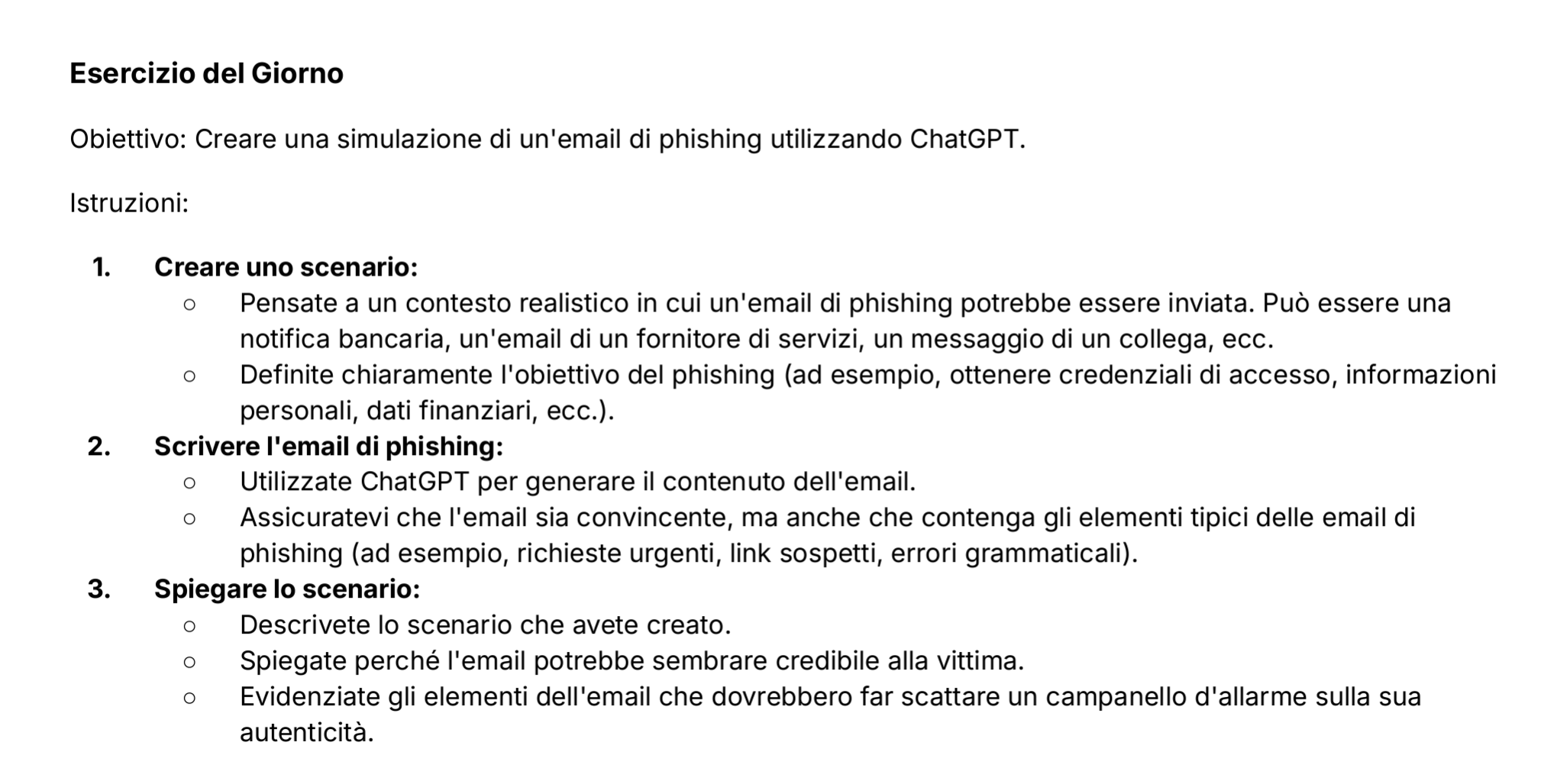
# Report: Simulazione Email di Phishing



## 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.

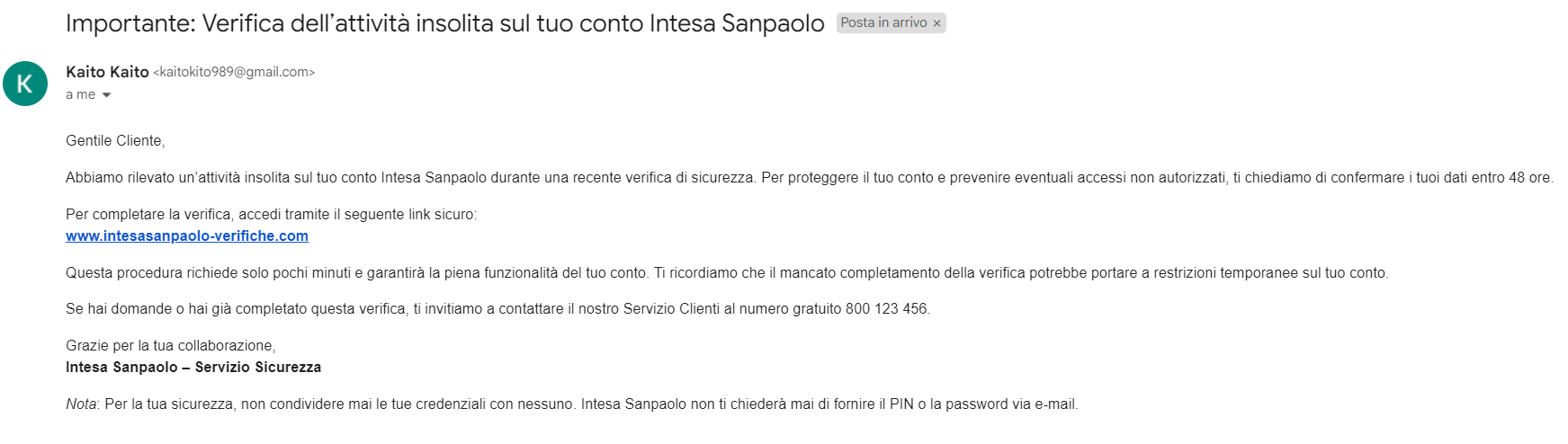
**Elementi dell’email che dovrebbero far scattare un campanello d’allarme:**

1. **Mittente sospetto:** L'email proviene da un indirizzo personale che da un dominio ufficiale
2. **Link fraudolento:** Il link indicato non è visibile, il che potrebbe nascondere un indirizzo fraudolento.
3. **Errori grammaticali e stilistici:** Sebbene minimi, ci sono incongruenze che possono indicare la natura non ufficiale del messaggio.
4. **Richiesta di credenziali:** Nessuna banca reale chiederebbe di inserire dati sensibili tramite email.



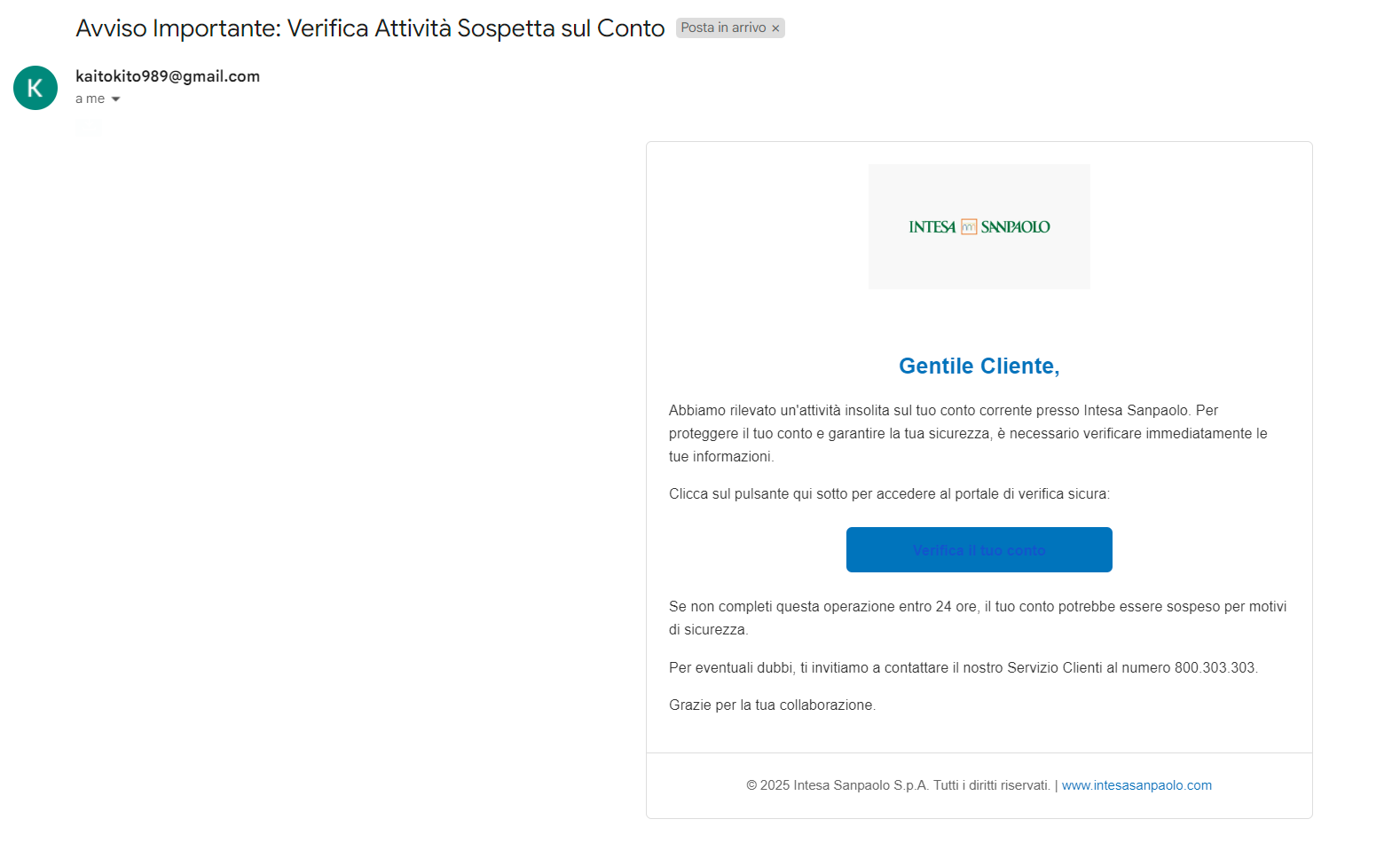
Bonus 1: fare mail irriconoscibile  
Bonus 2: fare anche l'html copiando una mail di phishing

Bonus 1:



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.