Esempio email phishing

Oggetto: Avviso Importante: Verifica del tuo Account
Da: servizi-clienti@banca-fittizia.com
Caro Cliente,
Abbiamo rilevato un accesso sospetto al tuo account. Per proteggere i tuoi dati, ti preghiamo di verificare le tue informazioni cliccando sul link qui sotto:
Verifica il tuo Account
Se non completi la verifica entro 24 ore, il tuo account sarà bloccato.
Grazie per la tua attenzione.
Cordiali saluti,
Il Team di Servizio Clienti
Banca Fittizia

Caratteristiche Comuni:

- **Saluto Generico**: Usano frasi come "Caro Cliente" anziché il tuo nome.
- **Urgenza**: Spingono a un'azione immediata.
- **Link Sospetti**: I link sembrano legittimi ma possono portare a siti fasulli.
- **Email del Mittente Sospetta**: Controlla attentamente l'indirizzo email.

Ricorda sempre di essere cauto e di verificare le email prima di agire!
4o mini.

Che cos'è il phishing?

Il phishing è un attacco tramite email che cerca di truffare le persone a fornire informazioni private come dati bancari o di accesso.
Il phishing utilizza il social engineering per truffare le persone, sfruttando tecniche come la falsificazione e la menzogna nelle email per indurre azioni inconsce negli utenti.

I cybercriminali scelgono il phishing per la sua semplicità, economicità ed efficacia nel rubare dati sensibili, causando danni come furto di identità, perdita di dati e infezioni da malware come ransomware.

Link

Condividere link nelle email è comune, ma i link nei phishing possono portare a siti con malware. Possono sembrare legittimi e sono inseriti in immagini per sembrare meno sospetti.(Un esempio e come nell'email che ho messo sopra ci sia un link dove ci sono I malware?)

Conseguenze di un attacco phishing

È essenziale comprendere le conseguenze di un attacco di phishing, per riuscirlo a prevernire ad esempio:

1. Furto di denaro dal conto bancario.
2. Addebiti non autorizzati sulla carta di credito.
3. Mutui e prestiti accesi a vostro nome.

Proteggersi dagli attacchi phishing

Verificare il mittente:

La prima difesa contro il phishing è verificare il mittente dell'email controllando l'indirizzo e confermando il dominio aziendale dopo la chiocciola**.**

Errori grammaticali:

Le email autentiche sono corrette grammaticalmente, mentre lo spam contiene errori ortografici. Controlla questo indicatore di spam. Soprattuto non clickare il link che potrebbero risultare malware or spyware.

Non condividere informazioni riservate

Usare software di sicurezza:

Provare ad utilizzare dei siti dove ti possono aiutare a rilevare se sono dell’email sospette e segnalare link dei siti falsi.