proofpoint.

Il report State of The Phish in breve

INTRODUZIONE

In circostanze normali, la cybersecurity può essere ardua. In tempi eccezionali - come la pandemia che ha portato una serie di cambiamenti drastici nei nostri ambienti di lavoro - può diventare estremamente complicata. Lo scorso anno, i professionisti della sicurezza delle informazioni hanno affrontato un'esplosione di truffe di phishing legate al tema del coronavirus e a un costante aumento degli attacchi di ransomware, dovendo al contempo proteggere gli utenti durante la loro repentina migrazione al telelavoro.

Il nostro report *State of the Phish* 2021 prende in esame queste tendenze e altri argomenti. Analizza i dati raccolti da sondaggi, simulazioni di attacchi di phishing e attacchi informatici reali per offrire una chiara visione delle minacce attuali più devastanti e delle principali vulnerabilità degli utenti. Inoltre, fa il punto sulle misure da adottare per proteggersi.

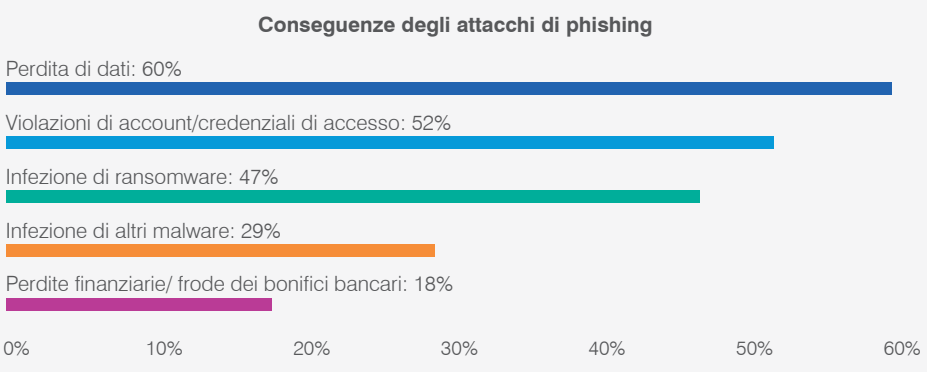
Quella che segue è una panoramica dei principali risultati del report.

LE MINACCE STANNO AUMENTANDO

Il 2020 è stato un anno eccezionale per gli attacchi di phishing, che hanno fatto numerose vittime utilizzando diverse tecniche.

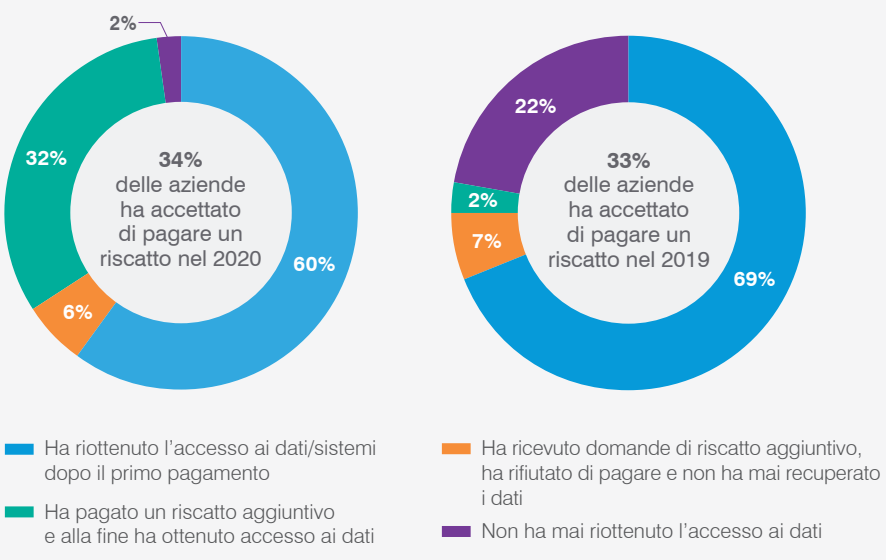
57%

dei professionisti intervistati in un sondaggio indipendente ha dichiarato che la loro azienda è stata vittima di un attacco di phishing andato a buon fine nel 2020, rispetto al **55%** nel 2019.



Una percentuale leggermente più elevata di vittime di ransomware ha pagato il riscatto per riottenere l'accesso ai dati e ai sistemi. Un numero inferiore tuttavia ha ottenuto ciò che era stato loro promesso, e quasi un terzo alla fine ha pagato un riscatto aggiuntivo.

Risultati a seguito del pagamento di riscatti (2020 e 2019)



INTERNAZIONALE

68% delle aziende statunitensi ha ammesso di aver pagato un riscatto nel 2020, il doppio rispetto alla media globale.

41% delle aziende spagnole ha rifiutato di pagare un riscatto dopo aver subito un'infezione, il che le rende le meno propense a negoziare con i criminali informatici.

78% delle aziende francesi è riuscito a riottenere l'accesso a dati e sistemi dopo aver pagato un unico riscatto, la percentuale più elevata di tutti i paesi esaminati (gli Stati Uniti occupano il secondo posto con il **76%**).

14% delle aziende tedesche ha rifiutato di pagare un riscatto aggiuntivo, la percentuale più elevata tra le nazioni incluse nel sondaggio.

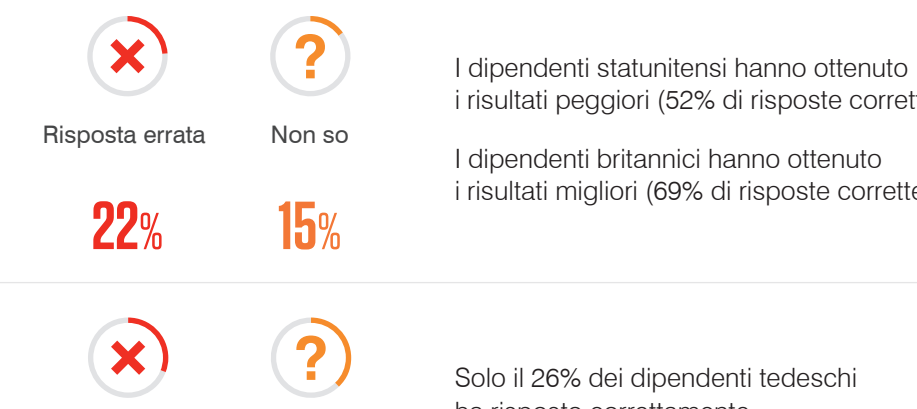
PRINCIPALI VULNERABILITÀ DEGLI UTENTI

Gli attacchi di oggi prendono di mira le persone, non soltanto la tecnologia. Risulta fondamentale identificare le principali vulnerabilità degli utenti per rafforzare la loro resilienza.

Oltre un utente su dieci ha fatto clic su un'email di simulazione di un attacco di phishing, mentre uno su cinque si è lasciato ingannare da un'email di simulazione di un attacco di phishing contenente un allegato.

Percentuale media di insuccesso sui test di phishing dell'11%

Tipi dei modelli di phishing: percentuali medie di insuccesso



Gli utenti di alcuni settori sono più vulnerabili di altri. Lo stesso vale per i diversi dipartimenti.

Percentuale media di insuccesso per settore

Percentuale media di insuccesso per dipartimento

I termini di cybersecurity comuni possono sembrare ovvi per i responsabili informatici, ma molti utenti non li comprendono.

Il nostro sondaggio sulla definizione di alcuni dei termini di sicurezza informatica proponeva un questionario a scelta multipla (tre) e l'opzione "Non so". Gli utenti che non conoscono la risposta possono presentare dei rischi tanto quanto coloro che forniscono la risposta sbagliata.

Cos'è il **PHISHING?**

Risposta corretta	Risposta errata	Non so
63%	22%	15%

I dipendenti statunitensi hanno ottenuto i risultati peggiori (52% di risposte corrette).

I dipendenti britannici hanno ottenuto i risultati migliori (69% di risposte corrette).

Cos'è il **RANSOMWARE?**

Risposta corretta	Risposta errata	Non so
33%	36%	31%

Solo il 26% dei dipendenti tedeschi ha risposto correttamente.

Il 42% dei dipendenti australiani ha risposto correttamente.

Cos'è il **MALWARE?**

Risposta corretta	Risposta errata	Non so
65%	21%	14%

I dipendenti spagnoli hanno ottenuto i risultati migliori (75% di risposte corrette).

I dipendenti statunitensi hanno ottenuto risultati al di sotto della media (54% di risposte corrette).

MISURE ADOTTATE DALLE AZIENDE

Anche se non suggeriamo di punire gli utenti per gli errori che commettono in buona fede, alcune aziende utilizzano un modello disciplinare per i recidivi:

Misure disciplinari per i recidivi

INTERNAZIONALE

82% delle aziende statunitensi ha implementato un modello disciplinare, la percentuale più elevata tra i paesi presi in esame.

72% delle aziende australiane richiede alle Risorse Umane di intraprendere azioni disciplinari per i recidivi.

35% delle aziende spagnole ha implementato un modello disciplinare, la percentuale più bassa tra i paesi presi in esame.

32% delle aziende britanniche ha affermato che il loro modello disciplinare non ha avuto alcun impatto sulla consapevolezza dei dipendenti.

30% delle aziende statunitensi è ricorso al licenziamento come misura disciplinare, la percentuale più elevata tra i paesi presi in esame.

SCARICA IL REPORT COMPLETO

Desideri saperne di più? Il report *State of the Phish* 2021 include dati provenienti da:

Un'inchiesta indipendente condotta tra	Un'inchiesta indipendente condotta tra	Oltre	Circa
3.500 adulti attivi in sette paesi (Australia, Francia, Germania, Giappone, Regno Unito, Spagna e Stati Uniti)	**600** professionisti della sicurezza informatica negli stessi sette paesi	**60 milioni** di simulazioni di attacchi di phishing inviati dai nostri clienti in un periodo di 12 mesi	**15 milioni** di email segnalate dagli utenti dei nostri clienti

Scarica il report per ottenere una fotografia dettagliata delle attuali minacce di phishing e i passi da intraprendere per implementare una strategia di cybersecurity incentrata sulle persone che ti aiuti a ridurre i rischi e a rafforzare la consapevolezza e la resilienza degli utenti.

www.proofpoint.com/it/resources/threat-reports/state-of-phish

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity e nella conformità, 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**.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.

proofpoint.