GUIDA ALL'INGEGNERIA SOCIALE

Come fare la cosa giusta

Contenuti

Perché le PMI dovrebbero preoccuparsi di social engineering

Le PMI sono sempre più consapevoli di essere obiettivi appetibili per i criminali informatici, secondo un sondaggio del 2019 condotto da Zogby Analytics per conto della US National Cyber Security Alliance, quasi la metà (44%) delle aziende con 251-500 dipendenti ha dichiarato di aver subito una violazione ufficiale dei dati negli ultimi 12 mesi. Il sondaggio ha rilevato che l'88% delle piccole imprese ritiene di essere quantomeno un obiettivo "abbastanza probabile" per i criminali informatici, tra questi quasi la metà (46%) crede di essere un obiettivo "molto probabile".

Il danno è reale ed esteso, come ben illustrato dal rapporto annuale Internet Crime Complaint Center (IC3) dell'FBI. Solo nel 2020, l'IC3 ha ricevuto 19.369 denunce di attacchi BEC (business email compromise) e EAC (email account compromise), con perdite stimate per oltre 1,8 miliardi di dollari. Per coloro che non lo sanno, gli attacchi BEC/EAC sono truffe sofisticate che prendono di mira sia le imprese che gli individui che eseguono trasferimenti di fondi.

Come riportato nel Data Breach Investigations Report 2019, il 33% delle violazioni ha incluso attacchi di ingegneria sociale, la seconda tattica più utilizzata dopo l'hacking.

Dopo che le PMI sono state vittime di una violazione

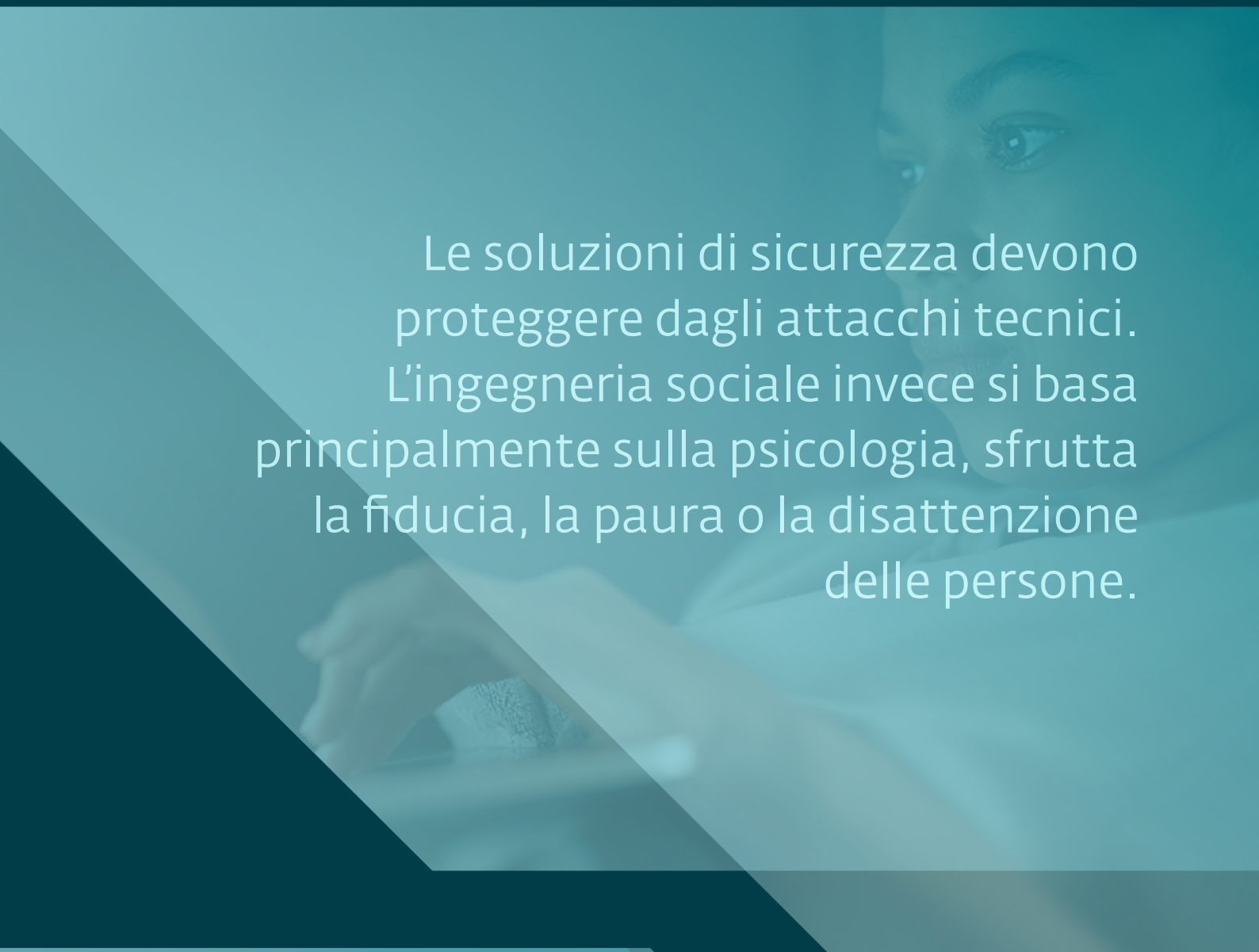
37%	25%	10%
ha subito una perdita finanziaria	ha presentato istanza di fallimento	ha chiuso l'attività

Fonte: NCSA

Introduzione

Lo scopo di questa guida è quello di aiutare a introdurre il concetto di ingegneria sociale e i rischi derivati a ogni dipendente dell'azienda. Gli esseri umani sono esseri emotivi, e l'ingegneria sociale è un modo molto efficace per approfittarne. Inoltre, gli attacchi di ingegneria sociale di solito non richiedono competenze tecniche altamente specifiche da parte dell'aggressore. Costringere migliaia di utenti a dare informazioni sensibili o a compiere azioni dannose si è dimostrato finora piuttosto semplice! Non fatevi ingannare - anche voi potreste facilmente diventare un bersaglio.

Nelle pagine seguenti, troverete una panoramica degli attuali trend di ingegneria sociale, così come esempi dei tipi più comuni di attacchi che possono influenzare il modo in cui i dipendenti agiscono online. Imparerete anche come riconoscere questi attacchi e proteggere voi stessi e la vostra azienda.



Le soluzioni di sicurezza devono proteggere dagli attacchi tecnici. L'ingegneria sociale invece si basa principalmente sulla psicologia, sfrutta la fiducia, la paura o la disattenzione delle persone.

Tipi di tecniche di ingegneria sociale

Spear phishing
Una forma mirata di phishing rivolta a un individuo, un'organizzazione o un'azienda specifica. Le tipiche campagne di phishing non prendono di mira le vittime individualmente, sono inviate a centinaia di migliaia di destinatari.

Vishing
Un metodo simile al phishing, ma che utilizza telefonate fraudolente al posto delle e-mail. I criminali informatici spesso si travestono da rappresentanti di banche o compagnie di assicurazione.

Smishing
Un tentativo di ingegneria sociale tramite messaggi di testo SMS. Il più delle volte, il tentativo di smishing mira a reindirizzare i destinatari a un sito web dove vengono raccolti i loro dati. Tuttavia, ci sono anche campagne in cui si chiede alle vittime di inviare dati sensibili in una risposta diretta via SMS.

(S)extortion
la (S)extortion è una truffa via e-mail di lunga data, che cerca di ricattare le vittime usando affermazioni e accuse infondate.

Impersonificazione
La tecnica dell'impersonificazione è la stessa del mondo reale. I criminali informatici contattano i dipendenti, in genere spacciandosi per il loro amministratore delegato, cercando di manipolare le vittime e far compiere loro delle azioni - ordinare e approvare transazioni fraudolente, per esempio.

Scareware
Software che utilizza varie tecniche ansiogene per forzare le vittime a installare ulteriori codici maligni sui loro dispositivi. Per esempio, un falso prodotto antivirus inganna gli utenti a installare un software specifico per rimuovere il problema, mentre in realtà questo programma è di solito dannoso.

Truffe di supporto tecnico
Gli aggressori cercano di vendere servizi falsi, rimuovere problemi inesistenti o installare una soluzione di accesso remoto nei dispositivi delle vittime e ottenere un accesso non autorizzato ai loro dati.

Phishing

Probabilmente vi è già capitato, ad un certo punto della vostra vita, di ricevere un' e-mail che sembrava provenire da una banca o da qualche noto servizio online che chiedeva di confermare le vostre credenziali o il numero di carta di credito. Si tratta di una tecnica di phishing molto comune. Tuttavia, le trappole di phishing cambiano costantemente - e a volte sono difficili da riconoscere.

Il phishing è un tipo di attacco di social engineering in cui il criminale cerca di ottenere le credenziali di accesso, in modo da raccogliere informazioni riservate o distribuire malware. Le campagne di phishing possono prendere di mira un vasto numero di utenti anonimi, una vittima specifica o un piccolo gruppo di vittime con truffe personalizzate (spear phishing). Gli attacchi mirati su specifici individui, per lo più di alto profilo aziendale - come i top manager o i titolari- sono etichettati come "whaling" (i cattivi alla ricerca del "pesce grosso").

I truffatori sanno che c'è una buona probabilità che qualsiasi messaggio venga scansionato per contenuti dannosi dal provider di posta elettronica, che devia tali e-mail direttamente nella cartella di spam. Ecco perché il contenuto dei messaggi fraudolenti cambia così spesso.

Secondo Google, nel mese di marzo 2020 i truffatori hanno inviato agli utenti di Gmail 18 milioni di email di phishing a tema COVID-19 ogni giorno .

Phishing

Da quando la pandemia da coronavirus ha iniziato ad espandersi, i truffatori non hanno perso tempo sfruttando l'incertezza, la paura e la scarsità di forniture generate dalla crisi. A marzo 2020 si è assistito a un'ondata di spam a tema COVID-19, in cui sono stati diffusi malware, sottratte informazioni sensibili o venduti prodotti contraffatti, come rivelato nel ESET Threat Report del primo trimestre 2020.

Non sorprende che la pandemia sia diventata una delle principali esche utilizzate dagli aggressori. La comparsa di ogni crisi crea nuove circostanze, che costituiscono l'ambiente ideale di innovazione per i cybercriminali.

Il 94% dei malware viene inviato tramite email.

Ogni minuto si perdono 17.700 dollari a causa di attacchi di phishing.

Circa 14,5 miliardi di email di spam sono inviate ogni giorno.

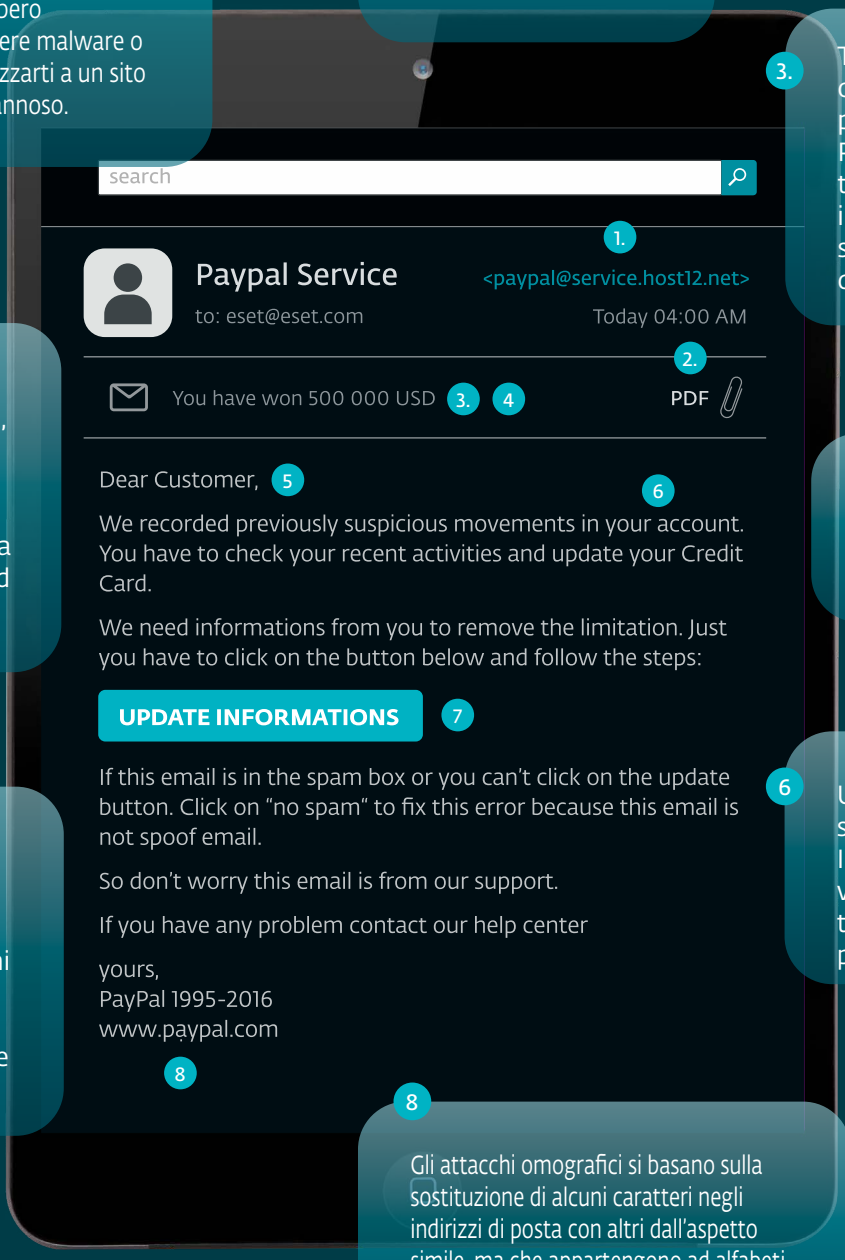
Fonti: CSO, hostingtribunal.com

Principali caratteristiche del phishing

1. Se non conoscete l'indirizzo e-mail, maneggiate il contenuto con cautela.

2. Siate sempre diffidenti da file allegati o link sconosciuti. Potrebbero contenere malware o reindirizzarti a un sito web dannoso.

3. Troppo spaventoso o troppo bello per essere vero? Probabilmente è una truffa... Ricordate che il social engineering si concentra sulle debolezze umane.



4. L'oggetto non è coerente con il messaggio.

5. Se il saluto è troppo generico, potrebbe essere un segno che non era indirizzato solo a voi, ma anche ad altre persone.

6. Un'urgenza sospetta? Il truffatore vuole che tu vada nel panico.

7. Una cattiva ortografia e errori grammaticali sono più comuni nelle email di phishing tradotte da altre lingue.

8. Gli attacchi omografici si basano sulla sostituzione di alcuni caratteri negli indirizzi di posta con altri dall'aspetto simile, ma che appartengono ad alfabeti diversi(come "ạ" contro "a" in paypal.com).

Smishing

Lo Smishing è un tipo di phishing che utilizza servizi di messaggistica, o SMS. Questo fenomeno si è molto diffuso anche durante i primi mesi della pandemia da COVID-19. Nella confusione del momento, per esempio, la gente ha cominciato a ricevere SMS che fingevano di essere messaggi che si spacciavano per messaggi ufficiali dei governi locali.

Lo scopo di questi attacchi è simile al phishing: i criminali informatici mirano **ad ottenere dettagli personali o a indurre la vittima a cliccare su un link di siti web pericolosi**. Un'altra tecnica è quella di fare leva sulla compassione. I criminali informatici inviano messaggi di testo con una richiesta di donazione per persone in situazioni disperate, come un fondo per le vittime di calamità naturali o altro tipo di beneficienza, richiedendo di inserire i dati della carta di credito.

All'inizio, era una sorpresa per molte persone che gli hacker potessero ottenere i loro numeri di telefono a loro insaputa. Ma come molti esperti di sicurezza informatica hanno sottolineato, **è più facile ottenere il numero di telefono di qualcuno che la sua e-mail, perché hanno un numero di opzioni limitato**. Indovinare i nomi degli indirizzi e-mail è più difficile perché permettono più caratteri.

Riuscite a individuare cosa c'è di sospetto in questo SMS?

Una banca probabilmente non manderebbe mai un link diretto come questo. Se avete dei dubbi, potete andare nel vostro online banking e controllare se avete ricevuto lo stesso messaggio. È sempre più sicuro andare su un sito ufficiale piuttosto che cliccare su un link sospetto.

Vishing

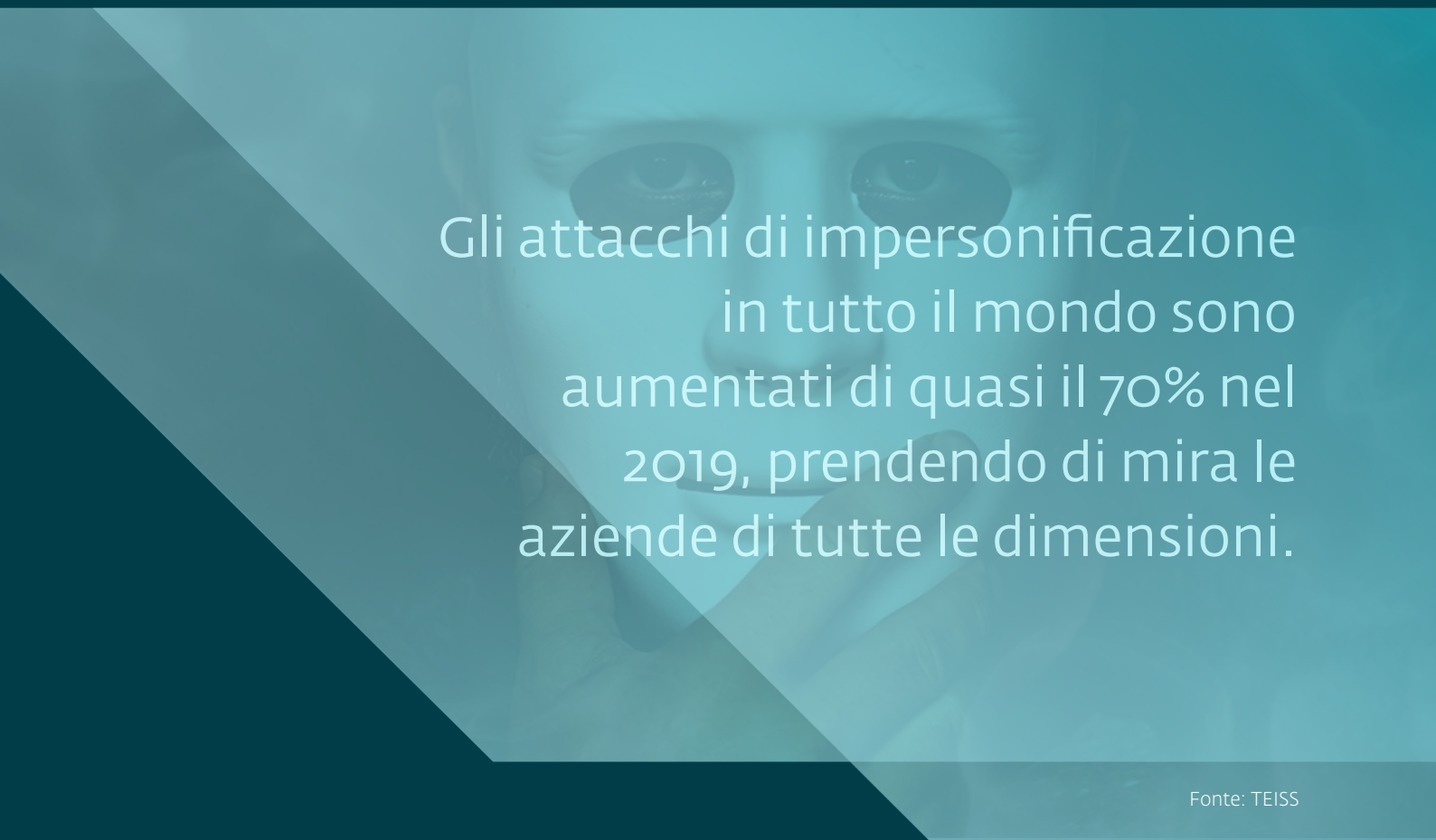
Il Vishing richiede abilità interpretative ancora maggiori rispetto ad altri tipi di truffe. Di solito funziona così: Un truffatore chiama al telefono **fingendosi di essere un rappresentante di un'istituzione ufficiale**. Informano la vittima di un conto bancario compromesso o di un'offerta di prestito non richiesta nel tentativo di ottenere informazioni personali e dettagli finanziari. Troppo bello o troppo brutto per essere vero? Chiedete loro maggiori dettagli, e **non condividete subito nessun dato sensibile**. In alternativa, potete terminare la chiamata e contattare personalmente il servizio clienti della banca, spiegando la situazione.

Impersonificazione: Quando un truffatore si spaccia per l'amministratore delegato

Diamo un'occhiata all'impersonificazione, un altro metodo di attacco non tecnico utilizzato dai criminali informatici per fingersi persone affidabili mentre cercano di manipolare le loro vittime. Come accorgersi se si viene contattati da un criminale informatico invece che da un collega?

L'impersonificazione è definita come la pratica di fingersi qualcun altro - in questo caso, **per ottenere accesso a informazioni di persone, aziende o sistemi informatici**. Per raggiungere questi obiettivi, i cybercriminali usano tra gli altri metodi telefonate, e-mail o applicazioni di messaggistica. In molti casi, i truffatori scelgono nomi del top management dell'azienda e impostano un'email che sembra scritta da un manager.

È abbastanza incredibile quante informazioni aziendali sano disponibili su piattaforme come LinkedIn da cui è possibile ricavare la struttura dell'azienda e i nomi dei suoi dipendenti. Un aggressore può utilizzare tali dati per cercare di contattare diversi dipendenti, **chiedendo loro di effettuare trasferimenti di denaro, pagare fatture o inviare dati importanti**. Ecco perché l'impersonificazione può essere così pericolosa per le aziende, questi attacchi potrebbero causare una violazione dei dati e perdite finanziarie.

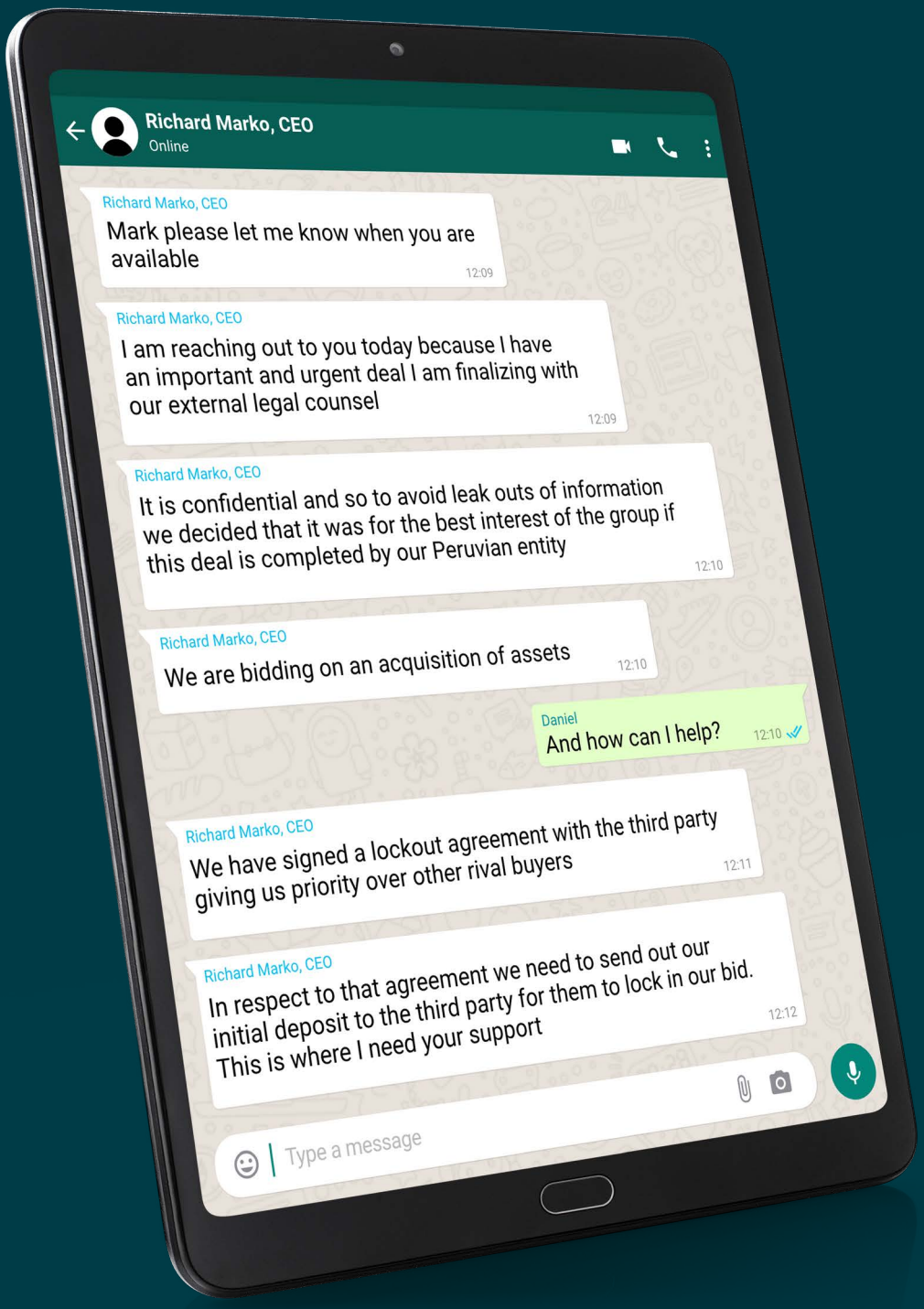


Gli attacchi di impersonificazione in tutto il mondo sono aumentati di quasi il 70% nel 2019, prendendo di mira le aziende di tutte le dimensioni.

Fonte: TEISS

Una storia vera: Attacco di impersonificazione contro ESET

I cyberattacchi possono capitare a qualsiasi organizzazione. Nel 2020, ESET ha subito tentativi di impersonificazione del proprio Amministratore Delegato tramite messaggi WhatsApp. in cui si fingeva l'esistenza di una grande offerta che richiedeva un deposito finanziario.



Come deviare gli attacchi di impersonificazione

Ricordate, la consapevolezza è la chiave. Più sappiamo sugli attacchi di impersonificazione, più possiamo evitarli. Vediamo come funzionano le e-mail di impersonificazione. Molti cercano di instillare un senso di urgenza e di paura. Questo sentimento induce le vittime ad eseguire il compito richiesto fra cui attività insolite e sospette, come acquisti non legati alla propria azienda con clienti che non conosciuti. Di solito criminali informatici cercano anche di stabilire una breve scadenza per i compiti richiesti.

I messaggi fraudolenti contengono spesso errori grammaticali o un utilizzo scorretto del marchio aziendale. Tuttavia, quelli sono solo i più facili da individuare. Gli aggressori abili nelle tecniche di impersonificazione più avanzata potrebbero creare un messaggio di posta elettronica molto realistico, includendo una foto o una firma ufficiale del dipendente alla fine di un'e-mail. Quindi, anche se l'aspetto appare autentico, siate cauti se trovate strana la richiesta nel messaggio.

NON PERDETE DI VISTA IL CONTESTO

A volte, siamo troppo occupati e prendiamo decisioni senza pensarci troppo. Forse serve qualche secondo in più, ma considerate sempre se l'email ricevuta abbia davvero un senso. Perché, esattamente, questo sta chiedendo proprio questo acquisto o questa informazione personale sensibile? **Qualsiasi cosa insolita e che si discosta dai processi tradizionali dovrebbe essere un segnale di avvertimento**. Anche se l'e-mail proviene apparentemente da una persona affidabile come il CEO, potrebbe essere una frode. Resta vigile e verifica qualsiasi richiesta con altri colleghi.

FUORI DALL'UFFICIO?

A volte, i criminali informatici possono venire a sapere che qualcuno è fuori ufficio e agire come se lo stessero sostituendo. In questo caso, verificate le informazioni in questione con il loro superiore o con i colleghi. Pensa sempre almeno due volte prima di agire.

Come deviare gli attacchi di impersonificazione

CONTROLLA L'INDIRIZZO E-MAIL

Ricevere un'email aziendale da un account personale? L'indirizzo e-mail potrebbe apparentemente appartenere a qualcuno che conosci. Ma è sempre meglio rispondere a quella persona al suo indirizzo email ufficiale. Inoltre, a volte, gli hacker possono usare un'email che sembra quasi un indirizzo aziendale ufficiale con solo una piccola differenza, ad esempio sostituendo "m" con "rn"

Implementare il tag "EXTERNAL

Con una recente modifica della sicurezza interna di ESET, le e-mail provenienti dall'esterno del dominio aziendale sono sempre etichettate come EXTERNAL. Sebbene questo sistema non sarebbe utile nel caso in cui il truffatore stia fingendo di inviare l'email dall'indirizzo privato del CEO, potrebbe comunque aiutare a identificare le email che cercano di falsificare il dominio aziendale (come il caso "m" e "rn").

VERIFICARE LA PERSONA ATTRAVERSO UN ALTRO CANALE DI COMUNICAZIONE

Se avete ricevuto un messaggio sospetto su WhatsApp, dovreste scrivere alla persona tramite un'email aziendale o richiamarla. In alternativa, si può anche comunicare **direttamente con la persona faccia a faccia**. Non preoccupatevi di disturbare qualcuno, anche quando potrebbe essere occupato. Per esempio, potreste essere riluttanti a disturbare il vostro Amministratore Delegato. Questo è naturale, perché più alta è la posizione di un collega, più esitiamo a contattarlo, specialmente quando è fuori ufficio. In questo caso, **considerate la possibilità di consultare un altro collega o un superiore**. Per esempio, il vostro CFO o COO dovrebbe essere a conoscenza del pagamento urgente di una corposa fattura in ritardo, quindi confrontatevi con loro. Ricordate: la prudenza ripaga sempre.

"Ciao, amico mio. Tu non mi conosci, ma io ti conosco molto bene. Meglio di quanto tu creda. Questa è la tua password, vero?"

Email come questa possono apparire nella casella di posta elettronica di chiunque. Il misterioso ricattatore in genere sostiene di aver spiato la sua vittima tramite la sua stessa webcam durante la visione di contenuti per adulti. Così l'hacker minaccia la vittima affinché paghi il suo silenzio, altrimenti svelerà il segreto a famiglia e colleghi (sexstortion). Per dimostrare che sono davvero entrati nel PC, forniscono una qualche password utilizzata dalla vittima. Gli atti di sexstortion si basano prevalentemente sul raggiro.

UN PERIODO D'ORO PER LE TRUFFE DI (S)EXTORTION

Un esempio lampante di come gli hacker abusano della tecnologia e delle crisi per diffondere attacchi è di certo la pandemia da COVID-19. Ora che molte aziende si sono spostate sul lavoro in remoto e sugli uffici casalinghi, dove i dipendenti non sono protetti dalla rete aziendale, il numero di minacce sul web è aumentato. Ad esempio, alcuni cybercriminali hanno minacciato di infettare le vittime e i loro famigliari col coronavirus se non avessero ceduto alle minacce.

Pagando le cifre richieste, non farete altro che perdere denaro e alimentare il business di questi criminali, aiutandoli a fare molti altri scam.

CAPIRE LE INTENZIONI DEL TRUFFATORE

Dovreste sapere che l'obiettivo principale delle email di sextortion è far pagare la vittima, preferibilmente in Bitcoin, permettendo agli hacker di ricevere il denaro in forma anonima. Le truffe sono un ottimo giro d'affari: Secondo l'Internet Crime Complaint Center dell'FBI, nel 2020, la truffe di (s)extorsion via e-mail hanno causato perdite per circa 70,9 milioni di dollari.

SAPERE COME REAGIRE ALLE TRUFFE DI (S)EXTORTION

Non inviate denaro, non rispondete e non cliccate su nessun link o allegato. Se cadete vittima di una truffa di (s)extortion, informa sempre i dipartimenti IT o di sicurezza interna dell'azienda. E, se possibile nel vostro Paese, segnalate immediatamente l'incidente (ad esempio, nel Regno Unito è possibile segnalare tali casi online all'Action Fraud, mentre negli USA è possibile sporgere reclamo sul sito dell'FBI).

La migliore prevenzione è quella di creare una password forte o una passphrase. Inoltre, il business della compravendita di password è la ragione per cui è necessario aggiornare le password regolarmente o utilizzare ulteriori fattori di protezione (autenticazione a più fattori).

SE LA PASSWORD È GIUSTA, NIENTE PANICO

Menzionare una password reale è solo una delle tecniche atte a preoccupare la vittima. Gli aggressori possono conoscere la vostra password, ma probabilmente è la sola cosa che hanno a disposizione. Probabilmente hanno comprato la password sul dark web, o potrebbe essere trapelata in seguito a una violazione dei dati.

NON SOTTOVALUTARE LE MINACCE ALLA SICUREZZA LEGATE AL LAVORO DA REMOTO

I luoghi di lavoro e gli uffici flessibili sono fantastici, ma solo se sono ben protetti e se si sa come gestirli. Le reti Wi-Fi sono altamente soggette ad attacchi, quindi se volete essere sicuri che la connessione e i dati aziendali siano al sicuro, è consigliabile usare una rete privata virtuale (VPN), che ti permetta di creare una connessione sicura alla rete aziendale.

Come fanno gli hacker ad accedere al vostro pc e alla vostra webcam?

Se gestite con attenzione, le truffe di (s)estorsione non fanno danni. Tuttavia, dovreste sapere che esiste un modo in cui gli hacker riescono ad accedere alle vostre webcam. Fanno spesso uso di un malware, per esempio un Trojan, per infettare il vostro dispositivo con un software di remot desktop, ma avranno bisogno della vostra collaborazione. A volte, è sufficiente scaricare qualche software sconosciuto. Pensi di avere scaricato quel che volevi, ma potrebbe esserci un malware nascosto all'interno del file. E così, inconsapevolmente avete aiutato gli hacker a infettare il vostro dispositivo. Non aspettatevi di vedere la luce della webcam accendersi appena iniziano a spiarvi. In questo modo non sarebbero più in incognito, no?

Se il vostro computer è stato infettato, l'hacker non solo può vedere i momenti intimi della vostra vita, ma può anche accedere a dati e documenti riservati o registrare le vostre discussioni nel caso in cui abbia anche violato il vostro microfono.

Come reagire a un messaggio di (S)extorsion

1. Agite con calma e cautela, evitando manovre avventate.
I criminali dietro le truffe di sextortion prendono di mira le umane debolezze nel tentativo di spingervi ad azioni lesive. Di conseguenza, se ricevete un messaggio che istiga paura, fermatevi e valutate la possibilità che nulla di quanto contenuto in quella e-mail sia effettivamente vero. Se vi rimangono dei dubbi, rivolgetevi sempre al reparto IT o all'assistenza tecnica del vostro provider di sicurezza.

2. Non pagate i sex-estorsori.
Le email di sextortion sono in genere semplici truffe. Questo significa che non c'è nulla di vero nelle affermazioni di questi criminali; quasi certamente non possiedono video su di voi o su ciò che avete guardato, non collaborano con le forze dell'ordine e non hanno ordinato a qualcuno di "provarci con voi".

3. Non interagite in nessun modo con l'e-mail ricevuta.
Non rispondete allo scam, non scaricatene gli allegati, non cliccate su nessun link presente né interagite con nessuno dei contenuti dell'email, perché sono elementi che possono portare a malware o altre minacce.

4. Controllate/modificate la vostra password.
In alcuni casi i criminali testano le credenziali rubate e, se funzionano usano l'account violato quantomeno per diffondere i loro messaggi. Perciò, se il criminale menziona una qualsiasi delle vostre password in uso, cambiatela immediatamente ed attivate l'autenticazione a più fattori, così da aumentare la protezione.

5. Inoltrate l'e-mail al vostro reparto IT.
Se la vostra azienda non dispone del personale IT, la misura minima da adottare è effettuare una scansione del computer e della rete con una soluzione di sicurezza affidabile e assicurarvi che nessuna delle password sia stata rubata o compromessa.

6. Mettete in sicurezza la webcam.
Per evitare possibili usi impropri della webcam integrata, usate un software di protezione o, almeno, coprite l'obiettivo con del nastro adesivo. Avrete così la certezza che i criminali non possano in alcun modo registrare un video su di voi davanti al dispositivo.

7. Utilizzate una soluzione anti-spam.
Un prodotto di sicurezza affidabile con funzionalità anti-spam potrà aiutarvi in futuro a impedire nuove email di sextortion nella casella di posta.

Altre di tecniche di ingegneria sociale da conoscere

Scareware è un tipo di malware che cerca di indurre le vittime ad acquistare e scaricare un software potenzialmente pericoloso. È un metodo che attira molto rapidamente l'attenzione della gente...spaventandola. Annunci pop-up difficili da chiudere, società di software con nomi che non avete mai sentito e scansioni non autorizzate del vostro computer alla ricerca di virus - tutti questi sono caratteristiche tipiche dello scareware.

Il problema è che tali programmi di solito mostreranno una lista di decine o centinaia di virus fasulli. I programmi scareware in realtà non scansionano il vostro computer, e questi presunti risultati sono del tutto falsi. Gli avvertimenti su una presunta infezione non fanno altro che manipolare l'utente e indurlo a scaricarne una reale. Queste truffe spesso si basano su falsi software di sicurezza, come Advanced Cleaner, SpyWiper, o System Defender.

Affidatevi a prodotti software conosciuti, testati e aggiornati

Così, sarete più consapevoli che un invito a scaricare un software gratuito potrebbe essere una truffa. È anche molto utile attivare un blocco dei pop-up sui dispositivi di lavoro e filtri URL. Stabilire strumenti di sicurezza web e firewall per bloccare gli aggressori sul nascere.

Le truffe di supporto tecnico sono strettamente legate allo scareware. Ma a differenza degli scareware, fingono di provenire da un'azienda affermata come Microsoft. Non inizieranno automaticamente la scansione del vostro computer. Potrebbero invece chiedervi di aprire alcuni file - per poi dirvi che quei file mostrano un problema... che in realtà non esiste. Secondo la US Federal Trade Comission (FTC), le truffe di supporto tecnico sono piuttosto frequenti. Nel 2019, la FTC ha ricevuto più di 100.000 segnalazioni di questo genere di truffe.

Checklist per gli amministratori IT

5 modi per proteggere la vostra organizzazione da attacchi di ingegneria sociale

1. Formazione regolare sulla sicurezza informatica per TUTTI i dipendenti, compreso il top management e il personale IT. Ricordate che tale formazione dovrebbe mostrare o simulare scenari di vita reale. I punti di apprendimento devono essere perseguibili e, soprattutto, attivamente testati al di fuori della sala di formazione.

2. Scansionate le password deboli che potrebbero potenzialmente diventare una porta aperta per gli aggressori nella vostra rete aziendale. Inoltre, proteggete le password con un altro livello di sicurezza implementando l'autenticazione a più fattori.

3. Implementate soluzioni per gestire le truffe telematiche in modo che i messaggi di spam e phishing vengano rilevati, messi in quarantena, neutralizzati e cancellati. Le soluzioni di sicurezza, comprese molte di quelle fornite da ESET, dispongono di alcune o di tutte queste capacità.

4. Create politiche di sicurezza comprensibili che i dipendenti siano in grado di attuare e che li aiutino a identificare i passi da compiere nel caso in cui debbano affrontare episodi di social engeeniring

5. Utilizzate una soluzione di sicurezza e strumenti amministrativi, come ESET PROTECT Console, per proteggere gli endpoint e le reti della vostra organizzazione, dando agli amministratori la piena visibilità e la capacità di rilevare e mitigare le potenziali minacce nella rete.

Da oltre 30 anni, ESET® è leader nello sviluppo di software e servizi di sicurezza IT per proteggere aziende e utenti finali in tutto il mondo. Con soluzioni che spaziano dalla sicurezza di endpoint e dispositivi mobili, alla crittografia e all'autenticazione a due fattori, i prodotti ESET offrono prestazioni elevate e sono facili da usare, proteggono e monitorano in modo discreto 24/7 i propri clienti, aggiornando le difese in tempo reale per mantenere gli utenti al sicuro ed evitare interruzioni alle attività aziendali. Per maggiori informazioni visita www.eset.com/it/