SOCIAL ENGINEERING

Oggetto dell’email:

"Avviso urgente: Il tuo account bancario sarà sospeso!"

Testo dell’email:

> **Gentile cliente,**
>
> Abbiamo notato che le credenziali sue dell’account bancario sono scadute e devono essere aggiornate immediatamente per evitare la sospensione.
>
> Per favore, accedi al nostro sistema sicuro e aggiorna i tuoi dati personali:
>
> Aggiorna il tuo account ora
>
> Se non riceviamo il tuo aggiornamento entro 24 ore, il tuo conto sarà sospeso permanentemente, e tutte le transazioni saranno bloccate.
>
> **Nota:** Questa è un'azione urgente. La mancata azione comporterà la perdita dell'accesso al conto.
>
> Grazie per la sua collaborazione.
>
> Cordiali saluti,
> **Il Team Sicurezza di Stellar Bank**
>
> ---
>
> **Messaggio inviato da**: stellarbank@banca-sucurezzà.it
> **Rispondi a:** noreply@banca-sucurezzà.it

Report di analisi: Email di phishing

Obiettivo del phishing

L’obiettivo principale di questa email di phishing è sottrarre le credenziali di accesso degli utenti, inducendoli a cliccare su un link fraudolento e a inserire informazioni sensibili, come username e password, su un sito malevolo. La tecnica sfrutta l’urgenza e la simulazione di un’istituzione bancaria affidabile per ingannare la vittima.

Elementi che permettono di riconoscere il phishing

1. **Indirizzo email del mittente sospetto:**
   Mittente: `stellarbank@banca-sucurezzà.it`
   L'indirizzo è simile a quello di una banca reale, ma contiene un errore evidente (sucurezzà invece di sicurezza). Questo è un indizio comune nei tentativi di phishing, dove gli attaccanti registrano domini simili per ingannare le vittime.

2. **Errore grammaticale e ortografico:**
   Errori come "le credenziali sue sono scadute" e "banca-sucurezzà" indicano una traduzione errata o una scrittura poco professionale, cosa improbabile in una comunicazione ufficiale.
   .
3. **Tono di urgenza:**
   Frasi come "Aggiorna le tue credenziali entro 24 ore" e "il tuo conto sarà sospeso permanentemente" sono progettate per spingere l'utente ad agire in fretta, senza verificare la legittimità del messaggio. Questo è un segnale tipico del phishing.

4. **Link fraudolento:**
   L'URL associato al pulsante "Aggiorna le tue credenziali ora" sembra legittimo a prima vista, ma l'URL reale è un dominio malevolo che non appartiene alla banca reale.
   Un utente attento potrebbe passare il mouse sul link senza cliccare per verificare l'URL effettivo.

5. **Richiesta di informazioni personali:**
   Una banca legittima non richiede mai di aggiornare username e password tramite email. Questo tipo di richiesta è un segnale di allarme evidente.

6. **Design leggermente imperfetto:**
   Nonostante l'uso di un logo e di un banner, i dettagli grafici possono sembrare meno curati rispetto agli standard delle comunicazioni ufficiali.

Elementi che rendono l'email credibile

1. **Logo e banner della banca:**
   L'email include un logo e un design che imitano lo stile grafico delle comunicazioni ufficiali della banca. Questo aumenta la percezione di autenticità.

2. **Struttura professionale:**
   L'email è organizzata in modo formale, con saluti e un corpo centrale. Questa struttura è tipica delle comunicazioni ufficiali.

3. **Nome dell'istituzione affidabile:**
   L'uso di un nome simile a quello di una banca nota genera fiducia negli utenti, inducendoli a credere che il messaggio sia legittimo.

4. **Presenza di un pulsante di azione (CTA):**
   Il pulsante ″Aggiorna subito″ è ben visibile e accattivante, aumentando la probabilità che l'utente clicchi senza riflettere.

5. **Simulazione di un problema di sicurezza:**
   La minaccia di sospensione del conto bancario è un problema plausibile che attira l'attenzione degli utenti, specialmente se non sono esperti.

Suggerimenti per Riconoscere e Prevenire Attacchi Simili

1. **Verifica dell'indirizzo del mittente:**
   Controlla attentamente l'indirizzo email per errori o domini sospetti.

2. **Passaggio del mouse sui link:**
   Prima di cliccare su un link, passa il cursore sopra per verificare che l'URL corrisponda al sito ufficiale.

3. **Attenzione ai toni di urgenza:**
   Le banche legittime non utilizzano toni eccessivamente allarmistici nelle loro comunicazioni.

4. **Conferma tramite canali ufficiali:**
   Se hai dubbi, contatta direttamente la banca utilizzando i numeri di telefono o i siti ufficiali.

5. **Utilizzo di software di sicurezza:**
   Soluzioni antivirus e antispam aggiornate possono rilevare e bloccare email sospette.

Conclusione

Questa email utilizza tecniche sofisticate, come l’imitazione del design di una banca e il tono professionale, ma contiene segnali evidenti di phishing che un utente attento può identificare. È fondamentale educare gli utenti a riconoscere questi segnali e a reagire con prudenza.