Scenario Creato:

Immagina una situazione in cui un cliente di una banca italiana, come Intesa Sanpaolo, riceve un'email apparentemente inviata dalla banca stessa. L'email afferma che c'è stata un'attività sospetta sul conto del cliente e che è necessario confermare immediatamente le proprie credenziali per evitare il blocco temporaneo del conto. L'obiettivo del phishing è ottenere le credenziali di accesso dell'utente e potenzialmente anche altre informazioni finanziarie, come il numero della carta di credito o il codice PIN.

Simulazione Email di Phishing

Scenario Spiegato:

Questa email è progettata per sembrare una notifica urgente da Intesa Sanpaolo, una banca reale e ben conosciuta in Italia. È plausibile che una persona possa ricevere un'email simile in caso di attività sospetta sul proprio conto, il che rende l'email credibile e aumenta la probabilità che la vittima clicchi sul link fornito.

Elementi di Credibilità:

- **Utilizzo del Nome della Banca:** Usare un nome noto come Intesa Sanpaolo rende l'email più credibile.
- **Contenuto Rilevante e Urgente:** L'avviso di un'attività sospetta spinge la vittima ad agire rapidamente per paura di perdere l'accesso al conto.
- **Link Convincente:** L'URL fornito sembra legittimo e correlato alla banca, sebbene contenga una lieve differenza rispetto al dominio ufficiale.

Campanelli d'Allarme sull'Autenticità:

- **Errore di Formattazione nei Numeri (€1,250,00):** In Italia, si usa il punto per separare i decimali, non la virgola.
- **Indirizzo Email Sospetto:** L'indirizzo del mittente non corrisponde al dominio ufficiale della banca (supporto@intesasanpaolo.com).
- **Richiesta di Credenziali:** Le banche reali non chiedono mai di confermare le credenziali tramite email.
- **Senso di Urgenza:** Un linguaggio eccessivamente allarmante è tipico delle email di phishing.

Questi elementi dovrebbero far scattare un campanello d'allarme per l'utente attento alla sicurezza delle proprie informazioni personali.

Davide Stefani