Argomento: Exprivia si parla di noi

Women for Security | Press

Sai riconoscere un email di phishing?

Sono ormai diverse le tecniche di attacco che gli attaccanti riservano agli utenti, ma tra le tante, quella maggiormente utilizzata, soprattutto in questo ultimo trimestre dell'anno, è il Phishing.

Cos'è il Phishing? Sai riconoscerlo? La parola ha pure una bella fonetica! Eppure non c'è tanto da scherzare quando diventiamo vittime di questo crimine informatico che mira al furto di dati sensibili.

Si tratta di una vera e propria una truffa elaborata. In pratica, i truffatori, fingendosi aziende, enti governativi, istituti bancari o altri enti affidabili, tentano di ingannare noi utenti per indurci a fornire volontariamente informazioni come le credenziali di accesso ai siti Web o, peggio ancora, i dati della carta di credito.

Nelle mail di phishing si richiede di effettuare aggiornamenti, convalidare o confermare le informazioni personali sensibili contenute nel proprio account, spesso suggerendo la presenza di un problema. Quindi noi utenti veniamo reindirizzati su un sito fasullo e spinti a immettere informazioni relative al nostro account, con conseguente furto di identità.

Gli hacker si impegnano molto per rendere i messaggi di phishing il più possibile simili a email e sms inviati da aziende considerate affidabili, motivo per cui è necessario prestare la massima attenzione quando si aprono questi messaggi e si fa clic sui link che contengono.

Ma come individuare un messaggio di phishing?

Oggi i truffatori di phishing sono diventati talmente esperti nello scrivere email, che a volte, paradossalmente, le loro comunicazioni risultano scritte meglio delle mail inviate dagli enti ufficiali; fortunatamente per noi, però, gli hacker commettono errori facilmente individuabili, una volta imparato a riconoscerli.

Infatti, ogni volta che si apre un'email o un SMS, è bene fare attenzione a questi segnali di phishing:

messaggio scritto male e con strani allegati - Può capitare di trovare piccole imperfezioni anche nelle comunicazioni inviate dalle aziende più affidabili, ma i messaggi di phishing contengono spesso errori grammaticali, di ortografia e altri errori palesi che le grandi aziende non commetterebbero. Inoltre, osserva bene eventuali allegati; oltre i file con estensione.exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf. Nel caso si tratti di un così detto "financial malware" o di un "trojan banking", il virus si attiverà per sottrarre dati finanziari. Altri tipi di virus si attivano quando sulla tastiera vengono inseriti "user id e password", così detti "keylogging", in questo caso i criminali sono in possesso delle chiavi di accesso ai nostri account di posta elettronica o di e-commerce;

aspetto un po' strano del logo - Per aumentare la propria credibilità, i truffatori di phishing spesso usano imitazioni dei loghi delle aziende o degli enti che decidono di impersonificare. Se il logo non è ben visibile nel messaggio, per proporzioni errate o bassa risoluzione, non è escluso che si tratti di un tentativo di phishing;

URL non corrispondente - L'obiettivo del phishing è indurre noi utenti a fare clic su link fraudolenti. Per verificare se un link è legittimo effettua queste verifiche:
Sposta il mouse sopra il link nell'email per visualizzarne l'URL, se questo contiene errori di ortografica è molto probabile che si tratti di una truffa. Passando il mouse sul link visualizzerai un'anteprima dell'URL. Se ti sembra sospetto, non aprirlo.
Fai clic con il pulsante destro del mouse sul link, quindi copia e incolla l'URL in un elaboratore di testi. Ciò ti consentirà di esaminare il link per individuare eventuali errori grammaticali o di ortografia senza aprire una pagina Web potenzialmente dannosa.
Per controllare l'URL su dispositivo mobile, premi a lungo sul link con il dito. Se noti che l'URL non corrisponde al presunto mittente del messaggio,

probabilmente si tratta di un'email di phishing.
Naturalmente, anche al lavoro, mai abbassare la guardia! Una truffa di phishing diffusa consiste nell'invio di email progettate per assomigliare a quelle inviate dai dirigenti aziendali. I messaggi chiedono ai dipendenti di trasferire fondi a presunti clienti, ma questo denaro in realtà va ai truffatori.

Esempi di recenti attacchi di phishing

CERT-PA, lavora all'interno dell'Agenzia per l'Italia Digitale (AgID) per supportare le amministrazioni nel prevenire e rispondere ad eventuali incidenti di cybersecurity.

CERT-PA ci mette in guardia da un ramsonware chiamato FTCODE nascosto in un file.doc, che a sua volta è contenuto in una cartella compressa, allegata ad una mail ordinaria o ad una PEC. Questa sorta di pericolosa matriosca cripta i dati dei PC colpiti e li blocca fino al pagamento di un riscatto.

Anche l'INAIL è stata costretta a discolparsi di fronte ad una recente truffa che la vede coinvolta come "mittente inconsapevole" in una campagna di phishing che richiede pagamenti indebiti ai destinatari. In questo caso la posta elettronica certificata (PEC), inviava con oggetto "Trasmissione atti INAIL", un allegato che riproduceva fedelmente la carta intestata dell'istituto. Nel documento si invitava l'utente ad effettuare un versamento ad un codice IBAN fasullo, che non ha niente a che fare con l'INAIL.

L'INAIL ora invita a verificare che le PEC inviate provengano dal dominio "postacert.inail.it" e che la firma contenuta sia certificata dietro il dominio "telecompost.it".

Recentemente l'Agenzia delle Entrate ha informato gli utenti di una mail truffa "Agenzia delle entrate-Riscossione", corrispondente al fittizio mittente del messaggio di posta. Nel testo della mail un link con scritto "ACCEDI DOCUMENTO" invitava a visionare alcuni documenti esattoriali, ma in realtà era l'appiglio con cui i truffatori entravano in possesso delle credenziali bancarie del destinatario.

Ovviamente l'Agenzia della Entrate, con apposito comunicato, si è dichiara estranea all'accaduto invitando gli utenti a prestare la massima attenzione.

Quando il phishing non viene rilevato

Gli hacker aggiornano frequentemente i propri metodi per non essere scoperti da chi, come noi, è consapevole di determinate minacce informatiche. Questo è il caso delle più recenti tecniche per evitare il rilevamento del phishing, basate sul riconoscimento delle macchine virtuali. Le aziende di sicurezza informatica spesso utilizzano dispositivi headless o macchine virtuali per determinare se un sito Web è di fatto una pagina di phishing. Alcuni kit di phishing contengono istruzioni JavaScript, un linguaggio di programmazione che consente di implementare funzionalità complesse nelle pagine Web, in grado di rilevare l'attività di una macchina virtuale sulla pagina. Se vengono identificati tentativi di analisi, il kit mostrerà una pagina vuota invece della pagina di phishing, eludendo le misure di rilevamento delle truffe.

Per non cadere vittima dei truffatori mantieniti sempre al corrente delle tecniche di phishing più recenti e, se accidentalmente inserisci dati in una pagina Web collegata a un'email sospetta, esegui una scansione completa del malware sul tuo dispositivo.

Una volta completata la scansione, esegui il backup di tutti i tuoi file e modifica le tue password.

Quindi cosa fare per proteggersi?

Fai attenzione alle tue informazioni personali quando navighi su Internet e sii prudente ogni volta che qualcuno ti chiede di divulgare dettagli sensibili sulla tua identità, dati finanziari o credenziali di accesso.

In caso di dubbio, contatta direttamente l'organizzazione che ti ha presumibilmente inviato il messaggio anziché aprire i link in esso contenuti.

Esamina attentamente le email sospette per controllare la presenza di indizi rivelatori di phishing.

Se per errore fai clic su un link di phishing, non

inserire alcun dato e chiudi la pagina, esegui una scansione antivirus, esegui il backup dei tuoi file e modifica tutte le password.

Per il resto basta essere consapevoli delle truffe, conoscerle bene, per saperle affrontare al meglio!