alle carte di credito, fino all'intimidazione su larga scala e alla richiesta di riscatto. Come accennato nel Capitolo 1, gli hacker

possono accedere ai dispositivi altrui attraverso tentativi di phishing e malware contenuti in messaggi di spam sospetti, ma questi non sono gli unici metodi che utilizzano. Una tecnica di hacking comune a cui molte persone possono essere soggette è la creazione di un falso punto di accesso Wi-Fi in un luogo pubblico che, una volta collegato, reindirizza la vittima a un sito web che può rubare i suoi dati personali.

Per evitare che ciò accada, le persone dovrebbero evitare di utilizzare reti Wi-Fi pubbliche e prestare sempre attenzione quando utilizzano i propri dispositivi in luoghi come ristoranti, aeroporti, centri commerciali o parchi.

Un'altra forma di software dannoso che può essere molto pericolosa per gli ultracinquantenni che iniziano a telelavorare è il **ransomware.** Si è rivelato molto pericoloso in quanto non solo è uno dei problemi di sicurezza di Internet più preoccupanti al giorno d'oggi, ma è anche molto comune. Questo malware cripta file e documenti da un singolo computer a un'intera rete, compresi i server. Dopo l'attacco ransomware, la vittima riceve le istruzioni per pagare un riscatto per sbloccare i file; in caso contrario, i dati preziosi saranno resi pubblici o venduti ad altri criminali informatici, da cui il nome "ransomware".

Fonte: freepick.com

Questo e altri malware si diffondono più comunemente attraverso gli allegati dei messaggi di spam di phishing, motivo per cui è fondamentale trattare con estrema

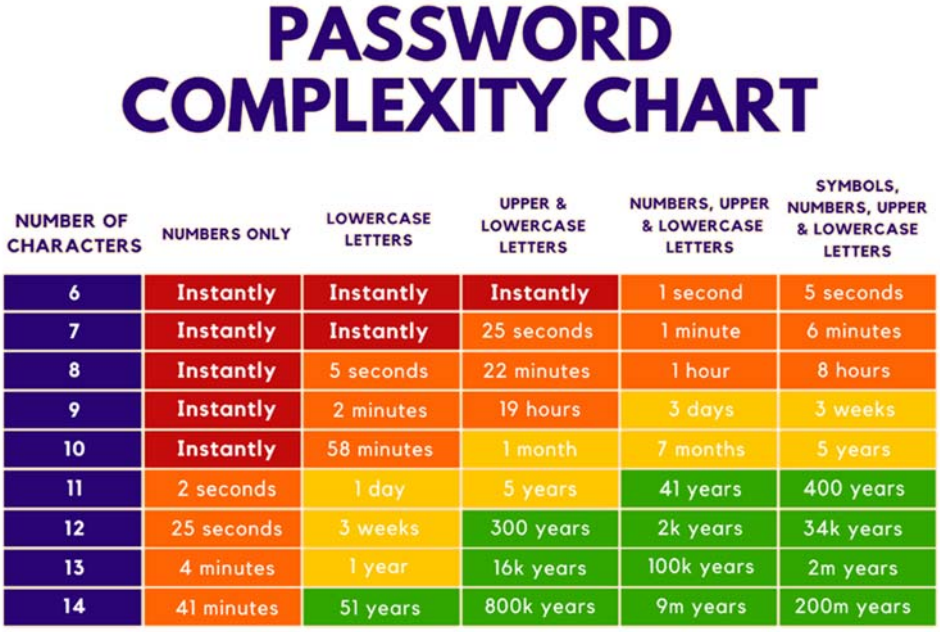
cautela qualsiasi e-mail sospetta. Gli attacchi ransomware sono molto pericolosi perché, se hanno successo, possono esporre preziose informazioni private di migliaia di dipendenti se sono rivolti a una specifica azienda.

Una delle forme di criminalità informatica in più rapida crescita è il furto d'identità. Il criminale ruba i dati personali, come le credenziali, i dettagli del conto bancario, le date di nascita, ecc. per impersonare la vittima e utilizzare tali informazioni per ottenere profitti monetari e causare ulteriori danni alle persone. I metodi utilizzati dagli hacker per farlo sono simili a quelli di altri crimini informatici. Possono acquisire questi dati preziosi attraverso tentativi di phishing o introducendosi nei computer utilizzando vari malware e punti di accesso Wi-Fi pubblici falsi o mal protetti. In seguito, possono utilizzare i dati per ottenere prestiti, acquistare vari oggetti o persino commettere reati a nome della vittima. È bene controllare regolarmente i rapporti di credito e verificare eventuali inesattezze o trasferimenti bancari che potrebbero sembrare sospetti. La somma di denaro mancante non deve necessariamente essere ingente, perché il ladro potrebbe rubare a migliaia di persone contemporaneamente. Le vittime di furto d'identità dovrebbero denunciare al più presto questo reato alle autorità, congelare i loro conti bancari e aprirne di nuovi. Se possibile, le vittime dovrebbero contattare le banche, gli istituti di recupero crediti e altri luoghi in cui sanno che il ladro ha utilizzato le loro informazioni personali. È anche importante contattare parenti, datori di lavoro e colleghi dell'azienda in cui si lavora attualmente, perché il ladro potrebbe essere in possesso anche delle loro informazioni.

Le tecniche utilizzate dagli hacker per rubare o portare il caos nella vita delle persone sono sempre più sofisticate. Tenendo conto di ciò, le persone devono sapere come proteggersi per ridurre al minimo le possibilità di essere una delle vittime dei crimini informatici. Esiste una contromisura di protezione che, una volta implementata, riduce il rischio di avere a che fare con i criminali informatici.

Creare una password forte. È fondamentale per mantenere al sicuro i dati preziosi. Una buona password non è ovvia, ma è facile da ricordare. Non dovrebbe essere più corta di 12 caratteri, perché con la tecnologia di oggi ci vogliono pochi secondi per

decifrare le password brevi. Una password forte dovrebbe includere simboli unici come numeri e lettere minuscole o maiuscole, per aggiungere un ulteriore livello di sicurezza. È importante che sia forte e difficile da dimenticare. Una tecnica comune per creare password forti consiste nel creare un acronimo da una citazione preferita o da una frase memorabile, aggiungendovi alcuni simboli speciali. Un'altra buona pratica è quella di utilizzare i gestori di password. Questi programmi generano e memorizzano le password dell'utente in un unico account crittografato in modo sicuro. Un'altra cosa fondamentale è mantenere le password private e non inviarle mai a nessuno tramite e-mail o SMS. Con i dati raccolti, il grafico seguente mostra quanto sia difficile per un hacker violare una password che può sembrare complessa per l'utente.



NUMBER OF CHARACTERS	NUMBERS ONLY	LOWERCASE LETTERS	UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS	SYMBOLS, NUMBERS, UPPER & LOWERCASE LETTERS
6	Instantly	Instantly	Instantly	1 second	5 seconds
7	Instantly	Instantly	25 seconds	1 minute	6 minutes
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2k years	34k years
13	4 minutes	1 year	16k years	100k years	2m years
14	41 minutes	51 years	800k years	9m years	200m years

Dati raccolti su: https://www.security.org/how-secure-is-my-password/

Dai dati raccolti, è facile confermare quanto affermato in precedenza. Una password di 12 caratteri dovrebbe essere il minimo per una sicurezza ottimale e non è nemmeno necessario che sia molto complessa. Per renderla infrangibile per almeno 300 anni, basta una password con lettere minuscole e maiuscole. Va notato che **è**

assolutamente sconsigliato inserire il proprio nome come password, poiché può essere facilmente decifrato, indipendentemente dalla lunghezza.

Capitolo 3 - Connessione Internet sicura

È risaputo che Internet è una fonte affidabile, ma pericolosa, di informazioni e intrattenimento. A causa della quantità di malware, spie e hacker che aspettano solo una buona occasione per attaccare, è fondamentale sapere come difendersi, perché a volte una buona password non basta. Esistono molti modi per rafforzare la sicurezza di una connessione Internet e molti di essi non richiedono conoscenze tecnologiche avanzate.

Per cominciare, si consiglia di implementare l'**autenticazione a due fattori** (2FA) ogni volta che è possibile. Già solo questo può dissuadere la maggior parte degli hacker dall'introdursi nell'account di qualcuno. Funziona come secondo livello di verifica quando si accede a un account, mentre il primo è di solito una password, il secondo è spesso una chiave unica inviata al numero di cellulare dell'utente che deve essere inserita dopo aver effettuato l'accesso con una password. È considerato un metodo molto efficace per proteggere gli utenti dal rischio di furto della password, poiché l'unicità della chiave rende molto più difficile per un hacker entrare in un account.

Un'altra buona pratica è quella di utilizzare una **rete privata virtuale (VPN)**. Ogni volta che ci si connette a una rete, viene scambiato un flusso di dati tra l'utente e i server. La VPN crea una connessione sicura tra queste due parti crittografando i dati prima che vengano inviati o ricevuti dagli utenti. Una VPN nasconde l'indirizzo IP e la posizione dell'utente, in modo che i criminali informatici non possano più scoprire l'ubicazione delle loro potenziali vittime perché, grazie alla VPN, le rintraccerebbero nella posizione del server VPN, rendendo molto più difficile accedere ai loro dati. È un ottimo strumento per proteggere la connessione quando si utilizzano reti Wi-Fi pubbliche in luoghi facilmente violabili come aeroporti o ristoranti.

Fonte: freepik.com

Per impostare questo tipo di connessione è necessario trovare un fornitore di servizi VPN affidabile e sottoscrivere un abbonamento. Sul mercato sono presenti alcuni provider che offrono i loro servizi gratuitamente, ma è consigliabile acquistare un abbonamento a pagamento in quanto offre maggiori funzionalità per una connessione più sicura. Una volta trovato il provider VPN preferito, all'utente verrà richiesto di scaricare il software necessario. Il download deve essere sempre effettuato direttamente dal sito web del provider, in quanto il download da una fonte diversa potrebbe comportare il download di file contenenti malware. La maggior parte delle app VPN è disponibile su una vasta gamma di dispositivi e la loro procedura di configurazione è accessibile a tutti. Una volta scaricata l'app e creato l'account, non resta che attivarla e non temere più che qualcuno si introduca nel nostro dispositivo.

Anche la **modifica del nome e della password predefiniti del router** può aiutare a proteggere la rete. Ogni router viene fornito con un nome e una password generici, necessari per la prima configurazione. Subito dopo, una buona pratica è quella di cambiare il nome e la password con qualcosa di unico, tenendo presente le linee guida per la creazione di una password forte. Questo perché i nomi dei router (SSID - service set identifier) contengono spesso la marca e il modello, il che rende più facile per gli hacker trovare router che sanno essere vulnerabili alle violazioni. È anche possibile

nascondere completamente l'SSID di un router, in modo che le probabilità che un hacker scopra la connessione siano prossime allo zero.

Fonte: freepik.com

Mantenere tutto aggiornato. L'aggiornamento di solito sembra una seccatura inutile e a volte può persino peggiorare il funzionamento di un dispositivo, aggiungendo nuove funzioni non necessarie o rimuovendo quelle che erano utili. È importante prestare attenzione alle notifiche di aggiornamento che possono apparire. Qualsiasi software non è privo di difetti. La maggior parte di essi contiene vulnerabilità nascoste di cui nemmeno gli sviluppatori erano a conoscenza all'inizio. Una volta scoperte, possono essere sfruttate dagli hacker. Per questo motivo, ogni software ha bisogno di versioni più recenti, che abbiano delle correzioni nei punti vulnerabili. Questo è molto importante dal punto di vista della sicurezza online, perché mantenere tutto aggiornato riduce anche le possibilità di successo di un attacco hacker. Gli utenti che aggiornano regolarmente il proprio software riducono le possibilità di un attacco informatico ai loro dispositivi, poiché è possibile che le vecchie vulnerabilità che potrebbero essere utilizzate dagli hacker siano già state risolte. Esiste la possibilità che l'aggiornamento possa interrompere alcune funzioni del software, o addirittura renderlo inutilizzabile su alcuni dispositivi; per questo motivo, una volta effettuato l'aggiornamento, è buona norma verificare che l'aggiornamento non abbia interrotto nulla. Inoltre, un software non aggiornato può perdere le funzioni più recenti che sono molto comode. D'altra parte, le versioni più vecchie del software possono smettere di

funzionare sui dispositivi più recenti o su quelli che vengono aggiornati. Anche se l'aggiornamento può sembrare un po' dispendioso in termini di tempo, è molto importante, non solo per motivi di sicurezza, ma anche per avere tutte le funzioni più recenti di un determinato dispositivo o software. Una buona pratica sarebbe quella di controllare settimanalmente il software utilizzato per aggiornarlo. Si tratta di un modo semplice e veloce per mantenere i dati più sicuri e migliorare le prestazioni del software utilizzato.

Il software antivirus è un must e dovrebbe essere installato su ogni dispositivo. Non è difficile cadere vittima di un attacco di phishing e al giorno d'oggi, con la crescente diffusione del lavoro a distanza, infettare un computer con un virus può causare un'interruzione obbligatoria del lavoro per giorni o addirittura settimane. L'antivirus è un software che controlla tutti i file o i dati installati o in fase di installazione su un computer. È fatto per determinare se uno dei file presenti su un computer possa essere una potenziale minaccia o causare danni agli utenti e ai loro dispositivi. L'antivirus funziona in due modi diversi. Uno di questi è un metodo **basato sulle firme**, che funziona come un elenco di file noti contenenti malware, pubblicati dalle aziende antivirus. Una volta trovata una corrispondenza tra il file presente nell'elenco e il dispositivo dell'utente, questo viene bloccato. Si tratta di un metodo comune che funziona bene, poiché ogni giorno vengono scoperti migliaia di malware, quindi l'elenco è davvero ricco di dati. L'unico inconveniente di questo metodo è che una volta che il dispositivo dell'utente viene infettato da un virus che non è presente nell'elenco, potrebbe non essere protetto da esso. L'altro modo in cui gli antivirus proteggono i dispositivi è quello **basato sul comportamento**. Questo metodo è più complesso e non è comunemente usato come gli altri, e solo gli antivirus più avanzati lo utilizzano. Come suggerisce il nome, questo metodo studia il comportamento di un determinato file e giudica se questo file può essere pericoloso per il dispositivo. Controlla eventuali tentativi di modificare o crittografare i dati sul dispositivo e li blocca perché li segnala come virus.

Fonte: freepik.com

Gli antivirus proteggono gli utenti non solo bloccando i file presenti sui loro dispositivi, ma la maggior parte di essi blocca anche gli utenti dall'accesso a siti non autorizzati che possono causare possibili minacce ai loro dispositivi. Alcuni di questi programmi possono anche pulire i cosiddetti "file spazzatura" per liberare spazio sul dispositivo. A volte questa procedura può anche aumentare la velocità di elaborazione di un computer o di uno smartphone. L'antivirus è un componente cruciale di ogni dispositivo che rischia di essere infettato da dati dannosi e offre un'ampia gamma di vantaggi che agiscono come una porta chiusa che non lascia entrare alcun virus e che respinge quelli esistenti.

Con tutti questi suggerimenti, è estremamente raro che qualcuno diventi vittima di un attacco informatico e anche se qualcuno tenta di rubare i dati dal computer di qualcuno, è estremamente improbabile che ci riesca.

Capitolo 4 - GDPR e sicurezza dei dati personali

Il Regolamento generale sulla protezione dei dati (GDPR), entrato in vigore il 25 maggio 2018, ha avuto origine negli anni Cinquanta. Fu allora che venne creata la Convenzione sui diritti dell'uomo, gettando le prime basi per la protezione dei dati personali. Tre decenni dopo, con l'avvento dei computer, fu creata la Convenzione sulla protezione dei dati, che dichiarava che la privacy era, di fatto, un diritto umano. Il 24 ottobre 1995 è stata emanata la Direttiva sulla protezione dei dati per regolare le leggi sulla protezione dei dati e il trasferimento dei dati personali al di fuori dell'Unione. 17 anni dopo, è stato proposto un aggiornamento di queste norme e, dopo 4 anni da quella proposta, il Regolamento generale sulla protezione dei dati è stato adottato dal Parlamento europeo per diventare pienamente applicabile in tutta l'Unione europea solo due anni dopo, nel maggio del 2018.

Fonte: freepik.com

L'obiettivo principale del GDPR è quello di dare ai cittadini dell'UE un maggiore controllo sui loro dati personali. Si tratta di un'imponente serie di 99 articoli che regolano le norme sulla protezione dei dati e le modalità di accesso ai dati. Ha sostituito la precedente direttiva sulla protezione dei dati del 1995, perché l'ambiente tecnologico era molto diverso da quello attuale. Al giorno d'oggi, quasi tutti i cittadini europei possiedono almeno uno smartphone e le aziende che offrono beni o servizi online sono diventate popolari quanto i loro equivalenti tradizionali. Con il GDPR, è più facile controllare quali informazioni personali possono essere memorizzate,

condivise o raccolte da varie parti. Queste informazioni possono variare dagli indirizzi IP, alle informazioni sul reddito mensile, alle abitudini alimentari di una persona.

Il GDPR prevede 7 principi fondamentali che dovrebbero essere utilizzati come guida per la gestione dei dati degli utenti. Queste regole possono essere percepite come un quadro di riferimento progettato per mostrare lo scopo principale del regolamento. Tra queste 7 regole ci sono:

- Legalità, equità e trasparenza.

Ciò significa che i dati devono essere conservati ed elaborati in modo legale. Non deve trarre in inganno gli altri utenti sulle modalità di archiviazione e di utilizzo dei dati.

- Limitazione dello scopo.

Suggerisce che i dati personali siano raccolti e conservati per finalità chiare, inequivocabili e legali e che non siano ulteriormente trattati in modo contraddittorio con tali finalità.

- Precisione.

Ciò significa che devono essere adottate tutte le misure ragionevoli per garantire che i dati personali inesatti siano immediatamente cancellati o corretti. I dati personali devono essere accurati e, se necessario, aggiornati.

- Minimizzazione dei dati.

Le organizzazioni non devono raccogliere più dati di quelli necessari dai loro utenti. I dati devono essere adeguati e limitati a quanto necessario per le finalità per cui vengono elaborati.

- Limitazione di stoccaggio.

Significa che i dati non devono essere conservati più a lungo del necessario.

- Integrità e riservatezza.

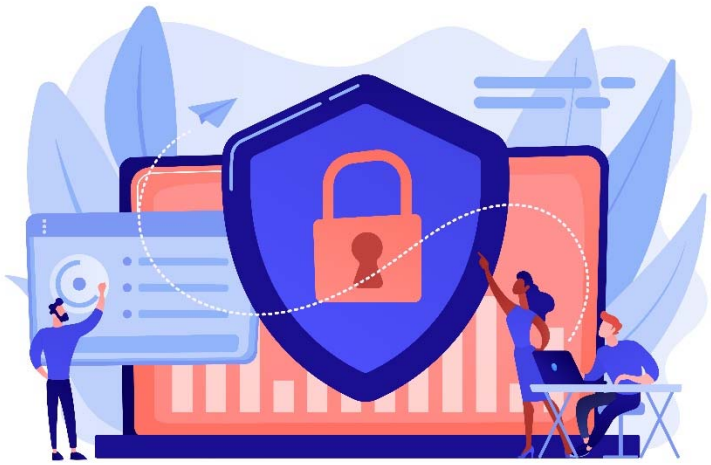
In altre parole, è la sicurezza dei dati memorizzati. Il trattamento deve essere effettuato con misure tecniche o organizzative adeguate a garantire la massima sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illegali e da perdite, distruzioni o danni non intenzionali.

- Responsabilità.

Ciò significa che le aziende devono dimostrare di seguire le regole sopra elencate e garantire di adottare misure per gestire i dati personali in modo etico.

Il GDPR è stato concepito per proteggere gli utenti e i loro dati. Tenendo questo in mente, ha previsto **otto diritti** per le persone. I più significativi sono:

- Il diritto all'informazione sulla raccolta e l'utilizzo dei propri dati personali.
- Il diritto di accedere, rivedere e ricevere una copia dei propri dati personali raccolti ed elaborati da alcune parti.
- Il diritto alla cancellazione dei propri dati personali.



Fonte: freepik.com

Gli altri cinque diritti delle persone sono: il diritto di rettifica, il diritto di limitare il trattamento, il diritto alla portabilità dei dati, il diritto di opporsi e il diritto di non essere sottoposti a un processo decisionale automatizzato.

Grazie alla crescente consapevolezza del valore delle informazioni personali, le persone hanno iniziato a prestare maggiore attenzione alla quantità di dati che forniscono alle aziende e preferiscono scegliere quelle parti che sono trasparenti sulla raccolta dei dati. A causa del GDPR, le aziende devono essere più consapevoli dei dati che raccolgono e di come li proteggono, a causa delle elevate multe associate alla mancata conformità alle norme del GDPR.

La conoscenza del GDPR e delle altre pratiche menzionate in questa guida possono non solo garantire un elevato livello di sicurezza dei dati personali degli utenti, ma anche rendere più difficile per i criminali informatici introdursi nei database delle aziende. Se applicate e comprese correttamente, le password forti e la conoscenza di varie pratiche dannose come il phishing e i virus possono far sentire le persone che lavorano da remoto molto più sicure in questi tempi in cui il telelavoro è diventato una pratica comune in tutto il mondo.

Capitolo 5 - Attività pratica

Pratica 1. Creare una password forte e memorabile.

Una password forte è lunga, complicata e contiene molti simboli, ma è anche facile da ricordare. Con queste premesse, creiamone una con questi semplici passaggi:

1. Pensate a una frase o a una citazione a cui pensate spesso. Ad esempio, una famosa citazione di Wayne Gretzky:
   Si perde il 100% dei tiri che non si fanno.
2. Ora, ricavate un acronimo da questa citazione:
   Y(ou) **m**(iss) **100 p**(ercent) **o**(f) **t(**he) **s**(hots) **y**(ou) **d**('ont) **t**(ake) =
   Ym100potsynt
3. A questo punto, aggiungete dei caratteri speciali. Ad esempio, sostituiamo "1" con "!", "p" con "%", aggiungiamo un trattino basso e cambiamo le maiuscole, in modo che l'effetto finale sia il seguente:
   Ym!00%ots_Ydt

La password sembra complicata, ma se la analizziamo, vediamo che è piuttosto semplice e facile da ricordare. Una buona pratica è quella di allenarsi a scriverla per qualche tempo, in modo che la nostra memoria muscolare ricordi l'ordine dei tasti premuti.

Fonte: freepik.com

Pratica 2. Controllate la vostra casella di posta elettronica per verificare la presenza di SPAM e di eventuali tentativi di phishing.

Abbiamo imparato a conoscere le varie e-mail dannose che ci possono essere inviate e a riconoscerle.

Aprite la casella di posta elettronica e controllate se ci sono pubblicità di prodotti mai sentiti o notifiche di vincite di premi. Controllate anche la presenza di e-mail sospette relative a fatture non pagate o sospensioni del conto. Analizzatele, ma in ogni caso **NON** aprite i link o gli allegati contenuti nei messaggi. Quindi, cancellate i messaggi e pensate a quante e-mail sospette c'erano.

Link utili:

Quanto è sicura la vostra password:
https://www.security.org/how-secure-is-my-password/

Come installare una connessione VPN:
https://www.businessnewsdaily.com/15710-how-to-install-a-vpn-connection.html

4. Bibliografia

Anderson, S. (2022). *Cos'è il phishing? Guida con esempi per il 2022*. SafetyDetectives. Recuperato il 10 maggio 2022, da https://www.safetydetectives.com/blog/what-is-phishing-and-how-to-protect-against-...

Awati, R. e Teravainen, T. (2021). *Cos'è lo spam via e-mail e come combatterlo?* SearchSecurity. Recuperato il 9 maggio 2022, da https://www.techtarget.com/searchsecurity/definition/spam?msclkid=9aeb4557cf8211ec82e6cfc07708ec54.

Barracuda. (2020). *Spear Phishing: Top Threats and Trends* (Vol. 5). Barracuda. Recuperato il 10 maggio 2022, da https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5...

Castagna, R., & Lavery, T. (2021). *Regolamento generale sulla protezione dei dati (GDPR)*. WhatIs.Com. Recuperato il 24 giugno 2022, da https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR.

Cheema, A. N. e Aamir, R. (2021). Tendenze dei crimini informatici. *Proc. 18th International Conference on Statistical Sciences*, *35*, 261-269. https://www.researchgate.net/profile/Muhammad-Suhail-6/publication/353070981_Comparison_of_Ridge...

Chng, S., Han Yu, L., Kumar, A., & Yau, D. (2022). Tipi di hacker, motivazioni e strategie: Un quadro completo. *Computers in Human Behavior Reports*, *5.* https://doi.org/10.1016/s2451-9588(22)00018-5

Esperti di marketing digitale - Comitato di revisione editoriale. (2021). *L'importanza dell'aggiornamento*. CHE! Company. Recuperato il 24 giugno 2022, da https://www.thatcompany.com/the-importance-of-updating...

D'Mello, Y. (2018). *Come siamo arrivati qui? Una breve storia del GDPR*. AiThority. Recuperato il 24 giugno 2022, da https://aithority.com/technology/analytics/how-did-we-get-here-a-brief-history-of-the-gdpr/.

Edwards, R. (2022). *Come posso proteggere la mia connessione a Internet?* SafeWise. Recuperato il 24 giugno 2022, da https://www.safewise.com/online-security-faq/secure-internet-connection/.

Elvin, A. E., Sundström, F., & von Heland, W. (2021). *Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations* (tesi di laurea magistrale). Dipartimento di Informatica, Lund School of Economics and Management, Lund University. Recuperato il 24 giugno 2022 da https://lup.lub.lu.se/student-papers/search/publication/9052971.

Tecnologia dell'informazione FIT. (2022). *Cos'è l'antivirus e perché è importante?* Recuperato il 24 giugno 2022, da https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/.

Fogg, S. (2022). *Che cos'è il GDPR? Le basi del Regolamento generale sulla protezione dei dati dell'UE*. Termly. Recuperato il 24 giugno 2022, da https://termly.io/resources/articles/what-is-gdpr/.

Fruhlinger, J. (2020). *Il ransomware spiegato: Come funziona e come rimuoverlo*. CSO Online. Recuperato l'11 maggio 2022, da https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it...

Gajić, A. (2022). *Statistiche sullo spam*. 99firms. Recuperato il 9 maggio 2022, da https://99firms.com/blog/spam-statistics/?msclkid=18264839cf8b11ec8144c5ced7add618.

Regolamento generale sulla protezione dei dati (GDPR) - Testo legale ufficiale. (2019). Regolamento generale sulla protezione dei dati (GDPR). Recuperato il 24 giugno 2022, da https://gdpr-info.eu/.

Gibson, K. (2022). *6 casi famosi di furto d'identità negli ultimi anni*. Eroi della sicurezza domestica. Recuperato il 12 maggio 2022, da https://www.homesecurityheroes.com/famous-identity-theft-cases/.

Gupta, M. (2021). Il furto di identità nel cyberspazio in India. *International Journal of Research Publication and Reviews*, *2*(7), 1700-1701. https://www.ijrpr.com/uploads/V2ISSUE7/IJRPR791.pdf

Hiley, C. (2021). *Breve storia della sicurezza informatica e dell'hacking*. CyberNews. Recuperato l'11 maggio 2022, da https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/?msclkid=ebaaa52cd10911ecbb48b6bc018d0384.

Jančis, M. (2022). *Come creare una password buona e forte*. CyberNews. Recuperato il 16 giugno 2022, da https://cybernews.com/best-password-managers/how-to-create-a-strong-password/.

Janssen, D. (2022). *La VPN spiegata: Come funziona? Perché usarla?* VPNoverview.com. Recuperato il 1° giugno 2022, da https://vpnoverview.com/vpn-information/what-is-a-vpn/.

Johansen, A. G. (2018). *Cosa fare in caso di furto d'identità: 14 passi*. LifeLock. Recuperato il 12 maggio 2022, da https://www.lifelock.com/learn/identity-theft-resources/do-these-things-immediately-if-your-identity-has-been-stolen.

Lopez, A. (2021). *I 10 motivi principali per cui un antivirus è importante*. Business 2 Community. Recuperato il 24 giugno 2022, da https://www.business2community.com/cybersecurity/top-10-reasons-why-an-antivirus-is-important...

Malwarebytes. (n.d.). *Che cos'è lo spam?* Recuperato l'11 maggio 2022, da https://www.malwarebytes.com/spam...

Martens, B. (2021). *La guida definitiva alla sicurezza di Internet per gli anziani (2022)*. SafetyDetectives. Recuperato il 24 giugno 2022, da https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors/?msclkid=9e7ed272cf5f11ecbe3d195abee11879.

Milasi, S., González-Vázquez, I., & Fernández-Macías, E. (2020). *Il telelavoro nell'UE prima e dopo il COVID-19: Dove eravamo e dove stiamo andando*. Centro comune di ricerca. Recuperato il 24 giugno 2022, da https://joint-research-centre.ec.europa.eu/system/files/2021-06/...

Minahan, B. (2020). *Come creare una password forte in 6 semplici passi*. aNetworks. Recuperato il 1° giugno 2022, da https://www.anetworks.com/how-to-create-a-strong-password-2021/.

Mitra, A. (2017). *Cos'è uno spambot e come fermare gli spambot?* TheSecurityBuddy. Recuperato l'11 maggio 2022, da https://www.thesecuritybuddy.com/anti-spam/what-is-spambot-and-how-to-stop-spambots...

Molinaro, D. (2022). *Come funziona l'autenticazione a due fattori (2FA)?* Avast. Recuperato il 1 giugno 2022, da https://www.avast.com/c-how-does-two-factor-authentication-work...

Movassagh, N. (2021). *Consapevolezza e percezione delle varianti di phishing da parte degli studenti di Polizia, Informatica e Criminologia della Canterbury Christ Church University.* (Tesi di Master). Canterbury Christ Church University School of Law. https://repository.canterbury.ac.uk/item/8yq89/awareness-and-perception-of-phishing-variants-from-policing-computing-and-criminology-students...

Peterson, S. (2019). *La guida definitiva per la sicurezza e la privacy online nel 2020*. The Hack Post. Recuperato il 1° giugno 2022, da https://thehackpost.com/the-ultimate-guide-for-online-security-and-privacy-in-2020.html.

Proofpoint. (n.d.). *Cos'è lo spoofing delle e-mail? Definizione ed esempi*. Recuperato il 24 giugno 2022, da https://www.proofpoint.com/us/threat-reference/email-spoofing?msclkid=df4910a2d03511ecb958bcffa531b6ab.

Spoofing e Phishing. (2022). Federal Bureau of Investigation. Recuperato il 10 maggio 2022, da https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing?msclkid=8cb3cf19d04d11ecb7c47a9f8893c5e8.

Tanwar, R., Choudhury, T., Zamani, M., Gupta, S. e Tajpour, A. (2021). Sicurezza delle informazioni e ottimizzazione. In *Sicurezza delle informazioni e ottimizzazione* (pp. 25-26). CRC Press. Recuperato il 10 maggio 2022 da https://books.google.nl/books?id=...

Contributori di TechFunnel. (2020). *Le più comuni tecniche di hacking per principianti*. Techfunnel. Recuperato l'11 maggio 2022, da https://www.techfunnel.com/information-technology/hacking-techniques/?msclkid=94348692d12111eca373f0ead6ff7fe9.

Tschabitscher, H. (2021). *Qual è un esempio di e-mail di spam?* Lifewire. Recuperato il 9 maggio 2022, da https://www.lifewire.com/what-and-why-spam-email-1173993#toc-what-are-some-examples-of-spam.

Tsonchev, A. (2020). *Sei delle più grandi minacce alla sicurezza della forza lavoro remota*. TechRadar. Recuperato il 24 giugno 2022, da https://www.techradar.com/news/six-of-the-biggest-security-threats-facing-the-remote-workforce?msclkid=9e80a80ccf5f11ec92c0ce7275373494.

Williams, L. (2022). *Che cos'è l'hacking? Tipi di hacker | Introduzione al crimine informatico*. Guru99. Recuperato il 24 giugno 2022, da https://www.guru99.com/what-is-hacking-an-introduction...

Fonte immagine del frontespizio: freepik.com