Simulazione di attacco phishing

Obiettivo dell'attacco:

Indurre un utente cliente della **BancoFiducia S.p.A.** (istituto bancario fittizio) a cliccare su un link malevolo per sottrarre le credenziali di accesso all'app di home banking.

E-mail phishing

Da: assistenza@bancofiducia-online.com
Oggetto: Azione urgente richiesta sul tuo conto BancoFiducia

Gentile cliente,

Abbiamo rilevato un'attivita sospetta sul tuo conto BancoFiducia e per motivi di sicurezza abbiamo bisogno di confermare la tua identita IMMEDIATAMENTE.

Se non conferma l'accesso entro 24h, il suo conto verra sospeso permanentemente per protezione.

Per evitare questo, clicca qui sotto per verificare i tuoi dati:

🔗 https://bancofiducia-verifica.com/login-secure

Attenzione: questo link è personale e deve essere usato solo da lei.
Grazie per la collaborazione.

Cordiali saluti,
Servizzio Clienti BancoFiducia
BancoFiducia S.p.A.
Numero verde: 800-000-000

Spiegazione scenario / contesto:

L'email è inviata durante un fine settimana, momento in cui il servizio clienti reale della banca potrebbe avere risposte più lente. Questo aumenta la probabilità che l'utente agisca d'impulso senza verificare.

Target:

Clienti generici della banca – l'attaccante non ha informazioni specifiche, quindi si affida a una comunicazione generica ma allarmante.

Tecnica usata:

- **Phishing via email** con:
  - Urgenza (sospensione dell'account entro 24 ore).
  - Errore ortografici per sembrare meno professionale (simulando truffe comuni).
  - Link a un dominio simile a quello della banca ma non ufficiale.
  - Invito a cliccare su un link e inserire credenziali.

Obiettivo finale:

Una volta che l'utente clicca sul link, viene portato a una **pagina clone dell'interfaccia di login dell'app BancoFiducia**, dove inserisce username e password, che vengono raccolti dal server dell'attaccante.

Possibili estensioni (facoltative per la tua esercitazione):

- Integrazione di un *keylogger* nel sito fasullo.
- Richiesta anche di OTP o codici della carta per un attacco *man-in-the-middle*.

Spiegazione del motivo per cui questa email di phishing potrebbe sembrare credibile a un utente medio:

Aspetto familiare: L'email usa il nome di una banca (in questo caso inventata "BancoFiducia") e una

struttura simile alle comunicazioni reali delle banche.
Tono professionale all'apparenza: Nonostante qualche errore, il messaggio è diretto, formale e firmato da un "Servizio Clienti".
Uso dell'urgenza: L'indicazione che il conto verrà sospeso entro 24 ore spinge l'utente ad agire impulsivamente, senza pensare troppo o verificare.
Presunta protezione dell'utente: Il messaggio fa leva sulla sicurezza ("attività sospetta", "protezione dell'account") per sembrare legittimo.
Presenza di un link apparentemente coerente: Il dominio falso contiene il nome della banca e potrebbe non destare sospetti a chi non è esperto (es. bancofiducia-verifica.com).
Timing strategico: Se ricevuta in un giorno festivo o la sera, l'utente non può facilmente contattare la banca per verificare e può cadere nella trappola.
Imitazione di comunicazioni bancarie reali: Frasi come "Gentile cliente" e "verifica dei dati" sono comuni nelle vere email delle banche.
Firma e recapiti falsi: La presenza di un numero verde (finto) e un nome aziendale danno un'illusione di autenticità.

Segnali di allarme per un utente medio

1. **Tono allarmante o urgente**
   Frasi come "Azione immediata richiesta", "Il tuo conto sarà sospeso" o "Accedi entro 24 ore" servono a spaventare e manipolare emotivamente l'utente.
2. **Errori grammaticali o ortografici**
   Le banche di solito inviano comunicazioni ben curate. Errori come "Servizzio clienti" o parole con accenti mancanti sono sospetti.
3. **Link sospetti o strani**
   Anche se il testo del link sembra familiare, è buona norma **passare il mouse sopra** per vedere l'indirizzo reale: se contiene parole strane, numeri, trattini o domini sconosciuti, è probabilmente falso.
4. **Richiesta di dati personali o credenziali**
   Nessuna banca chiederà mai via email di inserire il tuo **username, password, codice OTP o PIN** tramite un link.
5. **Messaggi non personalizzati**
   Le email vere spesso si rivolgono a te per nome. Un generico "Gentile cliente" può indicare un tentativo di phishing.
6. **Mittente sospetto**
   Anche se il nome sembra corretto, l'indirizzo email completo spesso tradisce l'inganno: controlla sempre cosa c'è dopo la @.
7. **Design poco professionale**
   Impaginazione disordinata, loghi sgranati o colori strani possono indicare che non è una comunicazione ufficiale.
8. **Non ti aspettavi questa email**
   Se non hai fatto nulla di recente che possa giustificare il messaggio (es. tentativi di accesso, modifiche all'account), diffida.

Regola d'oro per l'utente medio:

Se hai dubbi, NON cliccare sul link. Vai direttamente sul sito ufficiale della banca digitando l'indirizzo manualmente o contatta il servizio clienti.

Segnali di allarme per un utente esperto

1. **Dominio del mittente sospetto**:
   L'indirizzo assistenza@bancofiducia-online.com non corrisponde al dominio ufficiale della banca, che dovrebbe essere qualcosa come @bancofiducia.it.

2. **Link ingannevole**:
   Passando il mouse sul link (senza cliccare), si nota che l'URL punta a un dominio falso: bancofiducia-verifica.com – diverso da quello legittimo della banca.
3. **Errori grammaticali e ortografici**:
   Parole come "attivita", "verra", "Servizzio" scritte senza accento o con errori di battitura non sono tipiche delle comunicazioni bancarie ufficiali.
4. **Richiesta di inserire credenziali via link**:
   Le banche vere **non chiedono mai** di inserire dati sensibili tramite link ricevuti via email. Questo è un comportamento standard noto nel settore.
5. **Uso eccessivo di urgenza**:
   Frasi come "IMMEDIATAMENTE" o "verifica entro 24h o il conto sarà sospeso" sono tipiche del social engineering, usate per spingere l'utente ad agire senza riflettere.
6. **Firma poco curata e generica**:
   Non è presente un riferimento specifico al nome del cliente o a dati contestuali (es. ultime cifre del conto), come invece accade nelle vere comunicazioni bancarie.
7. **Design troppo semplice o incoerente**:
   Se l'email viene visualizzata in HTML, potrebbe avere un'impaginazione scarsa o elementi grafici non in linea con l'identità visiva della banca.
8. **Mancanza di certificazioni digitali**:
   L'assenza di un certificato SPF/DKIM valido o la mancata autenticazione del mittente (visibile nei dettagli dell'email) è un ulteriore campanello d'allarme.