Secure Online Desktop

I tuoi dipendenti sono preparati ad affrontare attacchi progettati per ottenere informazioni sensibili?

Scoprilo con una campagna di

Phishing etico

L’*elemento* più facilmente hackerabile è il dipendente distratto o ingenuo. Fornigli le risorse adeguate protegge lui e tutta l’azienda!

I dati sono allarmanti

96% degli attacchi arriva via email

Oltre **2.000.000** di siti di phishing

Perdita media per azienda **$80.000**

69% dei breach causati da dipendenti

Cos’è il phishing?

Si tratta di un fenomeno di **truffa informatica** che consiste nel **sottrarre le credenziali di autenticazione facendoli inserire all’utente stesso in una pagina falsa** che appare identica a quella di un servizio che il destinatario usa realmente.

Gli attacchi phishing di questo tipo sono difficili da individuare in modo automatico, perché **i link nelle email potrebbero apparire legittimi a una macchina**.

L’unico modo per evitare di venire ingannati è quello di sapere a quali indicatori fare attenzione ed essere sempre all’erta. Per questo è importante lavorare per *aumentare la resilienza* del proprio team a questo tipo di attacchi.

Se i dipendenti dell’azienda sono in grado di individuare i tentativi di attacco, i dati della compagnia saranno più al sicuro.

Secure Online Desktop

I vantaggi di una campagna di phishing etico

Testa la difesa aziendale

Testeremo i vostri dipendenti inviando messaggi del tutto simili a quelli di una campagna phishing, ma in ambiente controllato, senza mai mettere a rischio realmente l'azienda.

Raccoglieremo le risposte e **le analizzeremo per generare un report e una formazione mirata.**

Analizza i risultati

La campagna di Ethical Phishing produce dei report dettagliati contenenti moltissime informazioni essenziali per identificare i *punti deboli* negli scenari testati.

Alcune delle informazioni raccolte: *numero di aperture messaggi, numero di click raccolti, quali credenziali vengono usate, etc.*

I dati vengono utilizzati anche per quantificare la consapevolezza degli utenti nel riconoscere email sospette.

Forma i dipendenti in modo specifico

Organizza una campagna di formazione e sensibilizzazione alla sicurezza informatica per i dipendenti.

Conducendo il servizio di phishing etico e **utilizzando i risultati per personalizzare il programma di formazione** del vostro personale, l'intervento risulta essere molto più efficace.

Secure Online Desktop

Metodologie usate

Raccolta di credenziali

Convinceremo i dipendenti dell’azienda a rivelare le loro credenziali.

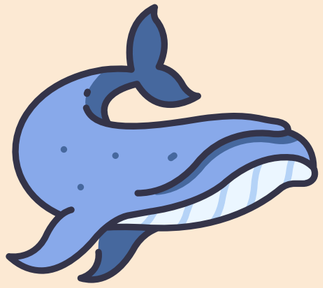
Questo servizio è ideale per **valutare la permeabilità** dei vostri dipendenti agli attacchi di phishing.

Inoltre, *tutte le credenziali ottenute possono essere riviste per garantire che aderiscano a una politica adeguata in materia di password.*

Spear phishing

In questo caso l'attacco è diretto a un gruppo target specifico di individui (ad es. il dipartimento finanze) **utilizzando informazioni specifiche per l'obiettivo o gli obiettivi.**

Questo tipo di phishing fa leva sull’attacco diretto a persone che non sono del tutto consapevoli delle tecniche di hacking.



Whaling

L'obiettivo dell'attacco sarà a livello dirigenziale all'interno dell'organizzazione.

Questi target sono particolarmente delicati perché una volta compromessi, posso esercitare una certa influenza su altri dipendenti.

Quali i traguardi da raggiungere

Il nostro approccio

Fare una campagna di Ethical Phishing nei confronti di un'azienda che lo richiede significa scoprire i punti deboli dell'azienda attraverso l'occhio dell'attaccante (hacker) con l'obiettivo finale di effettuare una vera e propria simulazione di un attacco informatico.

Cosa faremo

L'attività di phishing può comprendere fasi di Social Engineering, invio di messaggi o anche *telefonate-trappola*, volte a raccogliere informazioni sensibili o dati personali utilizzabili da un attaccante (hacker).

Cosa cerchiamo di trovare

La campagna di Ethical Phishing ha l'obiettivo di scoprire quanto i dipendenti di un'azienda siano sensibili e "raggirabili" riguardo alle truffe tramite contatti digitali. Capiremo quanto i dipendenti siano restii a divulgare informazioni personali, codici di accesso o dati finanziari dell'azienda.

Cosa aspettarsi dopo la campagna

In seguito alla campagna di ethical phishing, e la conseguente formazione mirata a fornire gli strumenti necessari per riconoscere ed evitare il phishing, **i dipendenti saranno in grado di difendere la propria azienda semplicemente ignorando i messaggi sospetti.**

La miglior difesa contro il phishing è saperlo riconoscere!

Secure Online Desktop

Scegli la sicurezza per la tua azienda

Dal 2011 ci occupiamo di tecnologia Cloud e di sicurezza, affidati a dei professionisti esperti!

Scopri il servizio sul sito

Per ulteriori informazioni, i nostri contatti sono:

Via Zacchetti 6, 42124 - Reggio nell'Emilia (RE)
www.secure-od.com

Tel. +39 0522 1685330
Fax. +39 0522 015371
E-mail: info@secure-od.com
Pec: secure-od@pec.it

Secure Online Desktop