CYBERCHOLOGY
L'ELEMENTO UMANO

Costruire team resilienti
grazie alla Cybersecurity

ESET®

The Myers-Briggs Company

La sicurezza informatica è oggigiorno l'aspetto più importante da tenere in considerazione per qualsiasi attività. La maggior parte delle organizzazioni per un motivo o l'altro viaggia online, e la tecnologia è al centro della maggior parte delle funzioni aziendali. Con la pandemia da COVID-19, che ha agito da catalizzatore per una digitalizzazione accelerata in quasi tutti i settori industriali, è aumentata la pressione di mostrarsi resilienti e dinamici di fronte al cambiamento.

Per questo articolo di Cyberchology, **ESET**, leader globale nella sicurezza IT, ha collaborato con **The Myers-Briggs Company**, la più importante organizzazione di psicologia aziendale, per esplorare il ruolo essenziale che i dipendenti svolgono nel mantenere le organizzazioni al sicuro dalle minacce online, indagando sul collegamento tra il tipo di personalità e le vulnerabilità alla criminalità informatica. Il documento esamina anche gli atteggiamenti e le esperienze di oltre 100 responsabili della sicurezza informatica durante il lockdown per il COVID-19.

Quando il governo, nel marzo 2020, ha adottato misure di lockdown, il mondo del lavoro è cambiato radicalmente in modi che la maggior parte delle persone non avrebbe potuto immaginare. Ne è risultata l'implementazione in massa del lavoro a distanza, registrando una maggiore dipendenza dalla tecnologia come mai prima d'ora, andando ad intaccare conseguentemente le infrastrutture tecnologiche di molte aziende. I sistemi IT centrali sono stati sostituiti da una rete di singole connessioni individuali; ciascuno ha mostrato un maggiore senso di responsabilità nell'uso della propria tecnologia e nelle esigenze di sicurezza informatica. Un sistema di sicurezza frammentato non solo rende vulnerabili le aziende, ma implica anche gravi rischi in termini di fiducia dei dipendenti nella gestione della sicurezza informatica.

Il panorama della sicurezza informatica è in costante evoluzione per mitigare la crescente sofisticazione degli attacchi cibernetici che con il COVID-19 sono notevolmente aumentati. La ricerca di ESET ha rilevato che, dall'inizio del lockdown, la criminalità informatica è aumentata del 63% e che le aziende si trovano proprio nel mirino a causa della dispersione della forza lavoro. Come esploreremo in questo documento, il lavoro da remoto è una realtà destinata a durare, e le aziende dovranno adattare di conseguenza le proprie strategie di cybersecurity. La sicurezza informatica di un'organizzazione è nelle mani di ogni dipendente che appoggia le dita sulla tastiera e non può essere una faccenda che riguarda solo il reparto IT o i vertici aziendali.

In un momento in cui le aziende si affidano alla resilienza, gli attori malintenzionati sfruttano le vulnerabilità della sicurezza legate al lavoro a distanza. Semplici misure come l'utilizzo di un'interfaccia desktop virtuale o la crittografia per i file sensibili possono ridurre le probabilità di riuscita di un attacco. La ricerca di ESET per questo rapporto ha rivelato che più della metà delle aziende non disponeva di misure di continuità per una potenziale pandemia prima dell'insorgere del COVID-19; inoltre, mentre l'80% ha dichiarato di avere una strategia di lavoro a distanza, solo un quarto delle aziende la considera effettivamente efficace.

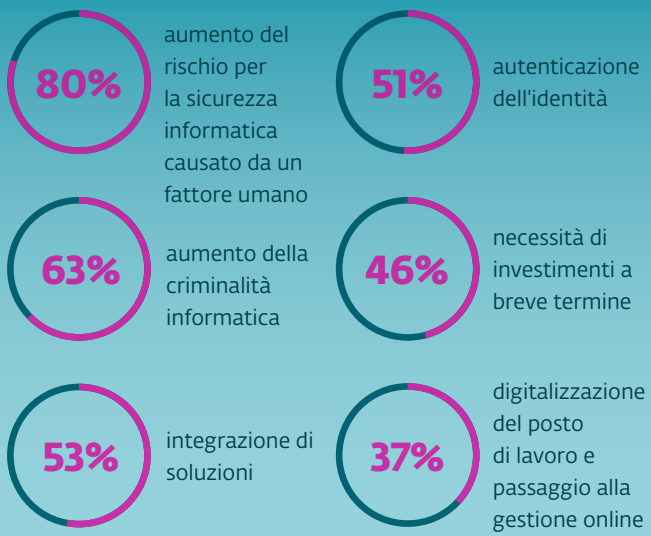
Se le aziende devono prosperare piuttosto che limitarsi a sopravvivere, è fondamentale una strategia di sicurezza informatica olistica che tenga conto delle singole personalità accanto a una soluzione software completa per gli endpoint. Con così tanta responsabilità che grava sui dipendenti che lavorano da diversi luoghi, dispositivi e reti, è inoltre essenziale la consapevolezza di buone pratiche di sicurezza informatica e una formazione personalizzata a tal riguardo. Questo documento analizzerà i motivi e le modalità tramite cui i team HR e Tech dovrebbero collaborare per costruire sistemi IT, strategie e team resilienti, per un business resiliente.

Le sfide della sicurezza informatica

Prima del COVID-19, gli attacchi informatici erano già in aumento; la pandemia e il lockdown hanno solo aumentato questo rischio. Dalle truffe di phishing ai malware correlati al COVID-19, i criminali informatici hanno individuato le vulnerabilità innate della forza lavoro dispersa e dei sistemi IT. I CISO hanno segnalato un aumento del 63% della criminalità informatica durante il lockdown; questo avveniva mentre molte aziende già faticavano a rimanere a galla o ad adattare rapidamente i loro modelli operativi e di business per sopravvivere. La pandemia ha cambiato il mondo del lavoro così come lo conoscevamo e le aziende dovranno adattare le loro strategie di sicurezza informatica per rispecchiare tali cambiamenti.

Oltre ai costi operativi e di reputazione che un attacco di per sé implica, le sanzioni comminate dagli organi di regolamentazione sono in aumento. Prima della pandemia, l'Ufficio del garante per la trasparenza (ICO) ha **comminato due sanzioni multimilionarie** alla British Airways e Marriott, in base alle norme del Regolamento generale sulla protezione dei dati (GDPR). Anche se le grandi aziende hanno risorse sufficienti per affrontare le conseguenze di un attacco, le piccole imprese rischiano di paralizzarsi.

Principali sfide segnalate dalle aziende durante il lockdown da COVID-19



La ricerca di ESET ha rivelato che per il 75% delle aziende, la metà delle attività è svolta da dipendenti che lavorano a distanza e che non lo facevano prima del COVID-19. Al contrario, meno del 25% delle imprese ha dichiarato di non essere in grado di lavorare perché non può realizzare i propri progetti a distanza. Anche se alla fine i dipendenti torneranno in ufficio, il lavoro a distanza in qualche forma resterà. Molte aziende sono state in grado di operare a distanza durante il lockdown, anche se con sistemi e processi adattati. Anche se la transizione è stata improvvisa, le imprese sono state costrette a innovarsi, a dimostrazione del fatto che è realmente possibile svolgere gran parte del lavoro da remoto.

Lo smart working ha portato flessibilità, ma ha anche modificato drasticamente i processi e i sistemi aziendali al fine di soddisfare la distribuzione della forza lavoro. Il rapporto dei dipendenti con i reparti IT, e viceversa, è cambiato. La collaborazione e il lavoro di squadra avvengono virtualmente; inoltre, la mancanza di una relazione faccia a faccia può ostacolare i canali diretti di comunicazione

Alcune delle misure di sicurezza di base adottate in ufficio devono essere utilizzate anche a casa, come l'obbligo per i lavoratori da remoto di utilizzare l'autenticazione a più fattori o una VPN per accedere alle reti interne. Ricordare ai lavoratori di abilitare gli aggiornamenti automatici e controllare la sicurezza delle proprie reti Wi-Fi è fondamentale come prima linea di difesa contro i criminali informatici.

Nel valutare le sfide associate ai dipendenti che lavorano da casa, l'80% delle aziende ha affermato che un aumento del rischio di sicurezza informatica causato da fattori umani le ha sottoposte a un qualche tipo di sfida. Inoltre, il 37% delle aziende ha dichiarato che la digitalizzazione del posto di lavoro e il passaggio a una postazione online è stato impegnativo. La concomitanza di sistemi IT aziendali frammentati e la mancanza di una sicurezza centrale, un improvviso passaggio al lavoro a distanza e un clima globale di stress e preoccupazione costituiscono un terreno ideale per un attacco informatico.

L'impatto dello stress sulle abitudini di sicurezza informatica

La crisi di coronavirus ha aggiunto altro stress e preoccupazioni alla nostra quotidianità. Concentrarsi e rimanere motivati sul lavoro può essere difficile e i dipendenti più vulnerabili sono particolarmente esposti alle minacce informatiche. Nel rapporto '**Personality and stress in a virtual world**', The Myers-Briggs Company ha rilevato che il 47% degli intervistati si dichiarava alquanto o molto preoccupato circa la propria capacità di gestire lo stress durante la crisi da coronavirus, con l'economia in recessione e una preoccupazione costante circa la salute di familiari e amici. Una pressione costante influenza in modo differente le diverse tipologie di personalità, e si manifesta a seconda delle modalità di ognuno di gestire lo stress e di reagire a determinate situazioni. I dipendenti già stressati possono essere più propensi a farsi prendere dal panico e a cliccare su un link dannoso, oppure la mancanza di attenzione ai dettagli può portare a una violazione della sicurezza non propriamente segnalata al reparto IT.

Saperne di più sul proprio profilo MBTI può essere d'aiuto. Ecco alcuni elementi che riguardano ciascun tipo, sulla base della parte più utilizzata della personalità, il Core Character™, e il modo in cui ogni tipo tende a comportarsi quando è sotto pressione.

Attivista (ESTP e ESFP)

Agenti di stress

- Mancanza di stimoli e entusiasmo
- Compiti teorici e astratti senza imminente applicazione pratica
- Confinamento fisico, ad esempio a causa di malattie o altre circostanze

Comportamento sotto stress quotidiano

- Continua ricerca di stimoli esterni ed eccitazione
- Può comportarsi in modo impulsivo o pericoloso o eccessivamente indulgente
- Vive solo nel momento presente e non prende alcuna decisione

Esploratore (ENTP & ENFP)

Agenti di stress

- Persone che dicono "non funzionerà mai"
- Troppi dettagli apparentemente irrilevanti
- Mancanza di varietà; non poter fare qualcosa di nuovo

Comportamento sotto stress quotidiano

- Condivide idee sempre più impraticabili con sempre più persone
- Incapace di prendere le cose sul serio, diventa distruttivamente "giocoso"
- Non si sentirà vincolato dalle decisioni

L'impatto dello stress sulle abitudini di sicurezza informatica

Direttore (ESTJ e ENTJ)

Agenti di stress

- Persone, sistemi o organizzazioni inefficienti
- Mancanza di determinazione, non essere in grado di prendere decisioni
- Doversi concentrare sui sentimenti delle persone, piuttosto che sul ruolo

Comportamento sotto stress quotidiano

- Diventa eccessivamente direttivo, energico, persino aggressivo
- Prende decisioni affrettate e le impone agli altri
- Respinge le evidenze/altre opinioni che non corrispondono al suo punto di vista

Nutrice (ESFJ e ENFJ)

Agenti di stress

- Conflitto con gli altri e tra gli altri
- Mancanza di calore, in quanto la sua cordialità non viene contraccambiata
- Ingiustizia nel mondo in generale

Comportamento sotto stress quotidiano

- Diventa effusivo e troppo amichevole
- Esigente nell'ottenere la soddisfazione dei propri e altrui bisogni
- Interpreta le situazioni sulla base dei propri valori, ignorando ogni evidenza

Conservatore (ISTJ e ISFJ)

Agenti di stress

- Dover agire senza informazioni o piani dettagliati e pratici
- Veder respinte le lezioni acquisite sulla base della sua esperienza passata
- Cambiare le cose che già funzionano

Comportamento sotto stress quotidiano

- Cerca ossessivamente quell'unica informazione importante
- Si ritira dal mondo esterno
- Non riesce a prendere una decisione fino a quando non ha trovato tutte le informazioni

L'impatto dello stress sulle abitudini di sicurezza informatica

Visionario (INTJ e INFJ)

Agenti di stress

- Non ha il tempo di pensare alle opzioni prima di rispondere
- Le sue idee ben ponderate vengono respinte o ignorate
- Persone disorganizzate e supponenti

Comportamento sotto stress quotidiano

- Si ritira, per costruire idee sempre più complesse nella sua testa
- Questi modelli possono diventare sempre più distanti dalla realtà
- Incapace di agire fino a quando ogni possibilità non è stata esplorata

Analista (INTP & ISTP)

Agenti di stress

- Le sue soluzioni accuratamente ragionate vengono respinte o ignorate
- Decisioni illogiche che non sono state ponderate
- Eccessive manifestazioni di approvazione o di empatia da parte di altri

Comportamento sotto stress quotidiano

- Si ritira per risolvere i problemi da solo
- Si fissa sulla ricerca dell'unica soluzione corretta
- Ignora le altre persone, prende decisioni senza informarle

Coscienzioso (ISFP & INFP)

Agenti di stress

- Persone che ignorano, mettono da parte o contravvengono i propri valori
- Lavorare in un contesto in contrasto con questi valori
- Persone o organizzazioni inflessibili e non pensanti

Comportamento sotto stress quotidiano

- Si ritira in un soliloquio
- Lavora in modo ossessivo basandosi su decisioni che si adattano ai suoi valori
- Ignora i fatti che non si adattano all'immagine che si è raffigurato

Resilienza

Ora che ci troviamo ad affrontare un cambiamento di paradigma nella nostra vita lavorativa e domestica, la resilienza è più importante che mai. Con oltre il 50% delle aziende che pianificano di mantenere in qualche modo le modifiche apportate durante la pandemia da COVID-19, il modo in cui le organizzazioni costruiranno la propria resilienza all'interno dei sistemi IT e dei team deve essere la priorità assoluta.

Avere dipendenti competenti e istruiti sulle migliori pratiche di sicurezza informatica costituisce la base per una strategia di resilienza. Come emerso dalla **ricerca sul Catphishing di Eset, che ha esaminato le abitudini in materia di sicurezza informatica di 2.000 dipendenti nel Regno Unito, il 69% dei britannici afferma di essere preoccupato per la propria sicurezza informatica, ma non ha idea di cosa fare al riguardo; il 68% delle persone fra 25-54 anni e il 55% degli over 55 ammette di avere dubbi o timori sulla sicurezza informatica.** Anche se i dipendenti nella fascia di età compresa tra i 16 e i 24 anni mostrano meno preoccupazioni, ciò non significa necessariamente che siano meno propensi a essere vittime di un attacco, perché la disinvoltura, la mancanza di competenze e di formazione possono rendere le aziende vulnerabili.

"Dalla ricerca Catphishing di ESET, che ha esaminato le abitudini di sicurezza informatica di 2.000 dipendenti nel Regno Unito, è emerso che il 69% degli inglesi sono preoccupati per la loro sicurezza informatica, ma non hanno idea di cosa fare al riguardo, con il 68% dei 25-54 anni e il 55% degli over 55 che ammette di avere preoccupazioni o timori sulla sicurezza informatica. "

Nonostante un evidente aumento delle minacce alla sicurezza informatica e la mancanza di competenze dei dipendenti, il 40% dei CISO ha riferito che il COVID-19 non ha prodotto alcun impatto sul budget riservato alla sicurezza IT, rispetto a quanto originariamente previsto. Questa noncuranza può esporre le aziende a futuri attacchi informatici senza le adeguate risorse per mitigarli. I team IT devono ripensare l'intera gestione della sicurreza, ora che il lavoro a distanza è diventato la norma e non l'eccezione.

La stragrande maggioranza degli attacchi informatici ha successo non per l'abilità dell'hacker, ma per errori umani e noncuranza. Infatti, l'80% delle aziende ha riferito che una sfida significativa durante il COVID-19 è stata l'aumento del rischio di sicurezza informatica causato dal fattore umano. Le modalità con cui le persone tendono ad acquisire le informazioni e comunicare possono determinare il modo in cui i diversi membri del team si approcciano alla sicurezza informatica, in quanto tutti i tipi di personalità hanno diversi punti di forza e debolezza che possono influire sull'esito di un attacco informatico.

L'indicatore Myers-Briggs (MBTI) analizza quattro aree della personalità: estroversione o introversione, sensitività o intuizione, ragionamento o sentimento, giudizio o percezione. Inoltre, studia il modo in cui queste aree si combinano dinamicamente per delineare l'intera persona. Ad esempio, chi ha una personalità più estroversa (elabora le proprie idee parlandone) tende a essere più vulnerabile alla manipolazione, all'inganno e alla persuasione da parte dei criminali informatici, mentre chi ha una preferenza per la sensitività (osserva e ricorda i dettagli) è più propenso a individuare gli attacchi di phishing, ma anche ad assumersi rischi in fatto di sicurezza informatica. Nonostante le diverse preferenze della personalità non garantiscano la consapevolezza o la conoscenza della sicurezza informatica, possono essere un punto di partenza per individuare i punti deboli della sicurezza informatica.

Se l'errore umano è responsabile della maggior parte degli attacchi informatici, le aziende non possono ignorare l'impatto dei tratti e delle caratteristiche personali sulle abitudini di sicurezza informatica dei dipendenti. La sicurezza informatica è stata a lungo considerata di responsabilità esclusiva dei reparti IT; tuttavia, per costruire una strategia di sicurezza informatica olistica che tenga conto del fattore umano, i dipartimenti IT e HR devono collaborare. Utilizzando test psicometrici e strumenti di autoconsapevolezza, i reparti HR possono aiutare a identificare la composizione dei team e a individuare le potenziali vulnerabilità. I reparti IT possono utilizzare questo informazioni per creare protocolli di sicurezza completi e una strategia informatica proattiva, così da essere sempre un passo avanti rispetto alle potenziali minacce.
Tenere conto delle preferenze della personalità può rendere la formazione sulla sicurezza informatica più coinvolgente ed efficace, facilitare l'attuazione delle buone pratiche, monitorate con controlli e aggiornamenti regolari creati in base alle personalità dei dipendenti. Questo è un aspetto

Resilienza

particolarmente importante se si considera il passaggio massivo al lavoro a distanza da parte di molte imprese. Poiché i team IT hanno meno visibilità e accesso fisico ai singoli dipendenti, garantire che la forza lavoro sia adeguatamente istruita sulle migliori pratiche di sicurezza informatica è fondamentale per proteggere l'intera organizzazione.

Il panorama della sicurezza informatica si è evoluto in modo significativo negli ultimi 12 mesi, poiché alcune minacce si sono camuffate per poi riemergere sotto con varie sembianze. La maggior parte di queste minacce può essere sostanzialmente identificata come malware o phishing; gli attacchi dannosi per i sistemi delle organizzazioni possono essere evitati quando le persone comprendono e sono consapevoli del tipo di attacco a cui potrebbero essere vulnerabili. Così facendo, le organizzazioni possono essere proattive nel mitigare i rischi informatici.

Phishing

Il phishing, comunemente effettuato via e-mail, è una truffa online in cui il criminale informatico si spaccia per un'entità affidabile, così da ottenere i dati sensibili riguardanti la vittima.

Il gruppo Sednit, conosciuto anche come APT28, Fancy Bear, Sofacy o STRONTIUM - è attivo almeno dal 2004 e negli ultimi anni ha fatto spesso notizia. Il 20 agosto 2019, il gruppo ha lanciato una nuova campagna indirizzata alle vittime abituali: ambasciate e ministeri degli esteri dei Paesi dell'Europa orientale e dell'Asia centrale. **L'ultima campagna** è iniziata con un' e-mail di phishing contenente un allegato dannoso in grado di lanciare una lunga catena di downloader, per poi concludersi con una backdoor. I tipi di personalità come ENFP e ENTP possono risultare più vulnerabili agli attacchi di phishing come quelli usati dal gruppo Sednit che utilizzano una semplice email. Nonostante che sia gli ENFP che gli ENTP possano essere esperti di informatica, la migliore pratica per questi tipi di personalità richiede di prendersi il tempo necessario per verificare la validità delle e-mail ricevute prima di rispondere e di essere sospettosi nei confronti di e-mail dal contenuto intrigante o dall'appeal emotivo.

ENFP

- Gli ENFP sono tra i primi a rendersi conto quando è in atto un nuovo processo di sicurezza
- Prenderanno molto sul serio la sicurezza informatica, se essa diventerà uno dei loro valori

Suggerimenti sulla sicurezza informatica:

- Siate sospettosi delle e-mail che suscitano un appeal emotivo
- Fermatevi a pensare prima di cliccare

ENTP

- Gli ENTP esperti di informatica si sforzeranno di essere competenti ed evitare errori "stupidi"
- Propensione a far sì che le cose avvengano (anche se questo può significare fare uno strappo alla regola)

Suggerimenti sulla sicurezza informatica:

- Se compromettete la sicurezza, altri potrebbero considerarvi incompetenti
- Cautela nel leggere le e-mail: potreste notare qualcosa

ESTP

- Una volta convinti che la sicurezza informatica è importante, gli ESTP possono individuare rapidamente quando qualcosa non va e agire immediatamente

Suggerimenti sulla sicurezza informatica:

- La sicurezza informatica è importante e le regole valgono anche per voi
- Ottenete esempi specifici di ciò che si può fare in modo diverso e agite di conseguenza

ESFP

- Gli ESFP agiranno rapidamente se si accorgono che qualcosa non va
- In generale, seguono le regole e i criteri di sicurezza IT

Suggerimenti sulla sicurezza informatica:

- Non fidatevi di una rete pubblica per i dati sensibili, anche se ha una password
- Non dare nulla per scontato: vale la pena essere vigili e magari perfino diffidenti

ISTJ

- È probabile che gli ISTJ individuino discrepanze ed errori nelle e-mail di phishing
- In generale, seguono le regole e i criteri di sicurezza IT

Suggerimenti sulla sicurezza informatica:

- Non utilizzate solo variazioni sulla/e stessa/e password
- State all'erta. Le esperienze passate non dovrebbero essere la vostra unica guida

ISFJ

- È probabile che gli ISFJ individuino discrepanze ed errori nelle e-mail di phishing
- È improbabile che venga colpito due volte dallo stesso attacco informatico

Suggerimenti sulla sicurezza informatica:

- Non fidatevi di una rete pubblica per i dati sensibili, anche se ha una password
- Fate attenzione su chi potete fidarvi. Online, le persone potrebbero non essere quello che pensate

Malware

I malware si manifestano in una grande varietà di forme, tra cui virus, spyware e ransomware; ognuna in grado di compromettere il computer e i dati. **DePriMon è un recente esempio di downloader** dannoso, con diversi stadi di infezione che utilizza molte tecniche non tradizionali. **Per raggiungere l'obiettivo, il malware registra un nuovo Port Monitor locale; questo è un trucco che rientra nella tecnica dei "Port Monitors" all'interno della knowledgebase di MITRE ATT&CK. Di conseguenza, il malware utilizza il nome "Windows Default Print Monitor", camuffando in questo modo la sua natura dannosa.**

I tipi di personalità come ESTJ e ENTJ possono essere più vulnerabili ai download dannosi, camuffati da software o moduli legittimi. Sebbene di solito sono i migliori nel rispetto del protocollo di sicurezza, questa tendenza potrebbe indurli a prendere una decisione rapida per amore dell'efficienza. Questi tipi di personalità dovrebbero concentrarsi sull'acquisizione di tutte le informazioni rilevanti prima di prendere decisioni e assicurarsi di consultare coloro che hanno una conoscenza più ampia in materia di sicurezza informatica.

ESTJ

- È probabile che gli ESTJ seguano le regole e i processi di sicurezza IT e cerchino di migliorarli
- In generale, prendono sul serio la sicurezza informatica

Suggerimenti sulla sicurezza informatica:

- Non fare sempre le cose allo stesso modo e non usare le stesse password
- Non cedete alla tentazione di prendere scorciatoie per essere più efficienti

ENTJ

- Gli ENTJ sono tra i primi a rendersi conto quando è in atto un nuovo processo di sicurezza
- Si terranno aggiornati e porranno domande per comprendere i problemi di sicurezza

Suggerimenti sulla sicurezza informatica:

- Non abbiate fretta di cambiare i processi di sicurezza; prima è meglio conoscerli più a fondo
- Evitate di scavalcare gli altri se hanno una conoscenza più approfondita in fatto di sicurezza IT

ESFJ

- Gli FSEJ sono consapevoli dei criteri di sicurezza informatica e li seguono coscienziosamente
- Creano abitudini di sicurezza e le usano per seguire le regole in modo efficiente

Suggerimenti sulla sicurezza informatica:

- Fate attenzione su chi potete fidarvi. Online le persone potrebbero essere diverse da quello che sembrano
- Non fare sempre le cose allo stesso modo e non usare le stesse password

ENFJ

- Seguiranno le regole quando saranno chiare
- Prenderanno sul serio la sicurezza quando saranno consapevoli degli effetti delle violazioni sulle persone

Suggerimenti sulla sicurezza informatica:

- Siate proattivi rispetto alla sicurezza IT, anche a casa vostra
- Non riutilizzate le password e non utilizzate la stessa password per applicazioni diverse

INFJ

- Gli INFJ possono complicare eccessivamente le cose e cercare significati nascosti. Questo può essere un vantaggio per la sicurezza informatica

Suggerimenti sulla sicurezza informatica:

- Se qualcosa non va, controllate, controllate e ricontrollate
- Non dimenticate di controllare i dettagli: sono importanti!

INTJ

- Gli INTJ danno grande valore alla conoscenza e si sforzano di essere capaci e competenti
- In generale, seguono le regole e i criteri di sicurezza IT

Suggerimenti sulla sicurezza informatica:

- Non è detto che voi sappiate tutto, anche se le regole sembrano inutili
- Se volete essere competenti, ricordatevi di controllare le e-mail nel dettaglio

Tendenze comuni

IoT

Le nostre vite sono sempre più invase da dispositivi, spesso tutti collegati tra loro e che funzionano con le stesse reti e gli stessi sistemi connessi. Sia a casa sia al lavoro, questi dispositivi collegati possono creare vulnerabilità a interi sistemi se non sono adeguatamente protetti, come ad esempio un telefono personale o uno smartwatch che si collega a una rete di lavoro. Recentemente, i ricercatori hanno scoperto che per un modello di smartwatch era possibile accedere alla posizione, al numero di telefono, alle **foto e alle conversazioni di ben oltre 5.000 ragazzi**, a causa della mancata protezione dei loro server da parte del produttore.
I tipi di personalità come ISTP e INTP possono essere vulnerabili quando si trovano a gestire i dispositivi collegati, anche se normalmente sono attenti a rispettare le regole. La pratica migliore per questi tipi di personalità è quella di non dare sempre per scontato di saperne di più, e di assicurarsi di non ignorare le regole o i protocolli perché si pensa che non siano applicabili a loro.

ISTP

- Gli ISTP nutrono una sana sfiducia nei confronti dei sistemi e delle altre persone online
- Sono propensi a seguire le regole di sicurezza IT quando hanno una logica

Suggerimenti per la sicurezza informatica:

- Sforzatevi di trovare le ragioni di una regola prima di concedervi uno strappo
- Fare le cose a modo vostro e impulsivamente può essere rischioso

INTP

- Molti INTP sono a conoscenza dei problemi di sicurezza informatica
- Gli INTP sono particolarmente consapevoli del fatto che chiunque può essere bersaglio di attacchi cibernetici

Suggerimenti sulla sicurezza informatica:

- Trovate le regole di sicurezza IT per la vostra organizzazione e seguitele
- Non sempre sapete tutto! Le regole ci sono per un motivo

INFP

- È improbabile che gli INFP facciano scelte improvvise e rischiose
- Se sono consapevoli degli effetti di una scarsa sicurezza sugli altri, riescono a comprendere la necessità delle regole

Suggerimenti sulla sicurezza informatica:

- La vostra organizzazione avrà delle regole di sicurezza informatica. Seguitele
- Per evitare di danneggiare gli altri, assumetevi la responsabilità personale della sicurezza informatica

ISFP

- Gli ISFP prendono sul serio la sicurezza informatica e sono attenti al loro comportamento online
- In generale, seguono le regole e i criteri di sicurezza IT

Suggerimenti sulla sicurezza informatica:

- Fermatevi un istante prima di cliccare
- Ricordate che le persone online, anche gli amici, possono non essere chi o cosa sembrano

Leadership

Una leadership forte è il fulcro di un business resiliente. Proprio come una forza lavoro fisicamente dispersa ha avuto un impatto sulla natura della sicurezza informatica, questo ha altrettanto influenzato il modo di concepire una leadership efficace. In tempi di crisi ci si rivolge ai propri leader per essere motivati e rassicurati; inoltre, la loro capacità di trasmettere una reale attenzione e consapevolezza relativamente alla sicurezza informatica è una parte essenziale per mantenere le aziende al sicuro. La sicurezza informatica è una questione che riguarda l'intera organizzazione e non un problema che i vertici devono affrontare o gestire da soli.

Proprio come l'anello più debole di una catena, un dipendente a qualsiasi livello di anzianità è in grado di mettere in pericolo un'azienda; di conseguenza, un approccio tradizionale di tipo piramidale non è necessariamente il modo migliore per incrementare la consapevolezza della sicurezza informatica. Inoltre, i vertici aziendali sono sottoposti ad attacchi più frequenti, basti pensare allo spear phishing, una pratica di attacco mirato con malware, che utilizza spesso informazioni personalizzate per apparire legittimi. Essere vittime di un attacco informatico ha poco a che fare con l'anzianità e molto di più con la formazione e la consapevolezza. Affinché una strategia di cybersecurity risulti efficace, è essenziale trasmettere abitudini e processi informatici positivi nella cultura aziendale senza che tali misure vengano percepite come un compito o un peso.

All'inizio di questo articolo, abbiamo proposto alcuni suggerimenti in base al "tipo" di personalità, sia per quanto riguarda lo stress che la sicurezza informatica. Questi consigli sono certamente una buona base di partenza per identificare i punti di forza e di debolezza individuali, è importante tuttavia che le aziende prendano in considerazione come le diverse personalità si manifestano in una dinamica di squadra. Il modo in cui un team interagisce produce un effetto diretto sul modo in cui risponde a un attacco informatico e sugli elementi di igiene informatica che possono essere ignorati nei momenti di stress o di panico. I leader devono inoltre riconoscere i propri punti di forza e debolezza personali per incoraggiare l'autoconsapevolezza all'interno del team e dell'organizzazione in generale.

Costruendo la propria consapevolezza di sé, i leader non solo possono comprendere meglio loro stessi, ma anche iniziare ad apprezzare le sfumature di comportamento del team, del loro reparto e dell'organizzazione. Il framework sui tipi di personalità MBTI è un modo efficace e semplice per farlo, ma per i leader che vogliono approfondire ulteriormente la loro comprensione, la seconda fase dell'MBTI potrebbe risultare molto utile. Per ciascuna delle quattro preferenze MBTI, la fase II esamina cinque aspetti del comportamento, fornendo un'immagine personalizzata dell'individuo. Per esempio, la maggior parte delle persone con una preferenza per l'estroversione si sentirà a proprio agio ad avviare conversazioni con estranei in situazioni sociali (Iniziatori), ma alcuni preferiranno mettersi in disparte e aspettare che gli altri si avvicinino a loro (Riceventi). Al contrario, la maggior parte delle persone con una preferenza per l'introversione assumerà il ruolo di Ricevente, ma altri mostreranno comportamenti di Iniziatori. Il risultato della fase II può essere particolarmente utile per i leader che si rendono conto di venire fraintesi dal proprio staff.

L'autoconsapevolezza del team è importante tanto quanto quella individuale quando si tratta di sicurezza informatica. La comprensione del profilo del team della fase II può aiutare a identificare le lacune comportamentali in cui un attacco informatico potrebbe trovare una via d'accesso; inoltre, può aiutare i team HR e IT a fornire una formazione personalizzata sulla sicurezza informatica in base alle esigenze del team.

Conclusione

Indipendentemente da ciò che porterà il futuro, due cose sono certe: il nostro modo di lavorare è stato modificato in modo permanente e gli attacchi informatici continueranno. La pandemia da COVID-19 non ha fatto altro che accelerare l'implementazione della tecnologia in tutti gli aspetti della vita; man mano che la digitalizzazione si espanderà nella vita domestica e lavorativa, la sicurezza informatica rimarrà il perno della sicurezza aziendale. Gli attacchi informatici sono una minaccia persistente per le organizzazioni e le aziende devono costruire team e sistemi IT resistenti, così da evitare le conseguenze finanziarie e di reputazione di un tale attacco. La comprensione della personalità può giocare un ruolo chiave nella strategia di sicurezza informatica di qualsiasi azienda, sia per migliorare l'efficacia della formazione sia per incoraggiare i dipendenti a investire maggiormente nella propria autoconsapevolezza e nelle proprie competenze. Comprendere che, nella sicurezza informatica, l'elemento umano è tanto importante quanto quello tecnico è il primo passo nella costruzione di protocolli olistici che tengano conto dei singoli punti di forza e debolezza.

In tempi di crisi, la leadership ha un profondo impatto sulla cultura organizzativa e sul morale. Quando i leader sono consapevoli di sé e del proprio team, possono implementare processi e pratiche in modo più efficace e guidare gli altri dipendenti nel percorso di autoconsapevolezza. È necessario innestare solide pratiche di sicurezza informatica a tutti i livelli di un'organizzazione e investire nella formazione dei dipendenti, sia nella sicurezza informatica sia nella consapevolezza di sé; questo permetterà ai team IT e HR di costruire strategie integrate, efficaci e proattive.