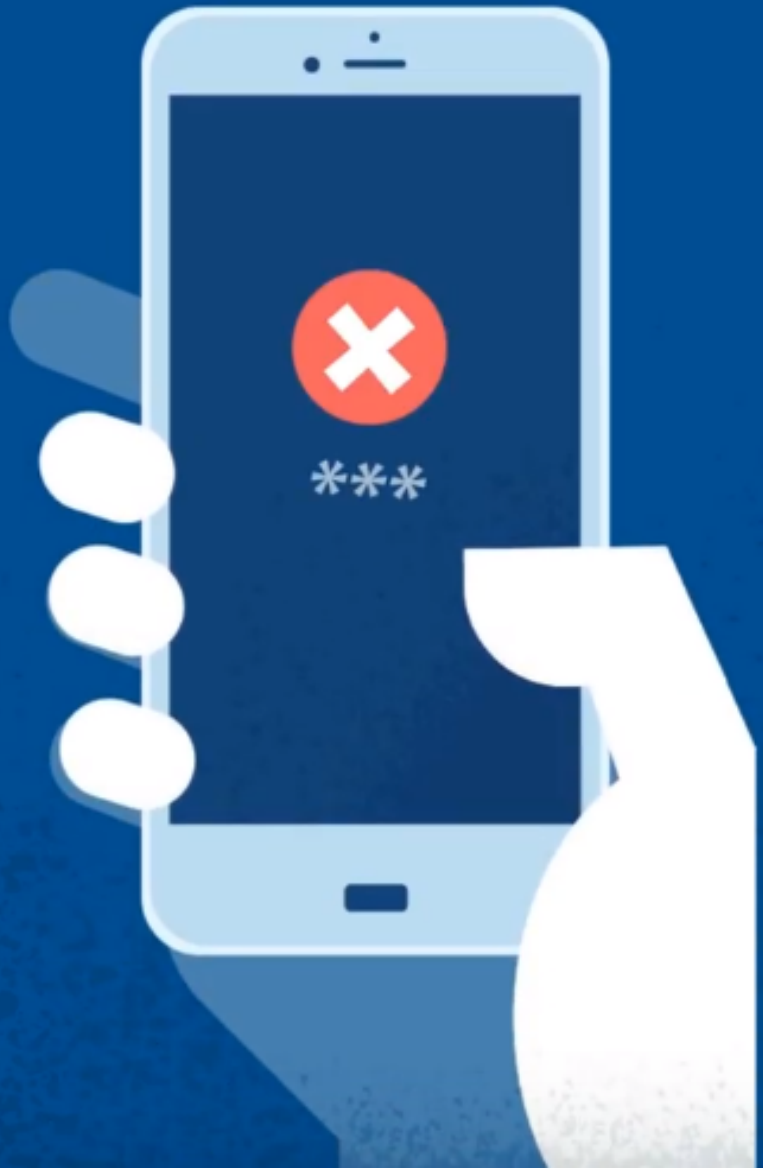
CYSED
HUMAN CYBER SECURITY EDUCATION

FATTORE UMANO E CYBER SECURITY: *i 10 comportamenti che mettono a rischio la tua azienda*

Conoscerli e prevenirli può salvare la tua impresa



Perché tanta importanza ai comportamenti umani?

Antivirus e altre soluzioni tecnologiche non bastano?

100 miliardi di dollari nel 2011, 500 miliardi di dollari nel 2017 e una previsione di **3000 miliardi di dollari per il 2021***.

Questo impressionante trend descrive l'esponenziale crescita dei danni economici per le aziende di tutto il mondo, **di ogni dimensione e settore**, per via di carenti sistemi di gestione della loro sicurezza informatica.

In **oltre il 95% dei casi,** come già dimostrato nel 2014 da IBM, gli incidenti di sicurezza informatica vedono la compresenza dell'**errore umano**.

È ormai evidente: un buon manager IT e un sistema tecnologico all'avanguardia non possono garantirti di evitare ingenti **danni economici, legali** e **d'immagine** alla tua azienda.

In ogni funzione aziendale e in ogni dipartimento, **dal magazzino all'ufficio del CEO**, e anche nelle operazioni più banali (come l'utilizzo del canale e-mail), si possono verificare comportamenti che possono mettere seriamente a rischio la tua azienda.

È necessario predisporre sempre la **responsabilizzazione** e, di conseguenza, la **formazione** di ogni singola persona che lavora nella tua azienda.

I dieci comportamenti presentati in questo decalogo sono solo **la punta dell'iceberg** ma possono, fin da subito, darti un'idea dei rischi che la tua azienda corre.

"Puoi avere la migliore tecnologia di sicurezza, ma non è efficace se chi l'adopera è distratto o non è stato addestrato"

(The Economist 2015).

* *Fonti: Clusit (Associazione Italiana per la Sicurezza Informatica) e Varonis, azienda statunitense leader del settore Cyber Security.*

1. Comunicazioni aziendali attraverso WhatsApp

Puoi esercitare una funzione di controllo?

3. Applicazioni sullo smartphone aziendale

Come evitare che vengano sottratti dati sensibili?

5. I wi-fi pubblici

Quali rischi nasconde una rete pubblica per la tua azienda?

7. Comunicazioni aziendali via mail

Il phishing tramite le e-mail: come ridurre la vulnerabilità?

9. Social Network

La scelta dei contenuti a tutela dell'immagine aziendale

2. Geolocalizzazione

Competitor e criminali sanno dove sono le persone che lavorano nella tua azienda?

4. Aggiornamento dei software

Quanto è rischioso evitare gli aggiornamenti dei dispositivi aziendali?

6. I pagamenti

Quali sono i metodi di attacco più diffusi tra i cybercriminali

8. Gestione password

Come generare una password sicura con un metodo facilmente memorizzabile?

10. Navigazione su internet

La porta di accesso per gli hacker

1. Comunicazioni aziendali attraverso WhatsApp

Puoi esercitare una funzione di controllo?

1. Comunicazioni aziendali attraverso WhatsApp

Puoi esercitare una funzione di controllo?

La tecnologia

Con oltre un **miliardo e mezzo di utenti attivi**, WhatsApp (WA) è diventato lo **standard della comunicazione interpersonale**: il suo successo è legato alla facilità d'uso, alla flessibilità e alla velocità che caratterizzano questo strumento.

Originariamente introdotta come una delle tante app di Instant Messaging (IM) gratuite, nel giro di pochi anni WA è diventata una piattaforma social incentrata sulla **condivisione di informazioni**, anche in **ambito lavorativo**.

WA aggiorna costantemente le proprie funzionalità: **messaggi vocali**, **chat**, **condivisione e trasferimento** di allegati e questi aggiornamenti possono contenere delle falle, delle **vulnerabilità** sfruttabili dai cyber-criminali.

Come viene regolato l'uso di WA da parte di **tutte le persone** che lavorano nella tua azienda?

2

I rischi per la tua azienda

Electronic Frontier Foundation ha posizionato WA all'**ultimo posto** tra le applicazioni di IM in relazione alla sua (in)capacità di garantire la **privacy** dei dati dei suoi utenti.

Sapevi, ad esempio, che anche persone con competenze informatiche non particolarmente avanzate possono aggirare il sistema di crittografia ed aggiungere **sconosciuti** ad un gruppo WA senza il permesso dell'amministratore, modificare i **messaggi** di altri utenti o cambiare l'**identità** della persona che invia un messaggio?

Ciò per via delle numerose vulnerabilità, ancora irrisolte, dei gruppi WA.

Inoltre, avendo a disposizione per pochi secondi uno smartphone di qualcun altro, è possibile entrare in possesso di **informazioni riservate**, utilizzando i **backup** (non crittografati, quindi in chiaro) delle chat presenti nel telefono. Questo può avvenire anche in remoto, attraverso applicazioni malevole inavvertitamente installate sul cellulare.

Al di là del modello con cui la tua azienda concede l'**uso dello smartphone in ambito aziendale**, WA sfugge da qualsiasi meccanismo di controllo: una terra di nessuno nella quale puoi incorrere in **danni legati all'immagine aziendale** e alla **gestione di dati e informazioni sensibili**.

1. Comunicazioni aziendali attraverso WhatsApp

Puoi esercitare una funzione di controllo?

3

I comportamenti

La maggior parte delle **policy aziendali** tollera l'uso di WA per lo scambio di messaggi tra dipendenti, ma non consente l'invio di file aziendali in allegato.

Ovviamente la tua azienda non ha modo di accertarsi che questo avvenga realmente.

Ciò comporta **diversi rischi**:

1. l'inoltro di una conversazione a terzi costituisce un "**data disclosure**" non autorizzato;
2. utilizzare WA per lavoro può generare numerose **incomprensioni** ed essere percepito come un'**invasione** della sfera personale del cliente o del collega;
3. la **ricezione e l'invio di file di lavoro** ne comporta il salvataggio nella memoria del telefono, dove rimangono anche dopo la cancellazione;
4. nel caso di furto dello smartphone, la presenza di file o conversazioni coi clienti comporta una serie di problemi per la **privacy** degli stessi e per la possibile diffusione di **informazioni riservate** dell'azienda;
5. molti addetti alle vendite utilizzano WA come strumento di lavoro, con messaggi diretti al singolo o costruendo gruppi di clienti a cui fare **offerte non controllabili** dall'azienda.

In definitiva la tua azienda, pur riconoscendo che la velocità della comunicazione WA possa essere un catalizzatore per le performance, deve essere conscia dei rischi di uno strumento sul quale non può esercitare **alcuna funzione di controllo**.

2. Geolocalizzazione

Competitor e criminali sanno dove sono le persone che lavorano nella tua azienda?

2. Geolocalizzazione

Competitor e criminali sanno dove sono le persone che lavorano nella tua azienda?

La tecnologia

La **richiesta di attivazione** della funzione di geolocalizzazione (GL) da parte dei device è ormai una prassi sia negli ambienti Android e iOS che nel mondo Windows di Microsoft.
Questa richiesta può essere fatta in sede di inizializzazione all'uso del device o di volta in volta da app e siti web.
In genere la richiesta iniziale viene motivata dalla possibilità di **tracciare la posizione di un device** in caso di furto.

Moltissimi utenti utilizzano **sistemi di navigazione geografica** che hanno come prerequisito proprio l'attivazione della GL. Avide di attivazione di GL sono anche le app di **Health&Fitness**, spesso associate all'adozione di **dispositivi wearable**.

Molte app infine, soprattutto in ambito e-commerce, richiedono la GL non per necessità ma al fine di ottimizzare le proprie **campagne di vendita** su base geografica.

Ma l'attivazione della GL comporta dei rischi quando l'utente **opera in ambito aziendale**?

2. Geolocalizzazione

Competitor e criminali sanno dove sono le persone che lavorano nella tua azienda?

2

I rischi per la tua azienda

Per un'azienda di **grandi dimensioni** o comunque impegnata in **progetti di R&D** o in fase di trasformazione del proprio **portafoglio prodotti**, la geolocalizzazione presenta un rischio particolarmente alto.

Questo tipo di informazioni può essere molto prezioso per il business di **aziende rivali**. Ad esempio, sapere che un gruppo di manager dell'R&D si trova in una specifica location potrebbe costituire, implicitamente, un rilascio di **informazioni riservate:** su di una fusione, un'acquisizione o una cessione.

Inoltre questo tipo di informazioni può danneggiare l'**immagine dell'azienda**, il **bilancio d'esercizio**, la **solidità del brand** o rallentare lo **sviluppo** di un importante progetto di R&D.

2. Geolocalizzazione

Competitor e criminali sanno dove sono le persone che lavorano nella tua azienda?

3

I comportamenti

È possibile rivelare la propria posizione in molti modi.
Ad esempio, **condividere semplicemente una fotografia** di quel che stiamo facendo o di quello che stiamo mangiando può rilevare dove ci troviamo. In alcuni casi le **coordinate** della nostra posizione sono **salvate** nel nome della foto, per cui dalla foto caricata su internet si può ricavare la nostra posizione.

Ancor più rischioso è **quando diamo il consenso ad applicazioni di tracciare la nostra posizione**.

Infatti, esistono **app** che, una volta dato loro il consenso, **tracciano la nostra posizione per sempre**, anche quando l'applicazione è chiusa. Dove siano conservati, per quanto tempo, come vengano usati e con chi possano essere condivisi questi dati è spesso, volutamente, un'informazione **difficilmente reperibile**.
In genere lo **scopo** del tracciamento è meramente **commerciale**: poter realizzare pubblicità mirate e studi comportamentali su **big data**. L'utilizzo dei big data, con l'implementazione di intelligenze artificiali sempre più evolute ad analizzarli, saranno sempre più disparate, ad esempio in ambito **politico** ne stiamo vedendo i primi utilizzi.

Queste informazioni possono essere **facilmente rubate dai server delle applicazioni**. In questo modo i criminali possono conoscere i nostri spostamenti, prevedere gli spostamenti futuri e, di conseguenza, pianificare un furto, un sequestro o, semplicemente, passare **informazioni** preziose **ai tuoi competitor**.

Un'ultima curiosità: sai che è possibile vedere tutti i posti in cui sei stato in cui hai attivato la geolocalizzazione?
https://www.google.com/maps/timeline?pb.

3. Applicazioni sullo smartphone aziendale

Come evitare che vengano sottratti dati sensibili?

3. Applicazioni sullo smartphone aziendale

Come evitare che vengano sottratti dati sensibili?

La tecnologia

Uno studio di BT, azienda britannica leader nel settore delle comunicazioni, evidenzia che nel 2018 **più di due terzi** (68%) delle organizzazioni a livello globale ha subito **brecce tramite dispositivi mobili.**

Ormai quasi tutte le aziende prevedono l'utilizzo dello **smartphone personale** per lavoro (93%) e circa **4 su 10** hanno una **bring your own device** (BYOD) policy che ne regolamenta l'utilizzo nel contesto lavorativo. Se da un lato una policy troppo restrittiva può diventare un ostacolo per l'**utente finale**, una rigidità che ne rallenta tutte le operazioni, dall'altro, una policy troppo vaga non aiuta ad evitare i rischi.

Le app vengono installate previo passaggio dalle piattaforme **Android** e **iOS** che ne filtrano la disponibilità effettuando delle **verifiche sugli sviluppatori,** prima di rendere possibile il download dai rispettivi store.

Di fatto, però, né Android né iOS, e men che meno le aziende riescono ad avere un pieno **controllo** su tali app.

Quali sono quindi i rischi legati a tali applicazioni, soprattutto per **l'uso nella tua azienda**?

3. Applicazioni sullo smartphone aziendale

Come evitare che vengano sottratti dati sensibili?

2

I rischi per la tua azienda

Partiamo col dire che la tua azienda, soprattutto nell'ambiente Android, non è nelle condizioni di effettuare un reale controllo sul **comportamento degli utenti** rispetto all'uso delle app.

Sulla carta puoi attivare delle **funzionalità di blocco** che impediscono l'installazione di certe app. Nella pratica però queste funzioni sono **facilmente disattivabili**.

In più, la maggioranza delle aziende tende a muoversi con prudenza quando si tratta di **intervenire sugli smartphone** dei dipendenti, siano essi privati o aziendali. Questo perché imporre delle limitazioni potrebbe essere **fonte di demotivazione** per il dipendente e, di conseguenza, avere impatti negativi sulla sua performance aziendale.

Il problema dell'uso delle app sugli smartphone è, quindi, nelle mani **dell'utente** stesso.

3. Applicazioni sullo smartphone aziendale

Come evitare che vengano sottratti dati sensibili?

3

I comportamenti

Gli utenti finali quando cercano una applicazione per risolvere un problema tendono a scaricarne molte per provarle. Questo comportamento espone al rischio che tra le tante applicazioni installate ce ne sia una malevola. Non sempre ci si accorge di aver scaricato un'applicazione **contenente malware**.

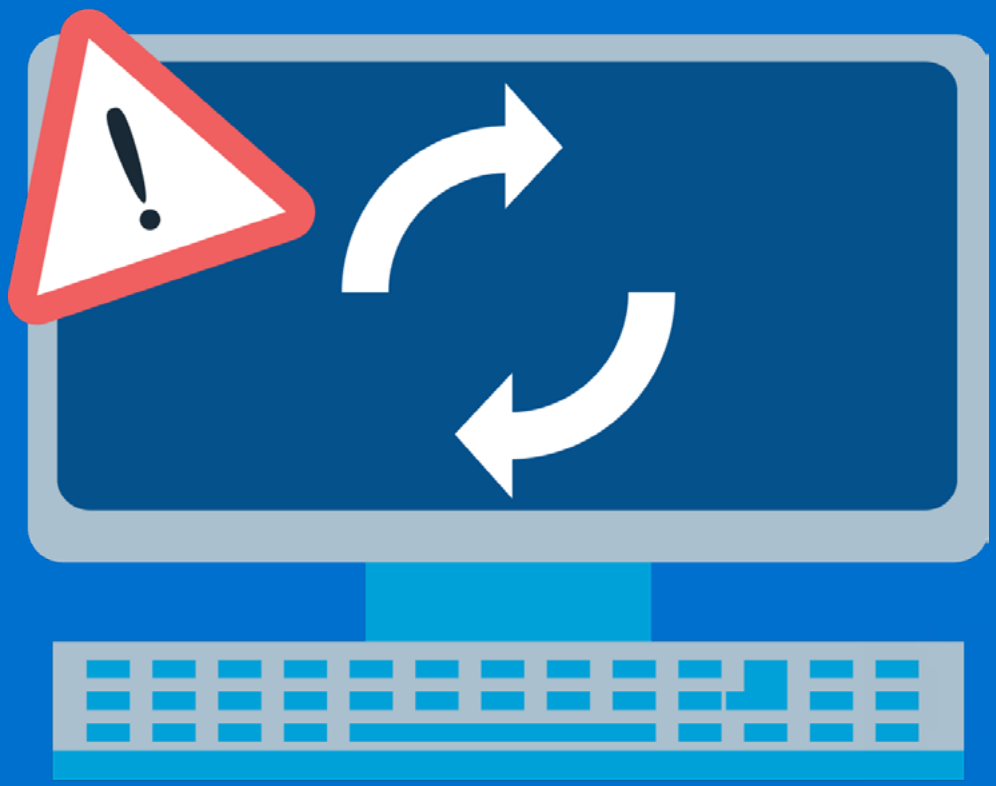
Si tende a dare per scontato che i filtri di **Apple e Google Store** possano eliminare tutte le applicazioni contenenti malware. L'utente finale si sente **deresponsabilizzato** nella scelta e non riflette sui potenziali rischi della proliferazione del mercato delle app. Molte applicazioni inoltre ci chiedono il consenso per **accedere a contenuti**, videocamera, GPS. Esiste un grosso traffico di informazioni personali per **scopi di marketing**, politici o addirittura criminali.

Un esempio? DressCode è un **trojan** che si annida in alcune applicazioni: una volta installato sul device, rimane silente ma permette di **comandare in remoto** il dispositivo. Se quest'ultimo è collegato alla rete aziendale, gli hacker ottengono l'accesso agli altri dispositivi connessi a quella stessa rete e sono in grado di **rubare dati sensibili**.

Sebbene vi siano dei rischi quando si scarica una app, l'utente finale tende ad ignorarlo.

Come difendersi? Innanzitutto è importante leggere le **review delle applicazioni** che scarichiamo e non utilizzare il cellulare per lo scambio di **documenti di lavoro**.

Il consenso alle app per accedere ai nostri dispositivi deve essere meditato. Seguire le indicazioni della **policy aziendale** è sempre la scelta migliore.



4. Aggiornamento dei software

Quanto è rischioso evitare gli aggiornamenti dei dispositivi aziendali?

4. Aggiornamento dei software

Quanto è rischioso evitare gli aggiornamenti dei dispositivi aziendali?

La tecnologia

Gli **aggiornamenti** per computer, smartphone e browser dovrebbero essere imprescindibili per la sicurezza dei device. Tuttavia, in molti casi gli utenti finali tendono a **rimandare** tali interventi, anche quando si tratta di **dispositivi aziendali**.

L'importanza degli aggiornamenti è **cruciale**: spesso, infatti, contengono patch che coprono importanti **falle nella sicurezza** rilevate dagli sviluppatori. Non esiste mai un software sicuro al 100% perché non sarebbe utile: non avrebbe la possibilità di **connettersi con altri device** o di scaricare applicazioni al suo interno.

La priorità degli sviluppatori è la **fruibilità**, la semplicità e l'applicabilità del device nella vita quotidiana.

Occorre quindi che l'utente finale sia il primo a porsi il problema della sicurezza e sia **consapevole** dei rischi a cui potrebbe esporre l'azienda.

4. Aggiornamento dei software

Quanto è rischioso evitare gli aggiornamenti dei dispositivi aziendali?

2

I rischi per la tua azienda

Aggiornare **costantemente** i propri dispositivi significa tutelarsi dal rischio che un malware possa **diffondersi nel sistema** sfruttandone le vulnerabilità. Un solo utente che non aggiorna il software mette a repentaglio tutta la **rete aziendale**.

Come evidenziato dal report annuale **Microsoft 2018**, si è registrato un aumento degli attacchi *supply chain compromise*: questo tipo di attacco consiste **nell'inserimento**, da parte dell'hacker, di un codice malevolo all'interno della **patch di aggiornamento** di alcuni software usati dalle aziende.

Per difendersi da questo tipo di attacchi ci sono **due semplici soluzioni**:

1. accertarsi della **sicurezza** dei server dei fornitori di software
2. tenere sempre aggiornato il **sistema operativo**

Un esempio tangibile dell'importanza degli aggiornamenti è il caso dello wiper **NotPetya**: inserito nell'aggiornamento di un software contabile, è andato a infettare i computer che non avevano aggiornato il sistema operativo. Il malware si è poi diffuso in tutta la **rete aziendale** e successivamente in quelle di fornitori e clienti, criptando irreversibilmente tutti i dati presenti all'interno. Banche, aeroporti, compagnie energetiche ucraine sono state le prime vittime, poi le aziende **di tutto il mondo**, per un danno di oltre 10 miliardi di dollari.

4. Aggiornamento dei software

Quanto è rischioso evitare gli aggiornamenti dei dispositivi aziendali?

3

I comportamenti

Perché l'utente finale ha la tendenza di **rimandare** gli aggiornamenti o di non effettuarli? Spesso questi vengono percepiti come una perdita di tempo o, specialmente nel caso degli smartphone, perché **rallentano le prestazioni**.

Questo atteggiamento viene autogiustificato dall'apparente senso di **controllo** che molti hanno sul mondo digitale, che porta a sottovalutare i rischi e **ignorare policy e direttive**. Sono soprattutto le nuove generazioni a sottovalutare le criticità legate alle nuove tecnologie: abituati fin da giovani all'uso, ne vedono solo i vantaggi e non riescono a valutarne obbiettivamente i **pericoli**.

5. I wi-fi pubblici

Quali rischi nasconde una rete pubblica per la tua azienda?

5. I wi-fi pubblici

Quali rischi nasconde una rete pubblica per la tua azienda?

La tecnologia

Siamo ormai abituati a essere **costantemente connessi** a internet, sia a casa, che in ufficio o in un esercizio commerciale. Diamo, infatti, per scontato di trovare **wi-fi pubblici** in stazioni, bar, ristoranti, negozi e non consideriamo i rischi che corriamo connettendoci a queste reti.

Il pericolo principale è dettato dal **furto di informazioni**, che può avvenire secondo due metodologie:

1. ***Spoofing***: l'attaccante crea un wi-fi simile a quello pubblico, che in realtà monitora tutti i dati che vengono inseriti. Si tratta di una tecnica molto semplice, basta scaricare determinati software come *Wifi Pinapple*;
2. ***Sniffing***: in questo caso l'hacker si connette al wi-fi pubblico ufficiale e, tramite software come *WireShark*, può osservare il traffico di pacchetti di dati inviati e ricevuti dai device.

Vediamo ora i rischi che questi attacchi comportano.

5. I wi-fi pubblici

Quali rischi nasconde una rete pubblica per la tua azienda?

2

I rischi per la tua azienda

L'obiettivo dell'attaccante che monitora il traffico degli altri utenti è quello di rubare loro le **credenziali** di accesso ai vari servizi online come mail, credenziali bancarie, social.

Inoltre, un altro rischio a cui si espone un **utente di wi-fi pubblici** è che il device venga infettato da un malware, con conseguenze diversificate: rallentamento del sistema, **spam** pubblicitario, furto di dati e un'alta possibilità che il **malware** si diffonda a tutta la rete aziendale.

È quindi importante non sottovalutare le conseguenze di un furto di **informazioni riservate** riguardanti i clienti: il GDPR, infatti, obbliga l'azienda a dichiarare i data breach, con conseguente danno all'immagine, la perdita dei clienti interessati dalla **perdita di dati** e dei potenziali clienti futuri.

Come tutelarsi, dunque? L'idea di dotare ogni dipendente di smartphone forniti di **antivirus** è una soluzione costosa e che non risolve il problema se non parzialmente, molto più efficace è una **formazione che educhi** l'utente finale ad un uso consapevole.

5. I wi-fi pubblici

Quali rischi nasconde una rete pubblica per la tua azienda?

3

I comportamenti

Il rischio si presenta in moltissime situazioni della vita quotidiana, anche **extra-lavorative**.

Si pensi, ad esempio, al caso del dipendente in vacanza in un paese extraeuropeo sprovvisto della **connessione 4G**. È probabile che utilizzi diversi wi-fi pubblici: nel caso in cui sul suo dispositivo personale siano conservate informazioni o dati di lavoro, il rischio di mettere a repentaglio l'azienda è alto.

Il furto o la breccia possono avvenire anche in modo più **mirato e sistematico**, come nel caso in cui un dipendente frequenti abitualmente un bar o un ristorante. Se il wi-fi di quell'esercizio commerciale non presenta un **adeguato livello di sicurezza**, il suo dispositivo sarà più facilmente esposto al furto di dati, specialmente da parte di chiunque sappia che quella persona frequenta quotidianamente quel locale.

L'esposizione a questo tipo di attacco è alta anche perché raramente gli smartphone sono protetti da **firewall o antivirus** e sono, quindi, facilmente accessibili. Inoltre è bene sapere che la maggior parte degli antivirus gratuiti per smartphone rileva **meno del 30% delle minacce**, fornisce quindi solo un apparente senso di protezione all'utente.

6. I pagamenti

Quali sono i metodi di attacco più diffusi tra i cybercriminali

6. I pagamenti

Quali sono i metodi di attacco più diffusi tra i cybercriminali

La tecnologia

Sapevi che il **phishing** è il metodo di attacco preferito dai cybercriminali e che è in continua crescita (+0,55%)? A evidenziarlo è il report Microsoft 2018, nel quale vengono approfonditi tre particolari tipi di truffe:

1. **Man in the middle**: l'hacker si inserisce all'interno di una conversazione tra cliente e fornitore, sostituisce l'IBAN della fattura con uno di sua scelta, lasciando però **inalterato l'indirizzo mail** da cui proviene il documento fiscale;
2. **Truffa del CEO**: l'attaccante riesce ad ottenere l'indirizzo mail di un dirigente dell'azienda e comunica la necessità di effettuare un pagamento immediato. Quello che rende così efficace questa truffa è la **pressione emotiva** di una comunicazione che proviene da una fonte autorevole e comunica un'estrema urgenza. Questi due fattori favoriscono una decisione veloce, euristica ed inibiscono un ragionamento strutturato sui rischi che si corrono ad effettuare un pagamento di questo tipo senza le dovute verifiche;
3. **Keyloggers**: si tratta di malware in grado di rilevare tutto quello che la persona digita sulla tastiera per inviarlo successivamente all'attaccante, che ha l'intento di trovare **password o numeri di carte di credito**. La modalità di diffusione più consueta di questi malware è sempre l'allegato tramite mail, oppure il download tramite browser o torrent.

6. I pagamenti

Quali sono i metodi di attacco più diffusi tra i cybercriminali

2

I rischi per la tua azienda

Il rischio principale è, ovviamente, quello di perdere un'ingente **somma di denaro**: anche qualora l'azienda riuscisse a recuperarla tramite l'assicurazione, l'investimento di tempo e risorse economiche sarebbe rilevante.

Per non parlare del **danno alla reputazione**, anch'esso considerevole, al pari dei costi di gestione legali, amministrativi e di eventuale notifica del *data breach*.

Questo tipo di attacchi elude il filtro di qualsiasi tipo di **antivirus o firewall** perché sfrutta la buona fede e il comportamento dell'utente finale: è quindi molto difficile da limitare e rappresenterà sempre una **vulnerabilità** intrinseca di ogni azienda che effettui qualsiasi pagamento online.

6. I pagamenti

Quali sono i metodi di attacco più diffusi tra i cybercriminali

3

I comportamenti

I reparti amministrativi, anche di piccole aziende, si trovano spesso a far fronte ad una **grossa mole di lavoro**, con stress crescente per il volume di mail e pagamenti da gestire.

La società li abitua a essere **veloci**, nei pagamenti, nelle consegne, il volume di e-commerce dell'azienda cresce e c'è il rischio che, per economia di tempo, le verifiche effettuate prima delle transazioni diminuiscano.

Come fare quindi? Il **metodo migliore** è controllare sempre:

1. che l'IBAN **corrisponda** alle coordinate bancarie
2. che l'IBAN sia **italiano**
3. se possibile telefonare al fornitore per accertarsi della **correttezza** degli estremi bancari, soprattutto le prime volte che si effettua un pagamento.

Sono procedure che richiedono più tempo ma garantiscono un ritorno impagabile in termini di sicurezza.

7. Comunicazioni aziendali via mail

Il phishing tramite le e-mail: come ridurre la vulnerabilità?

7. Comunicazioni aziendali via mail

Il phishing tramite le e-mail: come ridurre la vulnerabilità?

La tecnologia

Nonostante la comunicazione via Instant Messaging e social sia sempre più in crescita, gli scambi via e-mail restano lo **standard più diffuso per la comunicazione** aziendale.

I punti di forza delle e-mail risiedono, infatti, nella possibilità di salvare nel folder, gestire gli allegati, effettuare un **controllo aziendale** sul traffico e accedere da dispositivi mobili.

Si consideri però che nella maggior parte dei casi è proprio tramite le e-mail, e più nello specifico mediante il **phishing**, che le aziende vengono attaccate.

A confermare questa tendenza è stato anche **il report di Microsoft** sui trend Cybersecurity 2018, il quale mette in evidenza come gli attacchi informatici veicolati tramite e-mail malevole siano stati, nel corso del 2018, in **forte crescita**: dall'analisi di circa **500 miliardi di e-mail** in ingresso nei sistemi di posta elettronica, si è passati da uno 0,25% di e-mail di phishing all'inizio del 2018, a oltre uno 0,50% a fine 2018.

Una crescita impressionante.

Il rapporto Microsoft elenca ben otto modalità secondo le quali una e-mail malevola cerca di carpire informazioni all'utente o a portarlo a compiere azioni con ricadute negative, sia aziendali che personali.

7. Comunicazioni aziendali via mail

Il phishing tramite le e-mail: come ridurre la vulnerabilità?

2 I rischi per la tua azienda

Le conseguenze di un attacco di **phishing** sono molteplici e creano danni all'azienda sia in termini reputazionali, sia economici.

Gli attacchi più pericolosi sono quelli che, attraverso l'apertura di un file allegato contenuto in un'e-mail malevola, attivano un virus della famiglia **ransomware**.

Questi virus, in modo silente, criptano i file dei sistemi informatici, bloccando qualsiasi attività. L'unico modo per sbloccare questi file criptati è **pagare un riscatto** in bitcoin. Il pagamento del riscatto non da però la certezza di riottenere i file, gli hacker potrebbero richiedere il pagamento di un'ulteriore somma.

L'attenzione sui rischi del phishing è **molto aumentata** in questi anni.

Molte aziende conducono costantemente campagne con **phishing test**, simulando l'invio di e-mail malevole: l'obiettivo è verificare quanti utenti cadono nella trappola e sensibilizzarli di conseguenza con la somministrazione di pillole di **micro-learning**.

Non esistono dati precisi sulle percentuali di breccia dei phishing test: **un rapporto Verizon** parla, però, di oltre un 20% della popolazione aziendale che cade almeno una volta nella trappola e di un 4% recidivo. Numeri che indicano un'importante **vulnerabilità**.

Alcune aziende cercano di segnalare all'utente finale se una e-mail può essere sospetta e comunque contrassegnano, spesso con un **carattere bold** di allerta, quando una e-mail proviene dall'esterno.

I rischi del phishing e di tutti gli attacchi perpetrati via e-mail restano in larga parte nelle mani dell'**utente finale**, della sua vulnerabilità e scarsa sensibilizzazione.

7. Comunicazioni aziendali via mail

Il phishing tramite le e-mail: come ridurre la vulnerabilità?

3

I comportamenti

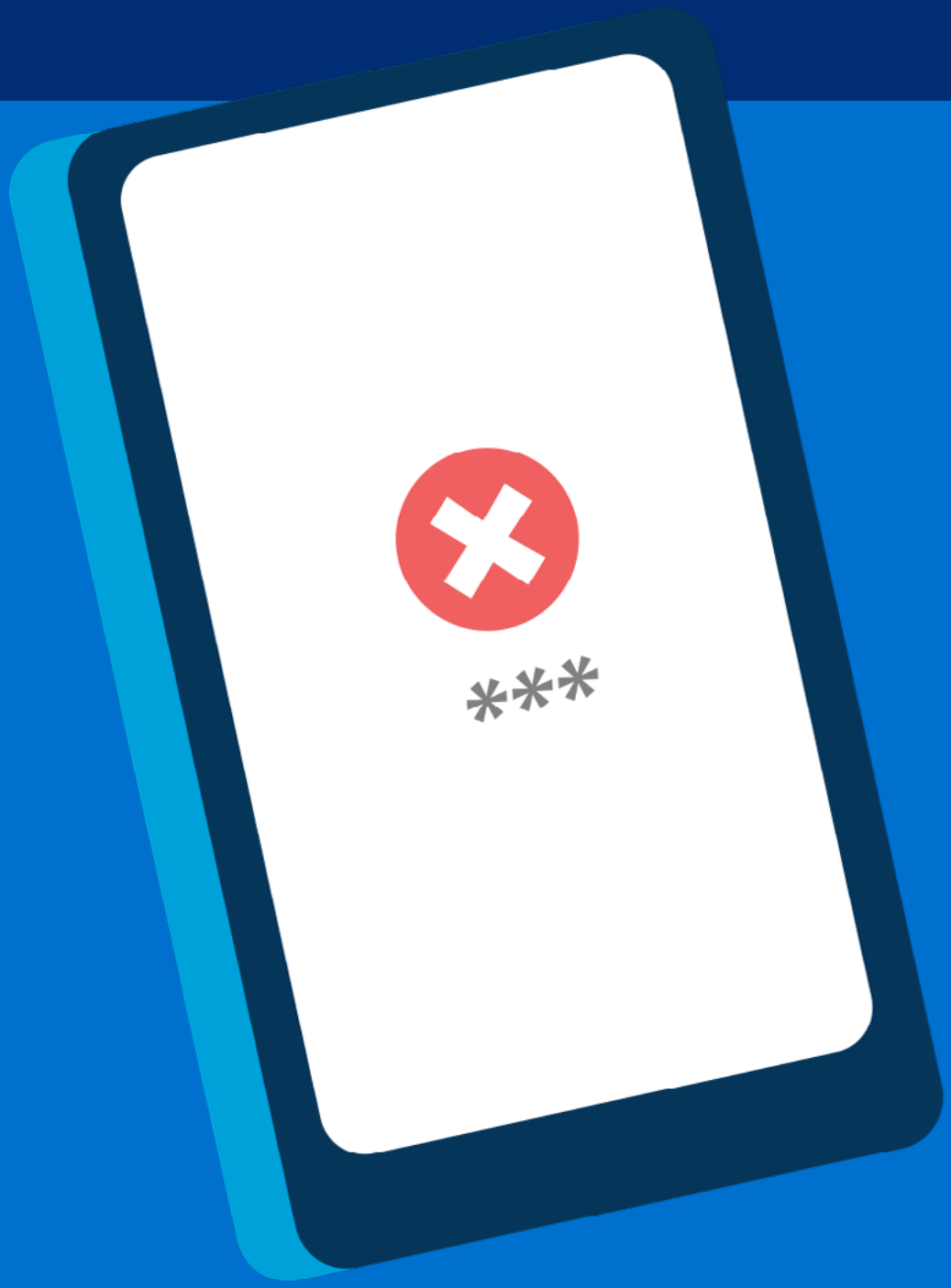
Ci sono una **serie di fattori** che spingono l'utente ad aprire un allegato o a cliccare su un link di un'e-mail malevola:

1. la mancanza di **awareness** o un'awareness incompleta o esclusivamente tecnica;
2. **specifici tratti di personalità** dell'end-user come nevroticismo e apertura mentale (*Helvi et al. 2014; McCormac et al. 2017*);
3. l'utilizzo di tecniche di social engineering da parte dei criminali che fanno leva sugli **aspetti emotivi** dell'utente finale: una fonte autorevole (reparto IT, AD, Studio Legale), un pericolo imminente che richiede un'azione immediata, il soddisfacimento di bisogni relazionali o economici.

La **psicologia** dell'utente finale resta perciò centrale nel generare una vulnerabilità.

Sembrerà paradossale, ma un buon livello di awareness sulla **Cyber Security**, da sola non previene comportamenti che comportano una sottovalutazione il rischio. Si pensi ad esempio al meccanismo dell''"over-confidence", per il quale un certo livello di **conoscenza tecnica** fa sentire l'utente erroneamente al riparo da qualsiasi attacco informatico.

Inoltre, ad una awareness sbrigativa si lega spesso una percezione di competenza molto alta, per via dell'**effetto Dunning-Kruger**: molte persone già hanno delle conoscenze legate alle nuove tecnologie e quindi, dopo una breve awareness si sentono esperti, anche se in realtà hanno ancora una visione distorta e superficiale dell'argomento.



8. Gestione password

Come generare una password sicura con un metodo facilmente memorizzabile?

8. Gestione password

Come generare una password sicura con un metodo facilmente memorizzabile?

La tecnologia

Applicazioni, siti, account, dispositivi: da ciascuno di essi viene richiesta un'autenticazione online della persona, spesso in modo veloce, per agevolare l'accesso al servizio. Come si fa a ricordare un numero sempre crescente di **credenziali di accesso**? La soluzione non è certo quella di usare sempre **la stessa password** o di usare password molto **semplici**.

Usando sempre la stessa password su diversi account ci si espone ad un attacco *credential stuffing*: l'attaccante tenta l'accesso ad un vasto numero di account **riutilizzando** credenziali trafugate in precedenza attraverso i data breach: **brecce nei server** di grosse compagnie come Google o Instagram.

Mentre usando chiavi d'accesso semplici si rischia che l'account venga forzato tramite attacco *brute-force*: una tecnica che attraverso un software, **inserisce credenziali comuni** o parole estratte da un dizionario, per tentare di accedere all'account.

Un altro problema per le aziende è la **condivisione**: in alcuni gruppi di lavoro la password viene condivisa e raramente rinnovata; di conseguenza chiunque abbia lavorato in passato in quell'ufficio può divulgarla per errore o per suo tornaconto.

Infine, **il salvataggio automatico** delle password può essere molto comodo, ma dobbiamo essere consapevoli che una volta che **l'attaccante** riesce ad entrare nel sistema ha libero accesso a tutti i nostri servizi.

8. Gestione password

Come generare una password sicura con un metodo facilmente memorizzabile?

2

I rischi per la tua azienda

Considera i rischi derivati dal **furto dell'identità digitale** di un dipendente: l'hacker potrebbe richiedere di effettuare un pagamento o effettuare una **transazione** in prima persona, come nel caso del furto dell'account Amazon, oppure danneggiare l'immagine dell'azienda, o ancora rubare **dati riservati**.

Il furto di una password di un utente che sulla carta ha pochi privilegi nell'**accesso ai sistemi aziendali**, non va sottovalutato.

Spesso questo furto è prodromico al **meccanismo di attacco** della *privilege-escalation*: l'attaccante, spostandosi orizzontalmente e verticalmente a partire da quell'utente con password nota, cerca di impossessarsi delle credenziali di altri utenti.

I rischi sono molteplici e l'azienda non ha modo di **controllare** che le password dei suoi dipendenti siano ben formate. Ma come si elabora una password sicura?

8. Gestione password

Come generare una password sicura con un metodo facilmente memorizzabile?

3

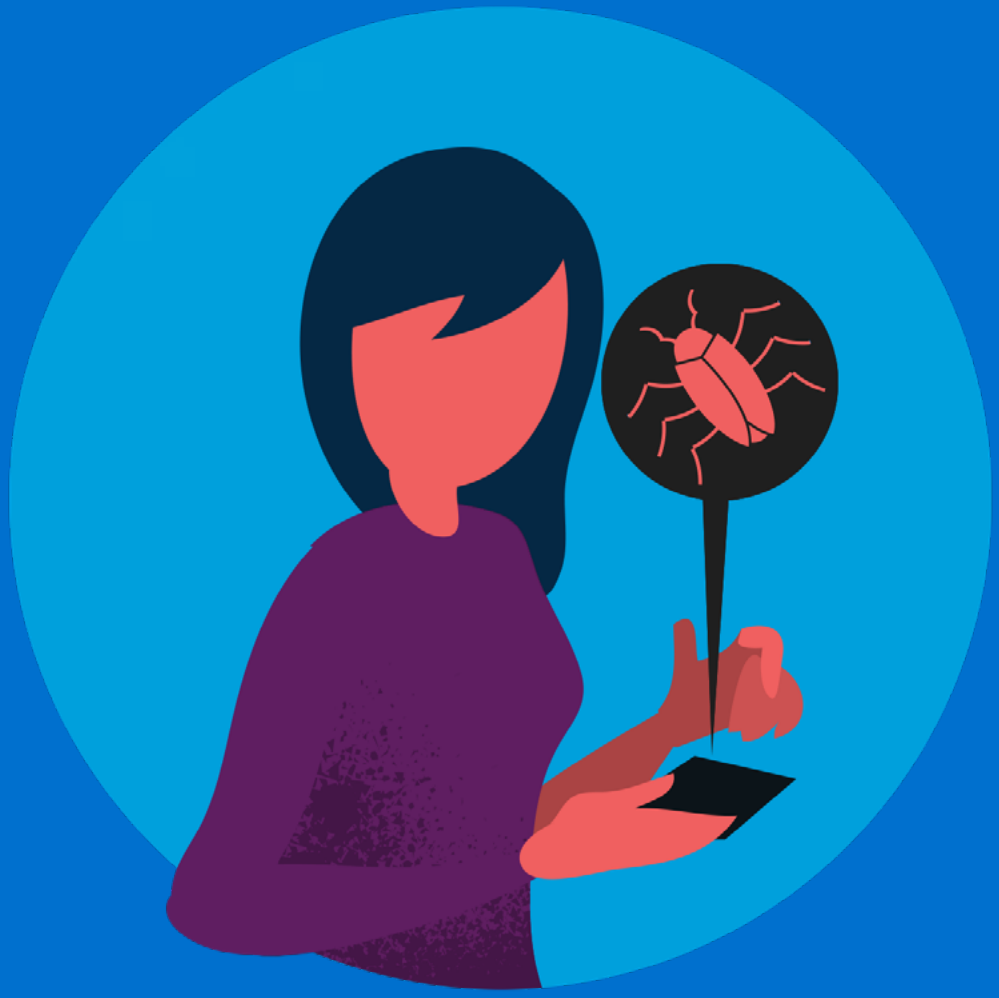
I comportamenti

Dimentica le solite "1234", "qwerty" e "password": un buon metodo per sviluppare una password efficace consiste nel **memorizzare una frase** e utilizzare le iniziali della frase per comporre una parola.

Un esempio potrebbe essere: "Sono ultimo di 3 fratelli ma sono il più furbo" che diventa "Sud3fmsipf"; una password apparentemente senza significato per un computer, ma **facilmente memorizzabile**.

Bisogna ricordare però di non utilizzare sempre la stessa **chiave d'accesso** per tutti gli account, occorrono delle variazioni. Ad esempio, alla fine della frase si può mettere un "F@CE" per "Facebook" o se è l'account di Google Mail si può mettere "GM@IL", il simbolo "@" sta per una "A" ma serve ad **aumentare la complessità** della password. Il risultato finale è il seguente: "Sud3fmsipfGM@IL" molto complessa ma facile da ricordare.

La cosa importante è trovare un proprio metodo per **generare password** e non sottovalutare i rischi. Certo, i meccanismi di **sicurezza** si affineranno sempre più, ma lo stesso faranno i metodi di attacco: ci saranno programmi capaci di provare migliaia di credenziali per ogni account o che utilizzeranno **l'intelligenza artificiale** per incrociare dati personali (come il nome del cane, la via o la data di nascita), per creare delle **combinazioni di password** possibili per quell'account o per bucare l'account tramite le domande di sicurezza.



9. Social Network

La scelta dei contenuti a tutela dell'immagine aziendale

9. Social Network

La scelta dei contenuti a tutela dell'immagine aziendale

La tecnologia

Essere presenti sui social comporta **visibilità**, che spesso si trasforma in pubblicità gratuita per l'azienda. Ci sono molti vantaggi nell'avere dipendenti che **postano informazioni** legate al proprio lavoro e alla propria formazione su social come LinkedIn, Facebook o Instagram.

Come vedremo, però, ci sono altrettanti rischi collegati. Il problema è la difficile **definizione** di ciò che è consentito postare e di ciò che non lo è.

Il riferimento ufficiale è la **Social Media Policy** aziendale, il cui contenuto può però creare più dubbi di quanti ne risolve: si fa spesso riferimento al "buonsenso" o a "comportarsi su internet come ci si comporterebbe di persona" ma il mondo reale non corrisponde a quello **virtuale** e senza una formazione specifica l'incidente resta dietro l'angolo.

In particolar modo per le **aziende** con un elevato numero di dipendenti.

2

I rischi per la tua azienda

I rischi per l'azienda come sempre sono molti: si va dal **danneggiamento** dell'immagine, dovuto alla natura dei contenuti pubblicati da un dipendente, alla diffusione di informazioni riservate, che potrebbero ad esempio rovinare il **lancio di un prodotto**, oppure essere informazioni utili alla concorrenza.

Spesso si sottovaluta il meccanismo di ricostruzione del "**puzzle**": ovvero il fenomeno per il quale tanti utenti rilasciano sui propri profili social piccoli brick informativi, che un attaccante potrebbe facilmente ricostruire, accedendo a un **segreto aziendale** o a un'informazione confidenziale.

I rischi non riguardano solo le informazioni di lavoro: anche il rilascio di **informazioni personali** tramite social può avere ricadute importanti per l'azienda. La disponibilità di molte informazioni personali facilmente reperibili su **internet** può esporci a un furto di identità che può essere sfruttato per danneggiare l'azienda.

Inoltre, le **convinzioni** politiche, religiose o altre informazioni sensibili potrebbero dare un'immagine negativa di quell'impiegato che, anche se espressa privatamente, **impatta sull'azienda** in cui lavora.

Infine, è importante ricordare che i **social network** usano i dati dei loro utenti per profilazione e pubblicità mirate, ma in alcuni casi potrebbero usarli illecitamente anche per **scopi politici** o economici: basti pensare allo scandalo della campagna Trump-Hilary Clinton in cui è stato implicato Facebook.

9. Social Network

La scelta dei contenuti a tutela dell'immagine aziendale

3

I comportamenti

Una prima buona regola per l'utente finale è quella di controllare le varie **impostazioni sulla privacy** dei propri social, sapere sempre con chi sono condivisi certi **contenuti** e che diritti di utilizzo hanno i social rispetto a quell'informazione.

Una precauzione utile è far sì che ci sia una **selezione** dei contatti aggiunti sui social, specialmente i social network aziendali, e **accettare** prevalentemente persone che conosciamo nella vita reale.

È importante che i dipendenti si accertino di condividere **poche informazioni** e di impostare la visibilità ai soli amici, in modo che sia più difficile che qualcun altro possa tentare di impersonare uno di loro sfruttando dati reperibili pubblicamente.

In generale, quanto più il dipendente è **attivo** sul proprio profilo social, tanto più dovrà muoversi con **cautela** nella sua partecipazione al social aziendale, fare in modo che le modalità di utilizzo e i contenuti postati siano appropriate al contesto ed ai rischi.

10. Navigazione su internet

La porta di accesso per gli hacker

10. Navigazione su internet

La porta di accesso per gli hacker

La tecnologia

L'accesso a internet è un requisito **irrinunciabile** per i dipendenti.

Non sempre c'è un reale bisogno per esigenze lavorative, ma l'uso dello **smartphone** e della conseguente possibilità di accesso a internet per effettuare ricerche, ha reso la navigazione una **necessità insindacabile**.

Come sempre la **rivoluzione digitale** mischia e confonde la dimensione personale e quella aziendale, in particolar modo nell'uso dei dispositivi mobili.

Ad esempio, negli ambienti Microsoft alcuni URL sono bloccati da **filtri di sicurezza** posti nella rete aziendale. Tuttavia, questi filtri sono **bypassati** nel momento in cui l'utente usa un device mobile personale, anche autorizzato all'uso aziendale.

10. Navigazione su internet

La porta di accesso per gli hacker

2

I rischi per la tua azienda

La presenza di **virus e malware** non si annida solo all'interno di e-mail di phishing; l'infezione può spesso avvenire nel corso della navigazione internet su **siti non sicuri**, link a download o attraverso pop-up ingannevoli.

Come già visto per il phishing, anche la **navigazione** internet può quindi essere una porta per gli attacchi degli hacker.

Indubbiamente **firewall e antivirus** in uso presso l'azienda possono ridurre considerevolmente le vulnerabilità, poiché identificano URL e indirizzi IP **sospetti**. Ma, anche in questo caso, il comportamento dell'utente finale, il cosiddetto **fattore umano**, resta lo snodo centrale per la sicurezza.

Attualmente molti motori di ricerca segnalano i diversi livelli di **sicurezza** di un sito (indirizzi http e https), ma spesso l'utente ignora questi suggerimenti, proseguendo nella navigazione.

10. Navigazione su internet

La porta di accesso per gli hacker

3

I comportamenti

Identificare correttamente quali sono le **pagine sicure** e quali non lo sono è un compito sempre più difficile. In certi casi vengono annidati **script malevoli** in pagine Google o in pop-up che vengono visualizzati in siti che di per sé sarebbero sicuri, ma che non hanno fatto un controllo accurato sui pop-up accettati e mettono inconsapevolmente a rischio i propri utenti.

Spesso l'insidia si nasconde dietro ad un click di consenso ad una **cookie policy** che, in realtà è solo un pop-up trappola e avvia il download di malware o spyware.

Ecco alcune precauzioni utili:

1. tenere sempre **aggiornati** i browser;
2. navigare solo su pagine https, ossia **sicure** perché criptate;
3. cancellare periodicamente la **cronologia**;
4. **non salvare** le password sui browser;
5. **evitare** il più possibile i download;
6. attivare sempre **l'autenticazione a due fattori**.

In generale, seguire sempre le indicazioni previste dalle **policy aziendali** e improntare sempre i propri comportamenti digitali a un sano e cauto scetticismo, senza mai farsi trascinare dalla fretta dilagante nel mondo digitale.

Vuoi approfondire gli aspetti tecnici e aumentare il livello di consapevolezza della tua azienda sulla cyber security?

Contatta un nostro referente e richiedi la tua consulenza gratuita della durata di un'ora via **Skype**.

Scrivi a: corsi@cysed.it

Ti interessa conoscere l'offerta formativa di Cysed e scegliere il corso più adatto alle esigenze della tua azienda?

Consulta la lista completa.

CYSED

HUMAN CYBER SECURITY EDUCATION