Approfondimenti Sul Phishing 2021

Anche se ha più di un quarto di secolo, il phishing resta ancora oggi una tecnica di attacco informatico estremamente efficace, principalmente perché continua ad evolversi. I cybercriminali sono molto abili ad identificare velocemente nuove opportunità di phishing (come quelle fornite dalla pandemia) ed a sviluppare nuove tattiche e tecniche di attacco.

Per le organizzazioni, il phishing è in molti casi il primo stadio di un attacco complesso e a fasi multiple. Spesso i cybercriminali sfruttano il phishing per ingannare gli utenti e indurli a installare malware o a condividere le proprie credenziali di accesso alla rete della vittima. Una semplice e-mail dall'aspetto innocuo può portare a un attacco di ransomware, cryptojacking o furto di dati.

Questo report espone i nuovi approfondimenti sul phishing, in base ai risultati di un sondaggio indipendente condotto tra 5.400 IT Manager in tutto il mondo che lavorano in prima linea nell'ambito della sicurezza informatica. Inoltre, esamina un caso reale di un attacco di phishing che ha portato ad una richiesta di riscatto di vari milioni di dollari.

Secondo il Data Breach Investigation Report di Verizon per il 2021, il 36% dei casi di violazione confermati deriva dal phishing (in aumento rispetto al 25% del 2019). I risultati di questo sondaggio possono essere utilizzati per valutare il proprio stato di protezione dal phishing e per identificare nuove opportunità per estendere la sicurezza.

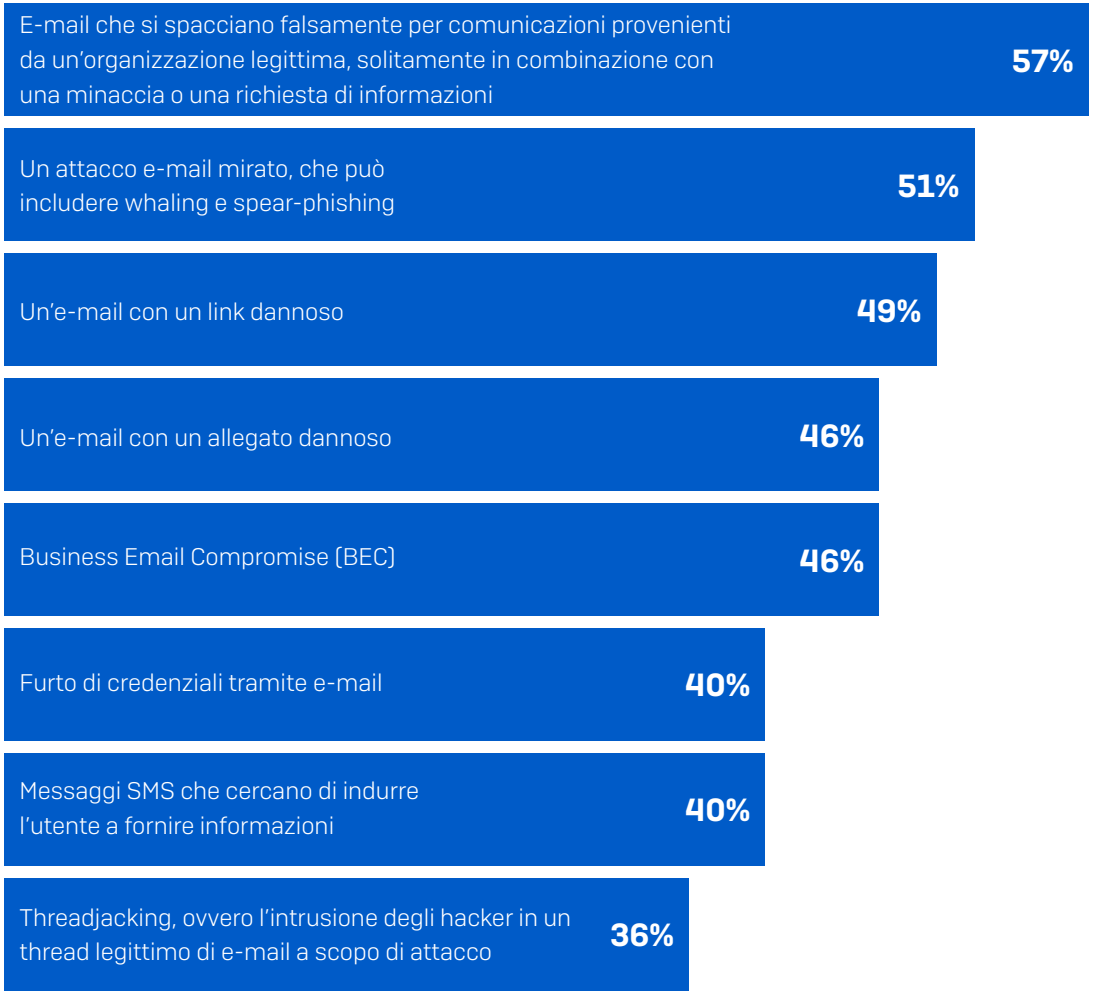
SOPHOS

1. La definizione di phishing varia a seconda delle persone

Che cos'è il phishing? Dal nostro sondaggio è emerso che anche tra i vari IT Manager esiste un'ampia disparità in merito a quello che viene considerato un attacco di phishing. L'interpretazione più comune lo definirebbe come l'*utilizzo di e-mail che si spacciano falsamente per comunicazioni provenienti da un'organizzazione legittima, solitamente in combinazione con una minaccia o una richiesta di informazioni*. Anche se questa è stata la risposta più frequente, meno di 6 partecipanti al sondaggio su 10 (57%) hanno selezionato questa opzione, il che dimostra quanto sia ampia la definizione attribuibile al phishing.

Il 46% degli intervistati classifica come phishing gli attacchi di Business Email Compromise (BEC), mentre più di un terzo (36%) ritiene che il phishing includa il threadjacking, ovvero l'intrusione di hacker in un thread legittimo di e-mail a scopo di attacco.

Quali delle seguenti opzioni ritenete possano essere considerate attacchi di phishing?



Quali di queste opzioni ritenete possano essere considerate attacchi di phishing? [5.400] alcune risposte sono state escluse

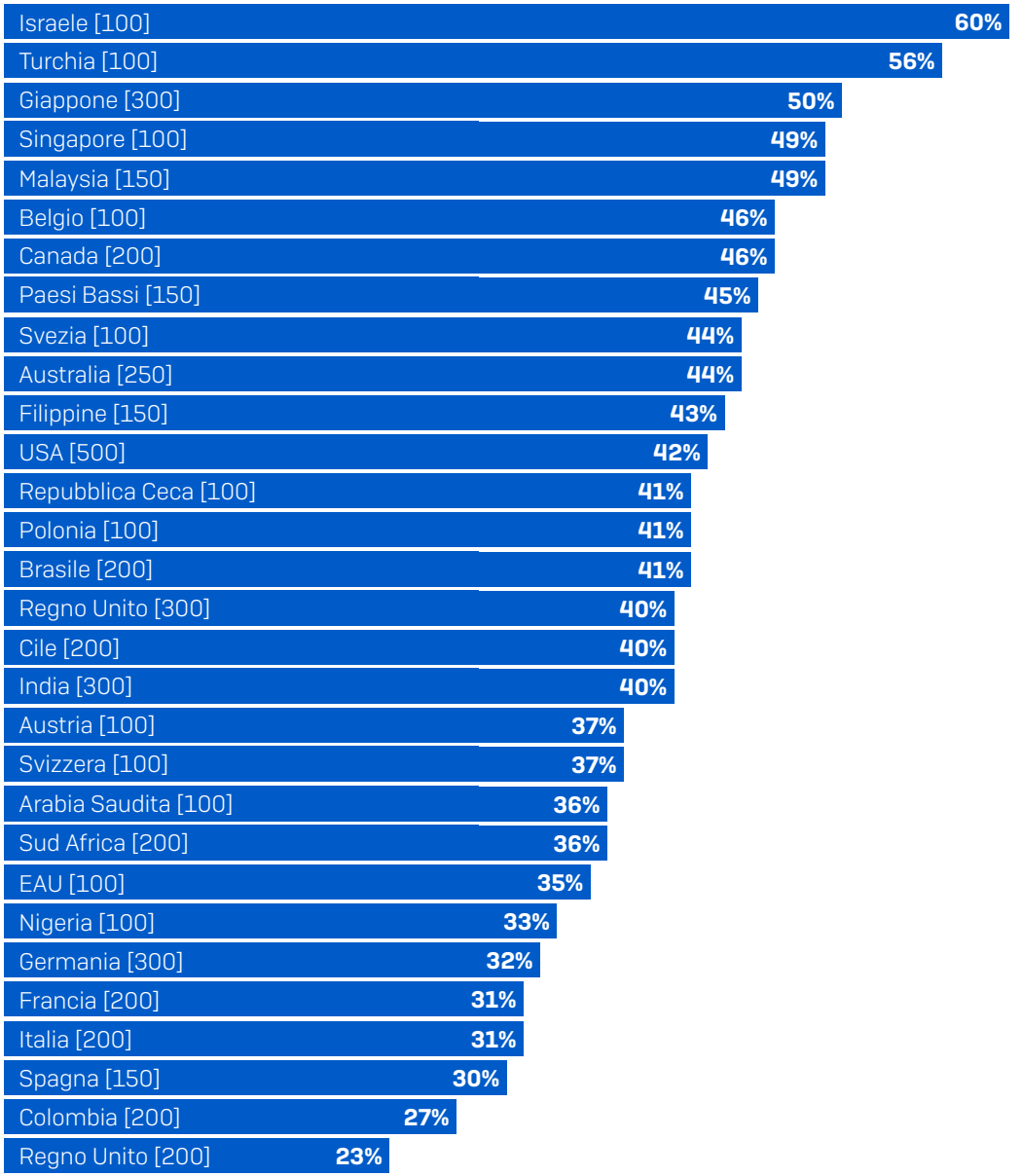
Anche i fattori culturali hanno un'influenza notevole su come viene inteso il phishing. Ad esempio, in Israele la percentuale di partecipanti che definisce come phishing i messaggi SMS che cercano di indurre la vittima a fornire informazioni è doppia rispetto a quella dei partecipanti in Messico (60% vs 23%). Sebbene questo fenomeno sia stato denominato da molti professionisti dell'IT "smishing" anziché "phishing", i messaggi fasulli che fingono di provenire da brand famosi e attendibili hanno le stesse conseguenze, indipendentemente da come vengono trasmessi.

Considerando queste differenze significative nella definizione degli attacchi di phishing tra chi opera in ambito IT, è ragionevole aspettarsi uno spettro di interpretazioni simile o più ampio tra i dipendenti non tecnici.

Capire che il termine "phishing" varia a seconda delle persone è un concetto importante per chiunque crei o conduca programmi educativi mirati alla sensibilizzazione sul phishing. Per realizzare corsi di formazione sul phishing efficaci è importante trovare una definizione di base del termine "phishing", in modo da poter inquadrare nel giusto contesto tutte le nozioni apprese.

CONCLUSIONE: DURANTE LA REALIZZAZIONE DI RISORSE EDUCATIVE E CORSI DI FORMAZIONE VOLTI ALLA SENSIBILIZZAZIONE DEGLI UTENTI, OCCORRE ESSERE CONSCI DEL FATTO CHE LA DEFINIZIONE DEL TERMINE "PHISHING" VARIA A SECONDA DELLE PERSONE. SE NON VIENE INQUADRATA NEL GIUSTO CONTESTO, LA FORMAZIONE AVRÀ UN EFFETTO MINORE RISPETTO A QUELLO ATTESO.

Percentuale di partecipanti che classificano come phishing i messaggi SMS che cercano di indurre l'utente a fornire informazioni



Quali di queste opzioni ritenete possano essere considerate attacchi di phishing? [base di partecipanti indicata nel grafico] Messaggi SMS che cercano di indurre l'utente a fornire informazioni

2. Dall'inizio della pandemia si è riscontrato un forte aumento del phishing

Il 70% dei partecipanti al sondaggio ha osservato, dall'inizio della pandemia, un aumento nel numero di attacchi di phishing contro la propria organizzazione. Tutti i settori sono stati colpiti, con un incremento maggiore nel settore pubblico (77%), seguito a breve distanza dai servizi commerciali e professionali (76%) e dalla sanità (73%).

La variazione minima tra i settori (pari a soli 10 punti percentuali prima degli arrotondamenti) dimostra che i cybercriminali attaccano in maniera indiscriminata, per cercare di colpire quante più persone possibili, al fine di aumentare le probabilità di successo.

Dalle ricerche dei SophosLabs è emerso che i cybercriminali sono stati abili a sfruttare rapidamente le opportunità offerte loro dalla pandemia e dai confini sempre meno nitidi delle modalità di uso lavorativo e privato delle tecnologie. Alcuni esempi includono:

- Il rapido aumento dello smart working. Con molta probabilità, gli hacker si auguravano che le persone avrebbero abbassato la guardia lavorando in smart working da casa, essendo in un ambiente diverso dal proprio ufficio.
- Incremento delle consegne a domicilio. Nei primi mesi della pandemia, quando le persone hanno cominciato a fare più acquisti on-line, i messaggi di phishing camuffati da comunicazioni provenienti da un'azienda di commercio elettronico sono diventati ricorrenti.
- Preoccupazione generale sulla pandemia. I cybercriminali hanno fatto leva sulle paure delle persone e sulla loro necessità di reperire informazioni sul COVID-19, realizzando truffe incentrate sull'argomento della pandemia. Hanno previsto che l'alto livello di preoccupazione avrebbe ridotto la probabilità che la legittimità di un messaggio venisse controllata da un utente prima di cliccare su un link.

Settore	Partecipanti che hanno osservato, dall'inizio della pandemia, un aumento nel numero di attacchi di phishing contro la propria organizzazione
Settore pubblico [117]	77%
Servizi commerciali e professionali [361]	76%
Sanità [328]	73%
Mass media, tempo libero e intrattenimento [145]	72%
Fonti di energia, petrolio/gas e utenze [197]	72%
Vendita al dettaglio [435]	71%
Istruzione [499]	71%
Altro [768]	71%
Pubblica amministrazione [131]	69%
Distribuzione e trasporto [203]	68%
Servizi finanziari [550]	68%
Edilizia e immobili [232]	68%
IT, tecnologie e telecomunicazioni [996]	68%
Industria manifatturiera e produzione [438]	66%

Avete osservato, dall'inizio della pandemia, un cambiamento nel numero di attacchi di phishing contro la vostra organizzazione? [base di partecipanti indicata nel grafico] Sì, un aumento significativo; Sì, un lieve aumento

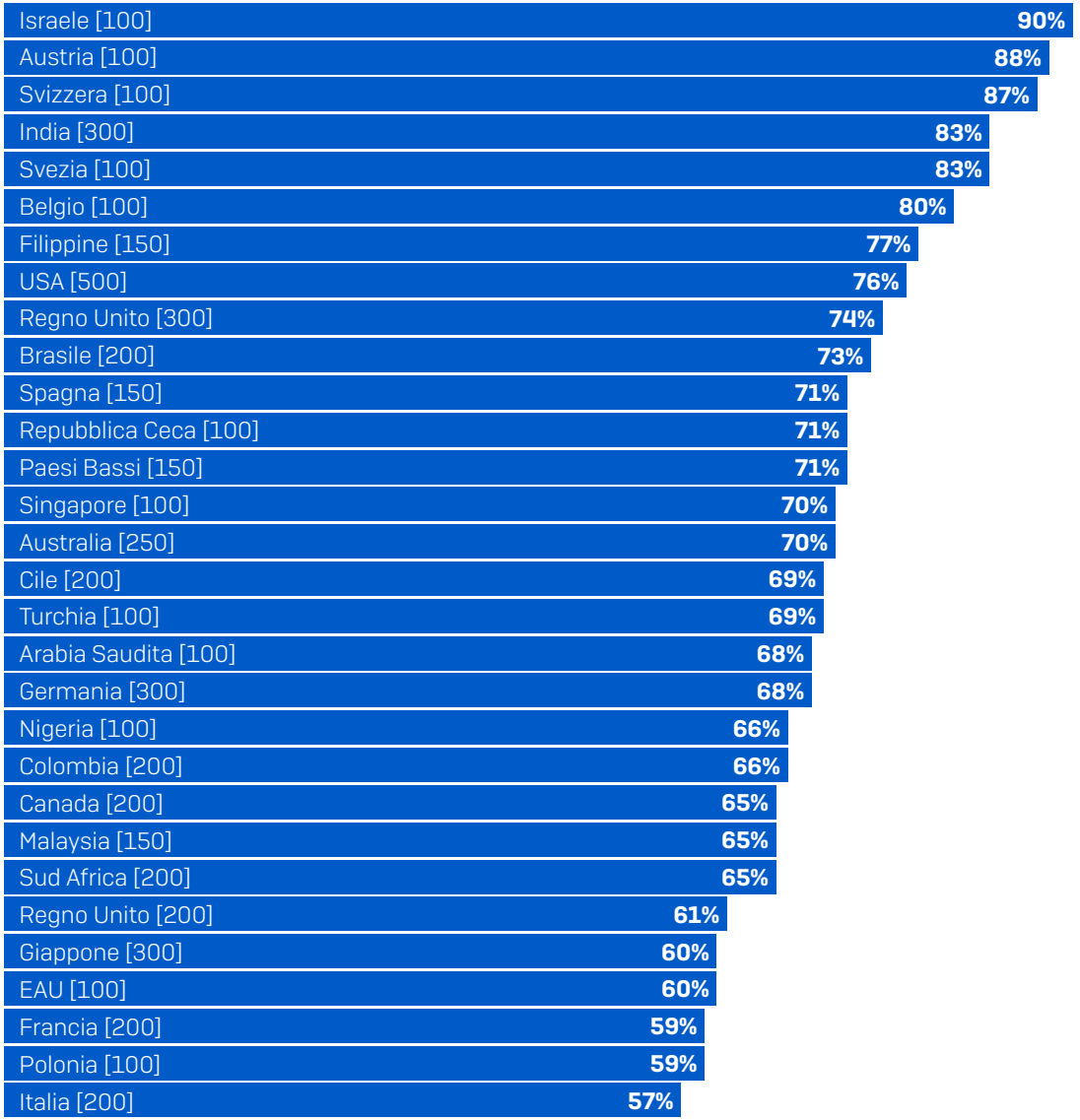
** Prima degli arrotondamenti, l'aumento era stato segnalato dal 76,92% dei partecipanti nel settore pubblico e dal 66,43% nell'industria manifatturiera, con una differenza effettiva pari al 10,48%*

Sebbene la differenza complessiva nei vari settori sia stata minima, dal sondaggio è emerso un divario notevole nell'incremento degli attacchi di phishing registrato, dall'inizio della pandemia, in base al paese. Per esempio, il 90% degli intervistati in Israele ha segnalato un aumento del phishing, rispetto al 57% in Italia. Anche se condizionati dalla definizione di phishing dei partecipanti e dalla loro capacità di monitorare e misurare gli attacchi, questi risultati offrono prospettive importanti sull'esperienza del personale IT che lavora in prima linea nel campo della sicurezza informatica.

Dietro agli innumerevoli tipi di e-mail di phishing si nascondono altrettanti cybercriminali diversi. I gruppi di hacker più abili sferrano principalmente attacchi mirati a vittime in paesi con un PIL elevato, come Austria, Svizzera e Svezia, per massimizzare il potenziale di generare un utile. Con molta probabilità, ciò ha contribuito alla maggiore diffusione del phishing in questi paesi. Allo stesso tempo, il phishing viene utilizzato anche in attacchi di massa che "sparano alla cieca", nei quali i cybercriminali sperano che, se riescono a colpire una vasta quantità di persone, prima o poi qualcuno cadrà in trappola.

CONCLUSIONE: OCCORRE PERSISTERE NELL'IMPLEMENTAZIONE DI ADEGUATE MISURE CONTRO IL PHISHING. I CYBERCRIMINALI UTILIZZANO QUESTA TECNICA SEMPRE PIÙ FREQUENTEMENTE, SENZA RISPARMIARE ALCUN SETTORE O PAESE.

Partecipanti che hanno osservato, dall'inizio della pandemia, un aumento nel numero di attacchi di phishing contro la propria organizzazione



Avete osservato, dall'inizio della pandemia, un cambiamento nel numero di attacchi di phishing contro la vostra organizzazione? [base di partecipanti indicata nel grafico] Sì, un aumento significativo; Sì, un lieve aumento

3. La maggior parte delle organizzazioni conduce programmi di sensibilizzazione sul phishing

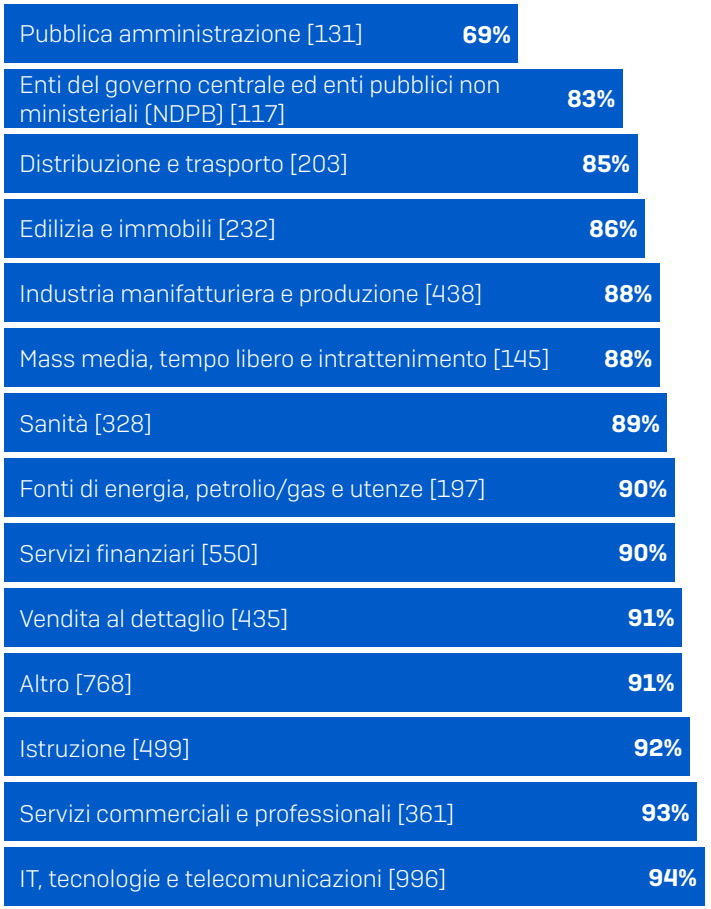
Il 90% delle organizzazioni ha implementato un programma di sensibilizzazione informatica sul phishing e un ulteriore 6% intende avviarne uno.

L'approccio più comune è la formazione su computer, adottato dal 58% delle organizzazioni. Più della metà (53%) conduce corsi di formazione con istruttori e il 43% effettua simulazioni di phishing. Il 16% delle organizzazioni utilizza una combinazione di tutte e tre le tecniche (formazione su computer, corsi con istruttori e simulazioni di phishing) per il proprio programma di sensibilizzazione.

Dal sondaggio è emerso che gli enti governativi non sono in grado di tenere il passo con gli altri settori per quanto riguarda l'implementazione di programmi di cybersecurity per la sensibilizzazione sul phishing. Agli ultimi posti si trovano infatti la pubblica amministrazione (69%) e il settore pubblico (83%). Sono statistiche preoccupanti, in quanto gli enti governativi sono bersagli presi di mira frequentemente dagli attacchi informatici: il settore pubblico è quello con la maggiore probabilità di subire attacchi ransomware basati sull'estorsione, mentre nella pubblica amministrazione si riscontra la più elevata probabilità di cadere vittima della cifratura non autorizzata dei dati durante un attacco ransomware.

CONCLUSIONE: SE LA VOSTRA AZIENDA RIENTRA NEL 10% DI QUELLE CHE ANCORA NON HANNO UN PROGRAMMA DI CYBERSECURITY PER LA SENSIBILIZZAZIONE SUL PHISHING, VI CONSIGLIAMO DI IMPLEMENTARNE UNO AL PIÙ PRESTO.

Partecipanti la cui organizzazione conduce programmi di sensibilizzazione sul phishing



La vostra organizzazione ha implementato un programma di cybersecurity per la sensibilizzazione sul phishing? [5.400] Sì, abbiamo implementato programmi di formazione su computer; Sì, conduciamo corsi di formazione con istruttori; Sì, effettuiamo simulazioni di phishing

90%

Percentuale di organizzazioni che hanno implementato un programma di sensibilizzazione informatica sul phishing

58%

Percentuale di organizzazioni con programmi di formazione su computer

53%

Percentuale di organizzazioni che conducono corsi di formazione con istruttori

43%

Percentuale di organizzazioni che effettuano simulazioni di phishing

La vostra organizzazione ha implementato un programma di cybersecurity per la sensibilizzazione sul phishing? [5.400] Sì, abbiamo implementato programmi di formazione su computer; Sì, conduciamo corsi di formazione con istruttori; Sì, effettuiamo simulazioni di phishing

4. I programmi di sensibilizzazione sul phishing sono una strategia consolidata

Quasi due terzi (65%) dei programmi di sensibilizzazione sul phishing sono stati implementati nel periodo di tempo compreso tra uno e tre anni fa. Questa statistica rispecchia la risposta delle organizzazioni alle nuove tecniche adottate dai cybercriminali verso la metà del decennio scorso. La maggiore efficacia dei sistemi di difesa informatica contro gli attacchi basati sul web in quel periodo ha costretto gli hacker a trovare nuovi vettori di attacco, come le e-mail, che a loro volta hanno generato l'esigenza di strutturare programmi volti all'educazione degli utenti.

Considerando il diffuso aumento del phishing dall'inizio della pandemia, è incoraggiante constatare che il 98% delle organizzazioni aveva implementato il proprio programma di sensibilizzazione sul phishing prima del COVID-19. Grazie a questi programmi, i dipendenti si sono trovati adeguatamente preparati per affrontare l'enorme quantità di e-mail di phishing inviate l'anno scorso.

Quando è stato implementato il programma di cybersecurity per la sensibilizzazione sul phishing della vostra azienda?	
Negli ultimi 12 mesi	2%
Da 1 a 2 anni fa	30%
Da 2 a 3 anni fa	35%
Da 3 a 4 anni fa	20%
Da 4 a 5 anni fa	12%
Più di 5 anni fa	0%
Non lo so	1%

Partecipanti al sondaggio la cui organizzazione ha implementato un programma di sensibilizzazione sul phishing [4.866]

CONCLUSIONE: CONTROLLATE E AGGIORNATE REGOLARMENTE I MATERIALI E LE ATTIVITÀ DI SENSIBILIZZAZIONE SUL PHISHING, PER GARANTIRE CHE SIANO SEMPRE COINVOLGENTI E PERTINENTI AL CONTESTO ATTUALE DEGLI UTENTI.

5. Le misure positive di monitoraggio prevalgono tra le strategie di valutazione delle attività di formazione

Quasi tutte le organizzazioni (98%) che hanno implementato un programma di sensibilizzazione degli utenti sul phishing valutano l'impatto delle proprie attività. Misurare e monitorare gli esiti permette alle organizzazioni di ottimizzare i programmi per migliorare i risultati.

Gli approcci più comuni includono il monitoraggio del numero di e-mail di phishing segnalate al reparto IT (68%) e/o il livello di segnalazione dei casi di phishing da parte degli utenti (65%). È incoraggiante osservare che la strategia più comune preveda l'utilizzo di misure positive di monitoraggio che indicano un buon livello di consapevolezza e comportamenti ottimali da parte degli utenti. L'identificazione di un tentativo di phishing e la sensibilizzazione su questo tipo di attacco permettono ai team IT di impedire proattivamente che altri utenti cadano in trappola.

Metà delle organizzazioni (50%) monitora la percentuale di clic nelle e-mail di phishing. Sebbene sia una misura negativa (poiché indica quando gli utenti diventano vittime della truffa), la percentuale di clic offre ai team IT i dati necessari per aiutarli a strutturare programmi di sensibilizzazione mirati a risolvere i problemi più comuni e a personalizzare i contenuti in modo da riflettere le realtà della propria organizzazione. Più sono i valori rilevati (sia positivi che negativi) monitorabili, migliori saranno i risultati.

CONCLUSIONE: VERIFICATE REGOLARMENTE I PROGRAMMI DI EDUCAZIONE DEGLI UTENTI TENENDO PRESENTE I RISULTATI DELLE VOSTRE VALUTAZIONI E FOCALIZZANDOVI SUL RICONOSCERE E PREMIARE I COMPORTAMENTI POSITIVI.

98%

Percentuale di organizzazioni che valutano l'impatto del proprio programma di sensibilizzazione

68%

Percentuale di organizzazioni che monitorano il numero di casi relativi al phishing inviati al reparto IT

65%

Percentuale di organizzazioni che monitorano le segnalazioni di e-mail di phishing da parte degli utenti

50%

Percentuale di organizzazioni che monitorano la percentuale di clic sulle e-mail di phishing

Quali elementi monitorate per valutare l'impatto del vostro programma di sensibilizzazione? [4.866 partecipanti la cui organizzazione ha implementato un programma di sensibilizzazione sul phishing] Numero di casi relativi al phishing inviati al reparto IT; Segnalazioni di e-mail di phishing da parte degli utenti; Percentuale di clic sulle e-mail di phishing. Non valutiamo l'impatto dei nostri programmi di sensibilizzazione sul phishing. Alcune risposte sono state escluse

Case study: ecco come un'e-mail di phishing ha portato a un attacco ransomware con un riscatto da vari milioni di dollari

Recentemente, il team Sophos Rapid Response ha ricevuto una richiesta di assistenza da parte di un'azienda che stava affrontando un attacco ransomware molto grave. Una volta isolato l'attacco, il team Rapid Response ha indagato sull'incidente per scoprire come aveva avuto inizio. Ecco i risultati delle indagini:

Tre mesi prima dell'attacco, un dipendente aveva ricevuto un'e-mail di phishing. L'e-mail sembrava provenire da un collega che lavora in un altro ufficio. Molto probabilmente, i cybercriminali erano riusciti ad accedere all'account e-mail del collega per ingannare altri dipendenti aziendali e indurli a ritenere il messaggio attendibile.

Il messaggio era molto breve e scritto in maniera sgrammaticata. Chiedeva al dipendente di cliccare su un link per prendere visione di un documento. Il link in realtà portava a una pagina web pericolosa e, quando il dipendente vi ha cliccato sopra, questo ha permesso ai cybercriminali di ottenere le credenziali di accesso dell'amministratore di dominio.

Secondo il team Rapid Response, l'e-mail di phishing è stata inviata da un Initial Access Broker, ovvero un hacker che procura accesso ad ambienti aziendali, per poi rivenderlo ad altri cybercriminali, che a loro volta lo utilizzano in vari tipi di attacco, inclusi ransomware e furto di dati.

In questo caso, il team IT della vittima è intervenuto, bloccando l'attacco di phishing. Sembrava che fosse tutto finito.

Tuttavia, otto settimane dopo, un cybercriminale ha installato ed eseguito sul computer della vittima due strumenti: Cobalt Strike e PowerSploit PowerView. Si tratta di strumenti commerciali che vengono utilizzati in maniera legittima dai penetration tester, ma anche a scopo malevolo dai cybercriminali. Molto probabilmente, questi hacker hanno sfruttato PowerView per perlustrare la rete e Cobalt Strike per mantenere la persistenza, il che gli ha permesso di restare nella rete.

Tutto è rimasto tranquillo per circa due settimane dopo le attività esplorative dei cybercriminali. Secondo il team Rapid Response, questo potrebbe essere perché il Initial Access Broker stava cercando un acquirente idoneo per vendere le credenziali di accesso.

Una volta conclusa la vendita, i nuovi "proprietari" delle credenziali hanno rapidamente usufruito del loro acquisto. Hanno fatto la loro comparsa sulla rete, installando Cobalt Strike su altri computer e cominciando a raccogliere e rubare informazioni.

Tre mesi dopo la prima e-mail di phishing, i cybercriminali hanno sferrato un attacco ransomware REvil alle 4 del mattino ora locale, esigendo un riscatto pari a 2,5 milioni di $.

Come ottenere protezione antiphishing basata su tecnologie di intelligenza artificiale con Sophos Email

Le tecnologie avanzate di machine learning **identificano gli impostori che sferrano attacchi di phishing e di Business Email Compromise (BEC)**

La scansione in tempo reale alla ricerca dei principali indicatori di phishing **blocca le tecniche basate sul social engineering**

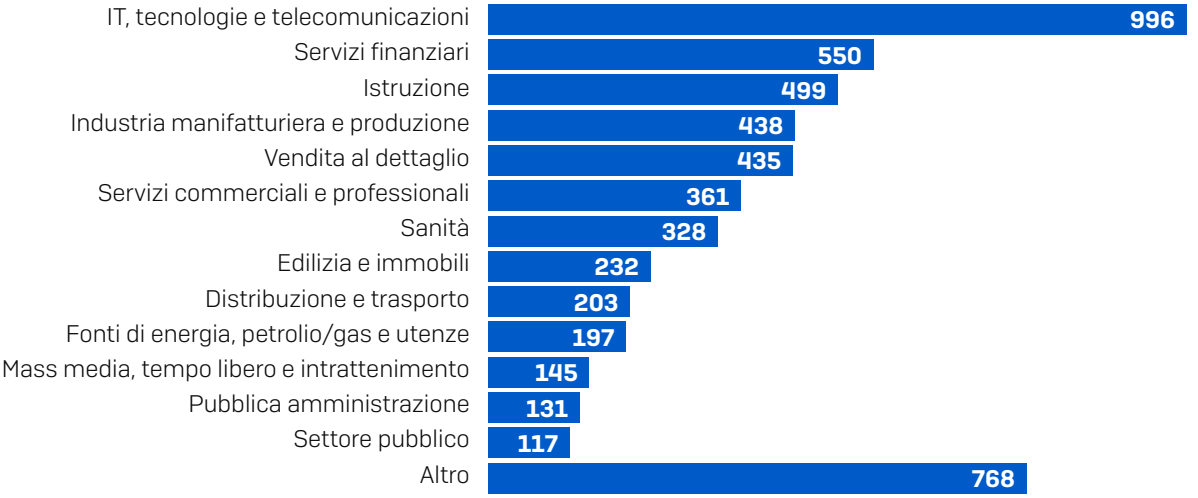
La protezione pre e post-recapito blocca **link dannosi e malware**

Per scoprire di più e per una prova gratuita, visitate sophos.it/email

Informazioni sul sondaggio

Sophos ha affidato a Vanson Bourne, un'azienda di ricerca indipendente, l'incarico di intervistare 5.400 decision maker dell'IT in organizzazioni di medie dimensioni (100-5.000 dipendenti) in 30 paesi. Il sondaggio è stato svolto nei mesi di gennaio e febbraio 2021. I partecipanti facevano parte di organizzazioni che operano sia nel settore privato che nel settore pubblico e nella pubblica amministrazione.

Numero di intervistati per settore



Numero di intervistati per paese

Paese	Num. partecipanti	Paese	Num. partecipanti	Paese	Num. partecipanti
Australia	250	India	300	Arabia Saudita	100
Austria	100	Israele	100	Singapore	150
Belgio	100	Italia	200	Sud Africa	200
Brasile	200	Giappone	300	Spagna	150
Canada	200	Malaysia	150	Svezia	100
Cile	200	Messico	200	Svizzera	100
Colombia	200	Paesi Bassi	150	Turchia	100
Repubblica Ceca	100	Nigeria	100	EAU	100
Francia	200	Filippine	150	Regno Unito	300
Germania	300	Polonia	100	USA	500

2021-08-13 WPIT (NP)

SOPHOS