CLIC COVID-19

Come il phishing ha sfruttato una crisi globale

ASPETTI CHIAVE

Italia

Come strategia di criminalità informatica, il phishing esiste da molto tempo. Allora come mai un metodo di truffa online così antico è ancora così diffuso? La risposta è semplice: perché ha ancora un tasso di successo incredibile.

Allora perché le persone continuano a fare clic?

Abbiamo intervistato 7.000 impiegati di Stati Uniti, Regno Unito, Australia/Nuova Zelanda, Germania, Francia, Italia e Giappone per studiare la loro conoscenza del phishing, analizzare le loro abitudini di clic e di posta elettronica e per scoprire come è cambiata la loro vita online dall'inizio della pandemia di COVID-19. Abbiamo quindi collaborato con il dott. Prashanth Rajivan, assistente professore presso l'Università di Washington, per capire perché il phishing funziona ancora.

In questo riepilogo esecutivo, vengono evidenziate alcune statistiche sorprendenti degli intervistati in Italia.

CARBONITE an opentext company | WEBROOT an opentext company

Nel complesso, il nostro sondaggio mostra che gli italiani non sono preparati a gestire gli attacchi di phishing.

Il 71% afferma di sapere come mantenere utenti e dati personali al sicuro dagli attacchi informatici.

Questo dato è significativamente più alto del livello di sicurezza medio globale (59%).

8 su 10 affermano di adottare misure di sicurezza per determinare se un messaggio di posta elettronica può essere dannoso.

Il 30% ammette di aver fatto clic su un collegamento di phishing nell'ultimo anno.

Questo dato rispecchia la media globale. Degli intervistati che sono stati oggetto di phishing, il 23% non lo ha mai segnalato. Come il Giappone, l'Italia ha ottenuto il punteggio peggiore per la segnalazione di phishing.

I dipendenti italiani non dimostrano abitudini impeccabili in materia di resilienza informatica.

Il 63% fa clic regolarmente su e-mail dai mittenti sconosciuti.

Il 18% di questi utenti lo fa "sempre", mentre il 45% fa regolarmente clic sulle e-mail dai mittenti sconosciuti se riconosce l'organizzazione che il mittente afferma di rappresentare o se la riga dell'oggetto dell'e-mail riguarda il loro settore.

Circa 1 su 5 utilizza i suoi dispositivi personali per lavoro.

Il numero di italiani che utilizza i dispositivi personali per lavoro (19%) è il più basso tra tutti i paesi intervistati. Il 28% utilizza i propri dispositivi professionali per motivi personali, mentre il 51% li usa per entrambi gli scopi. Questi due dati sono i più alti di tutti i paesi, superando notevolmente la media globale (rispettivamente 15% e 37%).

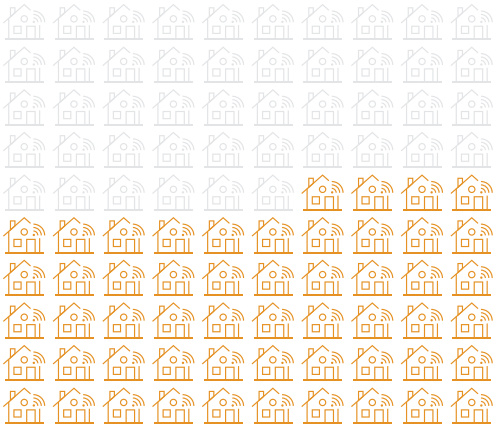
Il 76% non esegue il backup dei propri dati.

Ma il 47% afferma di aver avuto disogno di recuperare i file persi dall'inizio della pandemia, una percentuale superiore alla media globale.

Solo l'8% ritiene che tutti i dipendenti debbano avere un ruolo nella resilienza informatica della propria azienda.

La media globale è del 14%, con Australia/Nuova Zelanda che ritiene che la percentuale debba essere più alta (27%), mentre il Giappone più bassa (7%).

L'impatto del COVID-19 e del telelavoro



Oltre la metà (54%) ha aumentato il tempo che trascorre lavorando da casa.

Il 30% è più preoccupato per il phishing ora rispetto all'inizio dell'anno.

Circa 2 intervistati su 5 (38%) si sentono più pronti per individuare il phishing da quando lavorano da casa.

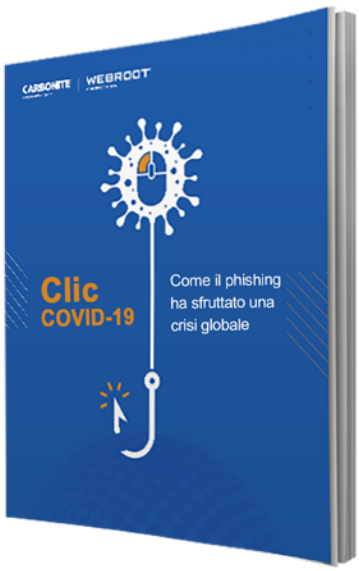
Circa 1 su 5 (18%) ha ricevuto e-mail di phishing specificamente correlate al COVID-19.

Il 23% afferma che la propria azienda ha aumentato la formazione sulla sicurezza informatica durante la pandemia.

Come possiamo migliorare?

Scopri i dati completi del sondaggio e la loro correlazione, leggi l'analisi del Dott. Rajivan e ottieni suggerimenti utili su come le aziende e gli individui possono essere resilienti contro gli attacchi di phishing nel report completo.

Visita il sito **https://mypage.webroot.com/covid-clicks-it.html** per scaricare la tua copia gratuita oggi.



Informazioni su Carbonite e Webroot

Webroot e Carbonite, società OpenText, utilizzano al meglio il cloud e l'intelligenza artificiale per fornire soluzioni di resilienza informatica complete per aziende, privati e provider di servizi gestiti. Per resilienza informatica si intende la possibilità di rimanere operativi, anche a seguito di attacchi informatici e perdite di dati. Ecco perché abbiamo unito le forze per fornire protezione degli endpoint, protezione della rete, formazione sulla consapevolezza della protezione e soluzioni di backup e ripristino di emergenza dei dati, nonché i servizi di intelligence delle minacce utilizzati dai principali fornitori di tecnologie di tutto il mondo. Grazie alla potenza del machine learning per la sicurezza di milioni di aziende e utenti, Webroot protegge il mondo connesso. Carbonite e Webroot operano a livello globale in Nord America, Europa, Australia e Asia. Scopri la resilienza informatica su carbonite.com e webroot.com