Report: Simulazione Email di Phishing

Esercizio del Giorno

Obiettivo: Creare una simulazione di un'email di phishing utilizzando ChatGPT.

Istruzioni:

1. **Creare uno scenario:**
   - Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata. Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
   - Definite chiaramente l'obiettivo del phishing (ad esempio, ottenere credenziali di accesso, informazioni personali, dati finanziari, ecc.).
2. **Scrivere l'email di phishing:**
   - Utilizzate ChatGPT per generare il contenuto dell'email.
   - Assicuratevi che l'email sia convincente, ma anche che contenga gli elementi tipici delle email di phishing (ad esempio, richieste urgenti, link sospetti, errori grammaticali).
3. **Spiegare lo scenario:**
   - Descrivete lo scenario che avete creato.
   - Spiegate perché l'email potrebbe sembrare credibile alla vittima.
   - Evidenziate gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

Scenario: Finta Notifica Bancaria

L'email simula una notifica di sicurezza urgente, sfruttando il timore dell'utente di perdere l'accesso al proprio conto bancario. Questo tipo di phishing è comune perché si basa sulla fiducia e sul riconoscimento del marchio, spingendo la vittima ad agire senza riflettere.

Perché l'email potrebbe sembrare credibile:

1. **Linguaggio professionale:** Il testo utilizza un tono formale e termini come "Servizio Sicurezza Online" per apparire legittimo.

2. **Dettagli plausibili:** Fa riferimento a Intesa Sanpaolo, una banca reale, e descrive restrizioni comuni come l'impossibilità di effettuare bonifici.

3. **Urgenza:** La minaccia di sospendere il conto entro 24 ore costringe la vittima a prendere decisioni rapide.

Elementi dell'email che dovrebbero far scattare un campanello d'allarme:

4. **Mittente sospetto:** L'email proviene da un indirizzo personale che da un dominio ufficiale
5. **Link fraudolento:** Il link indicato non è visibile, il che potrebbe nascondere un indirizzo fraudolento.
6. **Errori grammaticali e stilistici:** Sebbene minimi, ci sono incongruenze che possono indicare la natura non ufficiale del messaggio.

7. **Richiesta di credenziali:** Nessuna banca reale chiederebbe di inserire dati sensibili tramite email.

⚠️ Importante: Accesso limitato al tuo conto Intesa Sanpaolo! Posta in arrivo ×

Kaito Kaito <kaitokito989@gmail.com>
a me

Gentile Cliente,

Abbiamo rilevato un'attività insolita sul tuo conto presso Intesa Sanpaolo. Per proteggere il tuo conto e i tuoi fondi, abbiamo temporaneamente limitato alcune funzionalità del tuo account.

Cosa significa questo?

- Non puoi effettuare bonifici o pagamenti online.
- L'accesso al tuo conto potrebbe essere ulteriormente limitato se non verifichi le tue credenziali.

Per ripristinare immediatamente l'accesso al tuo conto, ti invitiamo a verificare le tue informazioni cliccando sul seguente link:

Verifica il tuo conto ora

Attenzione: Se non completi questa operazione entro 24 ore, il tuo conto potrebbe essere bloccato definitivamente.

Ti ricordiamo che la tua sicurezza è la nostra priorità. Per eventuali dubbi, contatta il nostro Servizio Clienti.

Cordiali saluti,
Intesa Sanpaolo - Servizio Sicurezza Online

© 2025 Intesa Sanpaolo S.p.A. Tutti i diritti riservati.

Bonus 1: fare mail irriconoscibile
Bonus 2: fare anche l'html copiando una mail di phishing

Bonus 1:

Importante: Verifica dell'attività insolita sul tuo conto Intesa Sanpaolo Posta in arrivo ×

Kaito Kaito <kaitokito989@gmail.com>
a me

Gentile Cliente,

Abbiamo rilevato un'attività insolita sul tuo conto Intesa Sanpaolo durante una recente verifica di sicurezza. Per proteggere il tuo conto e prevenire eventuali accessi non autorizzati, ti chiediamo di confermare i tuoi dati entro 48 ore.

Per completare la verifica, accedi tramite il seguente link sicuro:
www.intesasanpaolo-verifiche.com

Questa procedura richiede solo pochi minuti e garantirà la piena funzionalità del tuo conto. Ti ricordiamo che il mancato completamento della verifica potrebbe portare a restrizioni temporanee sul tuo conto.

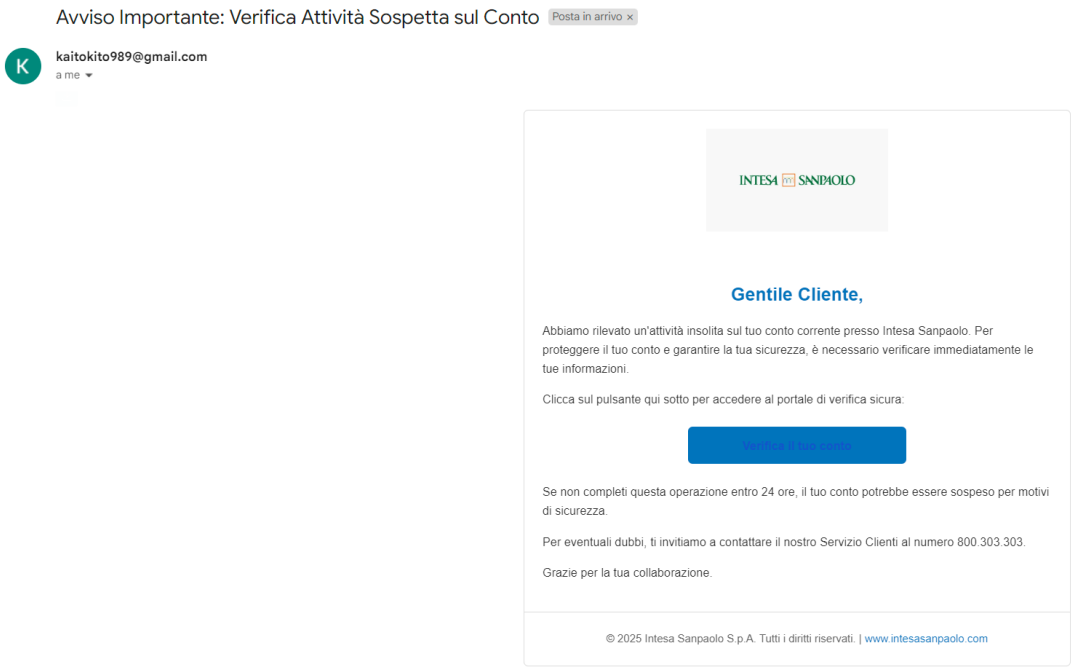
Se hai domande o hai già completato questa verifica, ti invitiamo a contattare il nostro Servizio Clienti al numero gratuito 800 123 456.

Grazie per la tua collaborazione,
Intesa Sanpaolo – Servizio Sicurezza

Nota: Per la tua sicurezza, non condividere mai le tue credenziali con nessuno. Intesa Sanpaolo non ti chiederà mai di fornire il PIN o la password via e-mail.

La seconda email elimina molti errori evidenti della prima, migliorando la grammatica, il tono e la formattazione. Il link è più credibile (simile al dominio della banca), il linguaggio è più professionale e l'urgenza è meno pressante (48 ore invece di 24). Inoltre, l'aggiunta di una nota finale ("non ti chiederà mai PIN o password") aumenta la percezione di autenticità, rendendo il phishing più sofisticato e difficile da individuare.

Bonus 2:



Questo rappresenta l'ultimo esempio di phishing richiesto, dove grazie all'utilizzo di elementi HTML l'email appare molto più credibile e professionale. Questo approccio riflette il modo in cui sono strutturate la maggior parte delle moderne email di phishing, sfruttando un design accurato e dettagli visivi per aumentare l'efficacia nel convincere le vittime.