CHE COS'È IL PHISHING

Il **phishing** è un tipo di attacco informatico in cui i malintenzionati cercano di ingannare le persone per ottenere informazioni sensibili come nomi utente, password, numeri di carte di credito o altri dati personali. Di solito, i truffatori si spacciano per entità fidate, come banche, organizzazioni governative o servizi online molto noti, per convincere le vittime a rivelare queste informazioni.

ESAME SETTIMANALE

Esercizio del Giorno: Creare una Simulazione di un'Email di Phishing

1. **Contesto**: Immaginiamo di ricevere un'email aprire la tua casella di posta elettronica da una presunta banca, che ci avvisa di una "verifica urgente" del nostro account. In questo caso, l'email finge di provenire da una banca ben conosciuta, ma in realtà è una truffa che mira a ottenere le credenziali di accesso al nostro conto bancario. L'obiettivo del phishing è rubare i dati di accesso (nome utente e password) e, eventualmente, informazioni finanziarie sensibili.

Obiettivo del phishing: Raccogliere le credenziali di accesso all'account bancario della vittima e possibilmente ottenere anche altre informazioni personali (come numeri di carta di credito) per compiere frodi finanziarie.

Oggetto: Verifica Urgente del Tuo Account Bancario

Da:sicurezza@bancahydrahackers.com
A:marco.rossi@azienda.it
Data: 6 dicembre 2024

Gentile Cliente,

Abbiamo rilevato un accesso sospetto al tuo account bancario e per motivi di sicurezza abbiamo temporaneamente limitato l'accesso al tuo account **HydraSecure Bank**.

Per evitare che il tuo account venga bloccato definitivamente, ti chiediamo di completare una **verifica urgente** entro 24 ore. Questo processo ci aiuterà a confermare la tua identità e ripristinare l'accesso senza interruzioni.

Per procedere con la verifica, clicca sul link qui sotto e inserisci le informazioni richieste:

Verifica il tuo account

Ti ricordiamo che il link sarà attivo solo per le prossime 24 ore. Se non completerai la verifica, il tuo account verrà bloccato permanentemente per proteggere la tua sicurezza.

Grazie per la tua collaborazione.

Cordiali saluti,
Il team di sicurezza di **Hydra Hackers Team**
Hydra Secure Bank
Servizio Clienti
Tel. 800-123-4567

---

http://www.hydrasecurebank-login-sicura.com/cambio-email

Perché questa email potrebbe sembrare credibile:

- **Apparenza ufficiale**: La truffa sembra provenire da una banca conosciuta, con l'uso di termini come "Servizio Clienti" e "Sicurezza".
- **Urgente e minaccioso**: L'email crea un senso di urgenza, affermando che l'account verrà bloccato se non si agisce subito. Questo induce panico, spingendo la vittima a cliccare sul link senza riflettere.
- **Link falso**: Il link sembra essere quello di una pagina ufficiale della banca, ma se ispezionato, si può notare che l'URL non è corretto (è un sito web falso, non legato alla banca reale).

Elementi della mail che dovrebbero far scattare un campanello d'allarme:

1. **L'email proviene da un dominio sospetto**: Nonostante l'oggetto dica "Servizio Clienti", l'indirizzo email potrebbe non corrispondere al dominio ufficiale della banca. Ad esempio, potrebbe essere qualcosa come "servizio-clienti@banca-falsa.com" invece di "servizio-clienti@banca-reale.com".
2. **Richiesta urgente e minacciosa**: Le email legittime di una banca raramente usano un linguaggio minaccioso e urgente. Le banche reali solitamente avvisano in anticipo e non chiedono azioni immediate.
3. **Errori grammaticali o stilistici**: Anche se l'email potrebbe sembrare ben scritta, in alcuni casi potrebbero esserci errori grammaticali o stilistici (ad esempio, "verifica urgente" potrebbe essere scritto in modo poco naturale in italiano, o il link potrebbe avere una struttura strana).
4. **Il link sospetto**: Passando il mouse sul link "Verifica il tuo account", si può notare che il sito non corrisponde al dominio della banca ufficiale. Inoltre, i link in queste email di phishing spesso puntano a pagine di login fasulle, progettate per raccogliere le credenziali delle vittime.

5. **Richiesta di informazioni sensibili**: Nessuna banca legittima ti chiederà mai di inviare informazioni sensibili via email. Se questo accade, è sempre un segno di phishing.