proofpoint.

DOCUMENTO DI SINTESI

State of the Phish 2020

L'email è il canale di comunicazione più importante per le aziende, ma oggi è anche il principale vettore per le minacce.

È il canale tramite il quale i pirati informatici hanno le maggiori probabilità di violare i loro bersagli: i tuoi collaboratori. Utilizzando un'ampia gamma di tecniche di phishing, inducono gli utenti a fare clic su un link non sicuro, a divulgare le proprie credenziali o addirittura a eseguire direttamente un ordine (come trasferire dei fondi o inviare file sensibili).

Per meglio comprendere questa minaccia, la sesta edizione del nostro report *State of the Phish* mette in evidenza i risultati delle indagini condotte su utenti finali e professionisti della sicurezza e dell'analisi di oltre 50 milioni di email di phishing simulato inviate dai nostri clienti ai loro utenti nel corso di 12 mesi. Valutiamo ciò che gli utenti sanno in merito ai termini e alle pratiche della sicurezza informatica. Analizziamo le minacce di phishing che i team della sicurezza delle informazioni devono affrontare. Infine, mostriamo come le aziende possono adottare un approccio incentrato sulle persone per gestire le attuali minacce di phishing.

Ecco i nostri risultati principali.

Consapevolezza degli utenti: sondaggio globale su 3.500 lavoratori adulti

- Solo il 61% ha correttamente individuato la definizione di phishing in un questionario a risposta multipla.
- Solo il 31% ha individuato correttamente la definizione di ransomware.
- I "millennial" continuano a conseguire risultati peggiori di altre fasce di età (compresi i "baby boomer") nel riconoscimento dei termini principali.
- Molti degli interpellati non applicano le buone norme in materia di sicurezza informatica:
  - Il 45% ha ammesso di riutilizzare la stessa password.
  - Oltre il 50% non protegge con una password la rete Wi-Fi domestica.
  - Il 32% non sa cosa sia una rete privata virtuale (VPN).
- Il 90% degli lavoratori adulti ha ammesso di usare i dispositivi forniti dal datore di lavoro per attività personali. Quasi il 50% ne consente l'utilizzo ad amici e familiari.

Le sfide informatiche: sondaggio globale su 600 professionisti della sicurezza delle informazioni

- Nel 2019 il 55% delle aziende ha subito almeno un attacco di phishing.
- La maggior parte delle aziende ha affrontato attacchi di social engineering che utilizzano diversi metodi:
  - Spear phishing: 88%
  - Violazione dell'email aziendale (BEC): 86%
  - Social media: 86%
  - SMiShing (phishing tramite SMS/testo): 84%
  - Vishing (phishing tramite chiamate telefoniche): 83%
  - Infezioni tramite chiavetta USB: 81%
- Nel 2019 il 33% delle aziende infettate dal ransomware nel mondo ha scelto di pagare il riscatto (un altro 32% ha subito l'infezione ma non ha pagato). Fra quelle che hanno negoziato:
  - Il 9% ha ricevuto ulteriori richieste di riscatto.
  - Il 22% non ha più avuto accesso ai propri dati, neanche a seguito del pagamento.
- L'85% delle aziende non offre agli utenti un tasto per la segnalazione delle email. Ciò rende più difficile per gli addetti alla sicurezza coinvolgere gli utenti nella difesa contro il phishing.
- Il 78% delle aziende ha affermato di poter quantificare un'apprezzabile riduzione della vulnerabilità al phishing grazie alle proprie attività di security awareness training.

Le azioni degli utenti: analisi dei dati Proofpoint

- Nel 2019 gli utenti finali dei clienti di Proofpoint hanno segnalato quasi 9,2 milioni di email sospette, un aumento del 67% rispetto al 2018. Nel solo terzo trimestre 2019 gli utenti hanno segnalato agli addetti alla sicurezza migliaia di gravi minacce:
  - Quasi 20.000 attacchi di phishing basati sulle credenziali
  - Oltre 4.000 attacchi contenenti malware, trojan di accesso remoto (RAT), backdoor e stealer (ladri di informazioni) ad alto rischio
- Tassi di denuncia più elevati indicano che gli utenti prestano maggiore attenzione alle esche utilizzate dal phishing e quindi una maggior propensione ad avvisare gli addetti alla sicurezza in merito ai messaggi sospetti. Ciò contribuisce a rafforzare le difese complessive contro il phishing. Pertanto, quando si analizzano i risultati dei test di phishing simulato per valutarne il successo, è meglio concentrarsi sui tassi di segnalazione piuttosto che su quelli di errore. Per esempio:
  - Gli utenti nei settori di finanza e istruzione hanno riportato la stessa percentuale media di insuccesso negli attacchi di phishing simulati: 8%.
  - Facendo un confronto, le società finanziarie hanno avuto il tasso di segnalazioni più elevato (20%) nelle prove di phishing, mentre le organizzazioni nell'ambito dell'istruzione il più basso (5%).
- Obiettivi e metodi degli aggressori possono cambiare molto nel corso del tempo, e le persone più attaccate ovvero Very Attacked People™ (VAP) di un'azienda non corrispondono sempre alle perone che ricoprono i ruoli più importanti in azienda (VIP).
- Le aziende devono adottare un approccio alle proprie vulnerabilità più incentrato sulle persone e permettere agli utenti di diventare una linea di difesa più solida. Devono esser consapevoli del fatto che qualsiasi utente può diventare un bersaglio in qualsiasi momento e devono utilizzare i loro dati e le informazioni sulle minacce per sviluppare un programma di security awareness training che riguardi sia l'azienda a livello complessivo, sia i diversi tipi di utenti colpiti con corsi mirati.

Principali risultati: Stati Uniti

- Solo il 49% degli impiegati statunitensi ha correttamente individuato la definizione di phishing.
- I dipendenti statunitensi sono inoltre quelli che si fidano di più delle reti Wi-Fi pubbliche: il 45% ritiene che luoghi di fiducia (come caffè e alberghi) offrano sempre delle reti sicure.
- Oltre il 70% permette ad amici e familiari di usare i dispositivi forniti dal datore di lavoro.

Principali risultati: EMEA

- I dipendenti tedeschi sono stati i più propensi a identificare correttamente la definizione di phishing (66%).
- I dipendenti francesi sono stati i migliori nel riconoscere le definizioni di SMiShing (54%) e vishing (48%).
- Quelli spagnoli hanno mostrato molta familiarità con la definizione del malware (79%), ma pochissima con quella del ransomware (22%).
- I dipendenti britannici sono risultati quelli meno informati sulla protezione delle reti Wi-Fi: il 21% ha affermato di non adottare misure di sicurezza per la propria rete domestica perché non sa come fare.
- Le aziende del Regno Unito sono quelle più inclini a imporre una sanzione economica ai dipendenti che restano vittime ripetutamente degli attacchi di phishing (21%). Le aziende francesi sono i più propensi a licenziare i "recidivi" (13%).
- Nel 2019 tutte le aziende spagnole hanno subito attacchi di SMiShing e basati sui social.
- Oltre la metà delle aziende tedesche che hanno scelto di pagare il riscatto dopo aver subito un attacco di ransomware non ha più avuto accesso ai propri dati.

Principali risultati: APAC

- I dipendenti australiani sono stati i più inclini a riconoscere la definizione corretta di ransomware (42%).
- Il 34% dei dipendenti australiani non sente la necessità di usare una VPN su nessuno dei propri dispositivi.
- Solo il 60% delle aziende australiane ha affermato di aver subito nel 2019 un attacco social, di SMiShing e di vishing, una percentuale ben al di sotto delle medie globali.
- Oltre il 20% dei dipendenti giapponesi ha affermato di utilizzare più volte una o due password per i propri account online.
- I giapponesi sono inoltre quelli con la percentuale più bassa nell'identificazione della definizione di SMiShing (17%).
- Nel 2019 solo il 42% delle aziende giapponesi ha subito un attacco di phishing andato a buon fine (molto al di sotto della media globale pari al 55%).
- Solo il 10% di esse ha pagato un riscatto a seguito di un'infezione di ransomware nel 2019.

APPROFONDISCI

Per maggiori informazioni visita **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.