Simulazione di un’email di phishing utilizzando ChatGPT

Scenario

Un cliente di Intesa Sanpaolo riceve un’email apparentemente ufficiale da parte della banca. Il messaggio segnala un’attività insolita sul conto e richiede una verifica immediata per evitare la sospensione dell’accesso. Il link presente nell’email conduce a un sito di phishing che imita la pagina di login della banca. L’obbiettivo dell’attaccante è quello di rubare le credenziali di accesso.

Email di phishing simulata

Mittente: sicurezza@intesasanpaolo-support.com
Oggetto: ⚠ Accesso non riconosciuto al tuo conto – Verifica richiesta

Corpo del messaggio:

Gentile Cliente,

Abbiamo rilevato un tentativo di accesso al suo conto Intesa Sanpaolo da un dispositivo non riconosciuto in data 27/02/2025 alle 21:15.

Per garantire la massima sicurezza, abbiamo temporaneamente limitato alcune funzioni del suo conto online. Per ripristinare il normale accesso, è necessario confermare la sua identità cliccando sul link sottostante:

Accedi per verifica

Se non effettuerà la verifica entro 24 ore, il suo conto potrebbe essere sospeso per motivi di sicurezza.

Per assistenza, può contattare il nostro servizio clienti al numero +39 800 303 303.

Grazie per la collaborazione,
Servizio Sicurezza Online
Intesa Sanpaolo S.p.A.
sicurezza@intesasanpaolo-support.com

Spiegazione dello scenario

1. Perché potrebbe sembrare credibile?

- Il mittente sembra un indirizzo ufficiale della banca.
- Il messaggio utilizza un tono professionale e fa riferimento alla sicurezza, inducendo paura e urgenza.
- L'email include una data e un orario specifico per far sembrare la minaccia reale.
- Viene fornito un numero di telefono che potrebbe sembrare autentico.

2. Elementi sospetti che indicano phishing:

- L'indirizzo email del mittente non è ufficiale: invece di un dominio come @intesasanpaolo.com, usa @intesasanpaolo-support.com, che può trarre in inganno.
- Il link porta a un dominio fraudolento: intesa-sanpaolo-verifica.com invece di intesasanpaolo.com.
- Pressione psicologica: l'urgenza e la minaccia di blocco del conto sono tipiche strategie di phishing.
- Mancanza di personalizzazione: una banca autentica usa solitamente il nome completo del cliente, non un generico "Gentile Cliente".
- Possibili errori grammaticali: alcuni dettagli potrebbero non essere perfetti, un indizio di email fraudolente.

Questo è un classico esempio di phishing bancario che sfrutta la paura della sospensione del conto per spingere la vittima a inserire le proprie credenziali su un sito falso. Per difendersi, un utente dovrebbe sempre:

1. Controllare il mittente e il dominio dell'email
2. Non cliccare su link sospetti ma accedere direttamente al sito ufficiale della banca
3. Verificare con la banca chiamando il numero ufficiale (presente sul sito vero)
4. Attivare l'autenticazione a due fattori per una maggiore protezione

Questa mail è la dimostrazione che anche gli utenti più esperti possono cadere in questa trappola.

OLTRE ALLA SIMULAZIONE DI UN'EMAIL DI PHISHING HO DECISO DI AGGIUNGERE UNA LANDING PAGE

Cos’è una landing page?

Una landing page è una pagina web creata con un obiettivo specifico, solitamente per convincere gli utenti a compiere un’azione. A differenza di un sito web tradizionale, una landing page è progettata per guidare l’utente verso un’azione ben precisa, senza distrazioni.

Intesa Sanpaolo - Accesso Sicuro

ATTENZIONE: Attivita sospetta rilevata sul tuo conto
Abbiamo rilevato un tentativo di accesso non autorizzato al tuo conto Intesa Sanpaolo. Per proteggere il tuo account, ti invitiamo a confermare la tua identita accedendo al tuo profilo. Ultimo accesso sospetto: 27/02/2025 alle 21:15
Posizione: Milano, IT
Accesso al tuo Internet Banking
Email o ID Cliente: _____
Password: _____

[Accedi per verifica]

Problemi di accesso? [Recupera le credenziali]
Non sei tu? [Segnala attività sospetta]
ATTENZIONE! SEI CADUTO IN UN TEST DI PHISHING!
Hai appena interagito con una simulazione di attacco di phishing organizzata per aumentare la consapevolezza sulla cybersecurity. Nessuna informazione e stata raccolta, ma il tuo comportamento e stato registrato a fini didattici.
Hai riconosciuto il phishing?
- Si --> Complimenti! La tua attenzione alla sicurezza e ottima.
- No, ho inserito i dati --> Nessun problema! Questo test serve per imparare a difendersi. Come proteggersi dal phishing?
- Controlla SEMPRE l'indirizzo del mittente
- Non inserire credenziali su pagine non ufficiali
- Controlla il link prima di cliccare
- In caso di dubbio, contatta direttamente la banca
Segnalalo subito! Se ricevi email sospette, inoltrale al reparto IT o alla sicurezza informatica.

Nel nostro caso, la landing page finge di essere una pagina di accesso a Intesa Sanpaolo, inducendo gli utenti a inserire le loro credenziali. Tuttavia, invece di raccogliere dati reali, la pagina registra solo le interazioni degli utenti per:

- Misurare la consapevolezza sulla sicurezza: Quanti dipendenti riconoscono il phishing?
- Individuare aree di miglioramento: Chi è più vulnerabile a questi attacchi?
- Formare il personale: Dopo il test, gli utenti imparano dai loro errori.

Una landing page può essere un potente strumento per testare, formare e analizzare il comportamento degli utenti nella cybersecurity.