

# Social Engineering

## Obiettivo dell'esercizio:

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

## Scenario:

Un utente riceve un'email che simula una comunicazione ufficiale di Intesa Sanpaolo.

Il messaggio avverte che e' stata rilevata un'attività sospetta nell'account, ed e' necessaria una conferma del numero di cellulare dell'utente.

Nell'email sara' presente un link che puntera' a una pagina web clone di Intesa Sanpaolo per l'ottenimento del numero di cellulare, a quel punto l'autore dell'email potra' chiamare la vittima spacciandosi per un operatore della banca e estrapolare altre informazioni sensibili tramite tecniche di social engineering.

**Nel migliore dei casi**, la vittima sarà in grado di riconoscere il tentativo di truffa e provvederà a segnalare tempestivamente l'accaduto alla propria banca.

**Nel peggiore dei casi**, l'utente, privo di adeguata esperienza digitale o non abituato a riconoscere segnali di phishing, potrebbe ritenere autentica la comunicazione e fornire informazioni sensibili durante la conversazione telefonica con l'attaccante, facilitando così il completamento della truffa.

## Email di phishing:

**Oggetto:** Intesa Sanpaolo - Verifica urgente attività sul tuo profilo

**Mittente:** sicurezza@intesasanpaolo.com (*spoofato*)

---

**Gentile Cliente,**

abbiamo rilevato un'attività insolita associata al suo profilo Intesa Sanpaolo.

Per garantire la massima sicurezza del suo conto, è necessario confermare il numero di cellulare associato entro le prossime 12 ore. In caso contrario, potrebbero essere attivate limitazioni temporanee all'operatività online.

Può procedere immediatamente alla verifica cliccando sul seguente link:

[VERIFICA NUMERO DI CELLULARE](#)

Le ricordiamo che Intesa Sanpaolo utilizza la verifica telefonica per garantire l'identità dei propri clienti e prevenire accessi non autorizzati.

**Attenzione.** Se non ha effettuato di recente modifiche al suo profilo o accessi da dispositivi nuovi, le consigliamo di completare la procedura il prima possibile.

Per eventuali dubbi o chiarimenti, può contattarci direttamente tramite l'app Intesa Sanpaolo Mobile, visitare il sito ufficiale o telefonare al numero 800.303.303.

I gestori della Filiale Digitale sono a sua disposizione.

Grazie per la collaborazione,  
**Intesa Sanpaolo**

---

**Note:**

L'hyper-text "**VERIFICA NUMERO DI CELLULARE**" punta al link "<https://intesa-verifica-profilo.com>" ovviamente falso.

## **Analisi dell'email di phishing:**

### **Perche' e' credibile?**

- Contiene gli elementi classici delle email di Intesa Sanpaolo, come i promemoria ambientali (vedere ultime pagine).
- Viene usato un linguaggio formale.
- Il falso senso di urgenza puo' spingere l'utente ad agire impulsivamente.
- Anche se il link non punta a un dominio ufficiale, può contenere parole chiave come "intesa", "verifica", "profilo" per sembrare legittimo.
- L'email cita l'app Intesa Sanpaolo, il numero verde reale (800.303.303) e sezioni del sito vero, elementi che conferiscono maggiore fiducia a chi legge.

### **Elementi che dovrebbero far scattare un campanello d'allarme:**

- **Richiesta sospetta di un'informazione personale (il numero di cellulare):**  
Le banche raramente chiedono di confermare dati personali cliccando su link in email, specialmente in casi non richiesti dall'utente.
- **Link esterno con dominio sospetto:**  
Anche se il testo del link sembra rassicurante, passando il mouse sopra il collegamento (senza cliccare) si può notare un dominio non ufficiale. Le vere email di Intesa usano solo domini come "[intesasnpaolo.com](https://intesasnpaolo.com)".

- **Urgenza non giustificata:**

La scadenza entro 12 ore è una classica tattica del phishing per impedire che l'utente si prenda il tempo di riflettere o contattare direttamente la banca.

**Di seguito, e' presente un'altra rappresentazione dell'email creata, auto-inviatomi per un esempio grafico.**



Matteo Pasetto <matteopasetto02@gmail.com>

---

## Intesa Sanpaolo - Verifica urgente attività sul tuo profilo

---

**Matteo Pasetto** <matteopasetto02@gmail.com>  
A: Matteo Pasetto <matteopasetto02@gmail.com>

2 maggio 2025 alle ore 12:53

**Gentile Cliente,**

abbiamo rilevato un'attività insolita associata al suo profilo Intesa Sanpaolo.

Per garantire la massima sicurezza del suo conto, è necessario confermare il numero di cellulare associato entro le prossime 12 ore. In caso contrario, potrebbero essere attivate limitazioni temporanee all'operatività online.

Può procedere immediatamente alla verifica cliccando sul seguente link:

[VERIFICA NUMERO DI CELLULARE](#)

Le ricordiamo che Intesa Sanpaolo utilizza la verifica telefonica per garantire l'identità dei propri clienti e prevenire accessi non autorizzati.

**Attenzione.** Se non ha effettuato di recente modifiche al suo profilo o accessi da dispositivi nuovi, le consigliamo di completare la procedura il prima possibile.

Prima di stampare, pensa all'ambiente \*\* Think about the environment before printing

---

Il presente messaggio, inclusi gli eventuali allegati, ha natura aziendale e potrebbe contenere informazioni confidenziali e/o riservate. Chiunque lo ricevesse per errore, è pregato di avvisare tempestivamente il mittente e di cancellarlo.

E' strettamente vietata qualsiasi forma di utilizzo, riproduzione o diffusione non autorizzata del contenuto di questo messaggio o di parte di esso.

Pur essendo state assunte le dovute precauzioni per ridurre al minimo il rischio di trasmissione di virus, si suggerisce di effettuare gli opportuni controlli sui documenti allegati al presente messaggio. Non si assume alcuna responsabilità per eventuali danni o perdite derivanti dalla presenza di virus.

Per lo svolgimento delle attività di investimento nel Regno Unito, la società è autorizzata da Banca d'Italia ed è soggetta alla vigilanza limitata della Financial Conduct Authority ( FCA ) e della Prudential Regulation Authority ( PRA ) . Maggiori informazioni in merito ai poteri di vigilanza della Financial Conduct Authority ( FCA ) e della Prudential Regulation Authority ( PRA ) sono a disposizione previa richiesta.

Nel Regno Unito Intesa Sanpaolo S.p.A. opera attraverso la filiale di Londra, sita in 90 Queen Street, London EC4N 1SA, registrata in Inghilterra & Galles sotto No.FC016201, Branch No.BR000036

In osservanza dei requisiti imposti da Internal Revenue Service (Agenzia delle Entrate degli Stati Uniti), qualunque discussione relativa a temi di natura fiscale contenuta in questo messaggio o nei suoi allegati non è intesa né è stata scritta per essere utilizzata, né può essere utilizzata, per (i) evitare l'imposizione di gravami fiscali secondo il codice tributario vigente negli Stati Uniti o (ii) per promuovere, sollecitare o raccomandare una operazione finanziaria o altra transazione indirizzata a un altro destinatario.

Nella Repubblica d'Irlanda, Intesa Sanpaolo Bank Ireland plc è regolamentata dalla Banca Centrale d'Irlanda ed è parte del Gruppo Bancario Intesa Sanpaolo S.p.A. Registrata in Irlanda come società numero 125216 – IVA Reg. IE4817418C IE, sita in 2nd Floor,

International House, 3 Harbourmaster Place, IFSC, Dublino 1, D01 K8F1, Irlanda.

\*\*\*

---

This email (including any attachment) is a corporate message and may contain confidential and/or privileged and/or proprietary information. If you have received this email in error, please notify the sender immediately, do not use or share it and destroy this email. Any unauthorised use, copying or disclosure of the material in this email or of parts hereof (including reliance thereon) is strictly forbidden.

We have taken precautions to minimize the risk of transmitting software viruses but nevertheless advise you to carry out your own virus checks on any attachment of this message. We accept no liability for loss or damage caused by software viruses.

For the conduct of investment business in the UK, the Company is authorised by Banca d'Italia and subject to limited regulation in the UK by the Financial Conduct Authority ( FCA ) and the Prudential Regulation Authority ( PRA ). Details about the extent of our regulation by the Financial Conduct Authority ( FCA ) and the Prudential Regulation Authority ( PRA ) are available from us on request.

In the UK Intesa Sanpaolo S.p.A. operates through its London Branch, located at 90 Queen Street, London EC4N 1SA. Registered in England & Wales under No.FC016201, Branch No.BR000036

To comply with requirements imposed by the IRS, we inform you that any discussion of U.S. federal tax issues contained herein (including any attachments) was not intended or written to be used, and cannot be used by you, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending any transaction or matter addressed herein to another party.

In the Republic of Ireland, Intesa Sanpaolo Bank Ireland plc is regulated by the Central Bank of Ireland and is a member of the Intesa Sanpaolo Group. It is registered in Ireland as company no.125216 – VAT Reg. No. IE 4817418C and located at 2nd Floor, International House, 3 Harbourmaster Place, IFSC, Dublin 1, D01 K8F1, Ireland.



Rispondi

Inoltra



Privo di virus.[www.avast.com](https://www.avast.com)