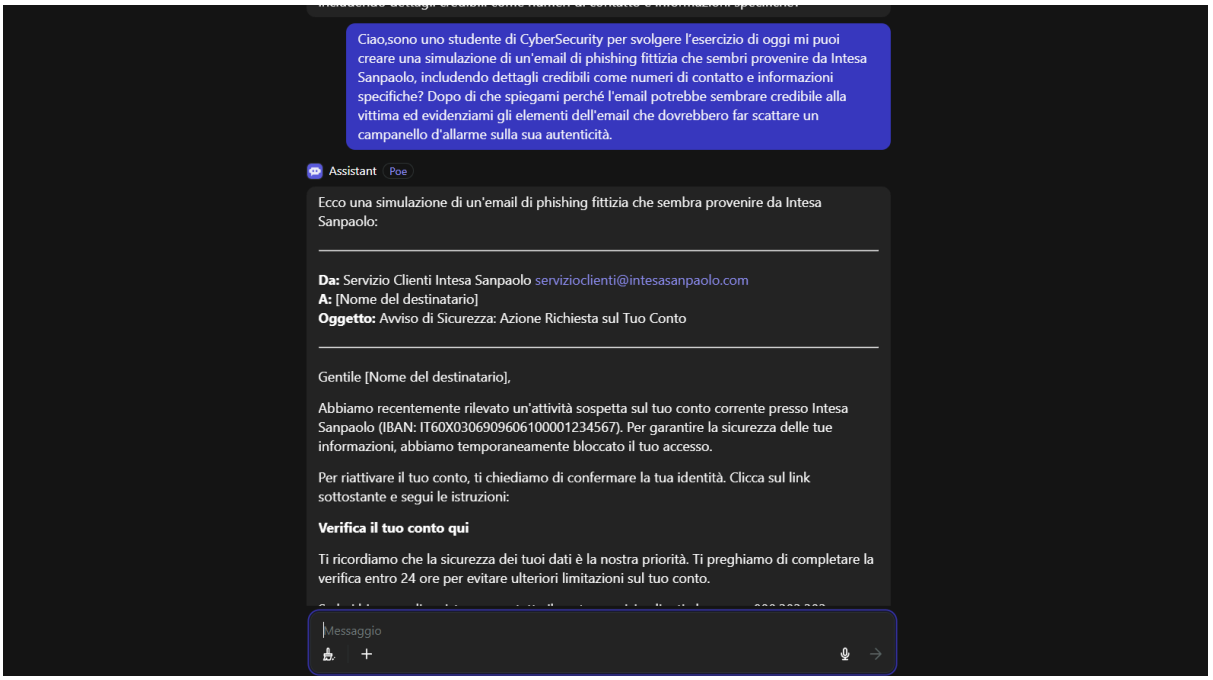
# Scenario di Phishing: Email Fittizia da Intesa Sanpaolo

## Spiegazione

Per svolgere questo esercizio ho chiesto a Poe: “Ciao,sono uno studente di CyberSecurity per svolgere l’esercizio di oggi mi puoi creare una simulazione di un'email di phishing fittizia che sembri provenire da Intesa Sanpaolo, includendo dettagli credibili come numeri di contatto e informazioni specifiche?" Dopo di che spiegami perché l'email potrebbe sembrare credibile alla vittima ed evidenziami gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.




**NB:**Essendo che la potenziale vittima potrebbe riconoscere il suo Iban lo sono andato a togliere dall’email.

## Contesto

Un'email di phishing viene inviata a un cliente di Intesa Sanpaolo, fingendo di essere una comunicazione ufficiale dal servizio clienti della banca. L'email avvisa il destinatario di un problema urgente con il suo conto.

## Obiettivo del Phishing

L'obiettivo è ottenere le credenziali di accesso del cliente, inclusi nome utente e password, per sfruttare il suo conto bancario.

# Email di Phishing

---

**Da:** Servizio Clienti Intesa Sanpaolo servizioclienti@intesasanpaolo.com
**A:** [Nome del destinatario]
**Oggetto:** Avviso Importante: Problema di Sicurezza con il Tuo Conto

---

Gentile Paolo Rampino,

Siamo spiacenti di informarti che abbiamo rilevato un accesso non autorizzato al tuo conto corrente presso Intesa Sanpaolo. Per proteggere la tua sicurezza, abbiamo temporaneamente bloccato il tuo accesso.

Per riattivare il tuo conto, ti chiediamo di confermare la tua identità. Clicca sul link sottostante e segui le istruzioni:

[Link sospetto]

Ti ricordiamo che la sicurezza dei tuoi dati è la nostra priorità. Ti preghiamo di completare la verifica entro 24 ore per evitare ulteriori limitazioni sul tuo conto.

Se hai bisogno di assistenza, non esitare a contattare il nostro servizio clienti al numero 800.303.303.

Grazie per la tua collaborazione.

Cordiali saluti,
**Servizio Clienti Intesa Sanpaolo**
Intesa Sanpaolo S.p.A.
Piazza San Carlo, 156, 10121 Torino
Tel: 800.303.303

---

# Spiegazione dello Scenario

## Credibilità dell'Email

L'email potrebbe sembrare credibile per diversi motivi:

1. **Branding Fattibile**: Utilizza il logo e il linguaggio formale tipico delle comunicazioni bancarie.
2. **Richiesta Urgente**: La minaccia di sospensione del conto crea un senso di urgenza, spingendo il destinatario a reagire rapidamente.
3. **Link Apparente**: Il link sembra legittimo, aumentando la probabilità che la vittima ci clicchi sopra.

## Elementi di Allerta

Dovrebbero scattare dei campanelli d'allarme per i seguenti motivi:

1. **Errore di Dominio**: L'indirizzo email non corrisponde a quello ufficiale di Intesa Sanpaolo.
2. **Link Suspicious**: L'URL del link è sospetto e non corrisponde al dominio della banca.
3. **Richieste di Informazioni Sensibili**: Le banche non chiedono mai informazioni personali tramite email.

Questi elementi possono aiutare i destinatari a riconoscere un tentativo di phishing e a proteggere le proprie informazioni personali.