**Attacchi di phishing: come proteggersi dagli hacker**

I truffatori attualmente sfruttano la fiducia dei clienti delle banche per ottenere dati di accesso, cioè nome utente e password, ai loro conti. Circa l'80% degli incidenti è causato da cattiva condotta dell'utente a causa di negligenza.

**Che cos'è il phishing?**

Il phishing è uno degli attacchi informatici più comuni e prende di mira i dati personali e sensibili. Con l'aiuto di notizie false e siti web, che sono spesso indistinguibili da quelli reali nel layout e nei testi, alle vittime viene chiesto di rilasciare i loro dati ai truffatori.

**Smishing, attacchi di phishing via SMS**, sono in aumento. Quando si utilizza lo smartphone, gli utenti sono meno consapevoli e presumono che i messaggi brevi siano più a prova di falsificazione rispetto alle e-mail. Ciò rende questi attacchi un immenso rischio per la sicurezza.

**Quanto è pericoloso il phishing?**

Gli attacchi di phishing colpiscono sia privati che aziende. Rubando i dati di accesso, in particolare i dati bancari, gli hacker hanno l'opportunità di effettuare transazioni. Di conseguenza, gli hacker possono rubare grandi quantità di denaro sia da privati che da aziende. Gli attacchi alle aziende possono anche causare enormi danni economici, poiché possono essere colpite somme di milioni.

**Come possono essere rilevati** **gli attacchi** **di phishing?**

Notifiche, che provengono da truffatori, hanno spesso determinate caratteristiche.

Una selezione di queste caratteristiche sono le seguenti che abbiamo riassunto per voi:

* Include errori ortografici o grammaticali
* Invita all'azione
* Segnala un'urgenza
* Manca il saluto personale
* Collegamenti personalizzati nel messaggio (fare clic con il pulsante destro del mouse per visualizzare l'indirizzo nascosto)
* Sono richiesti i dati di accesso e i numeri di carta
* Mancano le Umlaut
* Contengono caratteri cirillici
* Etc.

**Come** **può proteggersi?**
Oltre alla capacità di rilevare gli attacchi di phishing, non dovrebbe mancare un'ampia protezione.

Con questi 8 consigli può proteggersi:

* Installare programmi antivirus.
* Controllare l'indirizzo e-mail del mittente dei messaggi.
* Non condividere mai le Sue informazioni personali e sensibili con estranei. Innanzitutto, controlla l'impronta del sito Web ufficiale e, se necessario, chiama il mittente tramite questo numero di telefono. Non utilizzare il numero di telefono del messaggio, ma il numero del sito ufficiale.
* Non aprire ma allegati da mittenti sconosciuti. Particolarmente vulnerabili sono quei file che finiscono su .exe", ". msi" e ". scr".
* Utilizzare dati di accesso diversi per account diversi. In questo modo si evitano attacchi a più account.
* Utilizzare l'autenticazione a più fattori. Di conseguenza, il nome utente e la password non sono più sufficienti per hackerare un account.
* Gli aggiornamenti periodici e gli aggiornamenti dei sistemi possono aiutare a proteggere dagli hacker.
* Effettuare regolarmente sensibilizzazioni dei dipendenti, i cosiddetti corsi di formazione IT Awareness.

Dai programmi antivirus alle analisi delle vulnerabilità e all'autenticazione a più fattori, oltre a corsi di formazione: l'azienda IT KONVERTO offre sicurezza IT sotto tutti gli aspetti e aiuta a sviluppare una strategia di sicurezza adatta a Lei.