

## 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.  
*Esempi:* una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
- Definite chiaramente l'obiettivo del phishing.  
*Esempi:* 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
  - Contenente **elementi tipici delle email di phishing**:
    - 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 sospetti** dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.
- 

**Bonus 1:** fare mail irriconoscibile

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

---

## Scenario: Notifica di Blocco del Conto Bancario

### Contesto realistico:

Un utente riceve un'email che sembra provenire dalla propria banca. L'email avvisa che il conto bancario è stato temporaneamente bloccato per "attività sospette" e richiede una verifica urgente per

evitare il congelamento definitivo. L'obiettivo del phishing è ottenere le credenziali di accesso al conto online della vittima.

## Obiettivo

Ottenere le credenziali di accesso dell'utente.

### Email di phishing:

**Oggetto:** Urgente: Verifica necessaria per la tuo conto bancario

**Mittente:** assistenza@bancaintesa-supporto.com

#### Corpo dell'email:

Gentile Cliente,

Abbiamo rilevato attività insolite sul tuo conto bancario e, per proteggere la tua sicurezza, abbiamo temporaneamente bloccato il tuo accesso online.

Per evitare il congelamento definitivo del tuo conto, ti invitiamo a verificare immediatamente la tua identità entro **24 ore**. Basta cliccare sul link sottostante e accedere al tuo account per completare la procedura di verifica.

#### [Accedi al tuo conto sicuro](#)

Se non completi questa verifica entro il termine indicato, il tuo conto sarà disattivato e dovrà recarti presso una delle nostre filiali per riattivarlo.

Per ulteriori informazioni, ti preghiamo di contattare il nostro Servizio Clienti.

Cordiali saluti,

**Team Assistenza Bancaria**

Banca Imtesa

**Nota:** Questa è un'email automatica. Si prega di non rispondere direttamente a questo messaggio.

---

## Spiegazione dello Scenario

### 1. Perché lo scenario è credibile:

- L'email simula un evento che può generare ansia (il blocco del conto bancario).
- Utilizza un tono professionale e include dettagli tipici delle email ufficiali, come una firma aziendale e un invito a non rispondere direttamente al messaggio.
- Il mittente sembra autentico grazie a un dominio che imita quello reale della banca.

### 2. Perché l'email può ingannare la vittima:

- L'urgenza (entro 24 ore) spinge la vittima ad agire senza riflettere.

- Il link sembra plausibile, ma il dominio è leggermente diverso da quello ufficiale (ad esempio, "bancaintesa-verifica.com" invece di "bancaintesa.com").
- La minaccia di un congelamento definitivo del conto crea pressione psicologica.

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

- Il dominio dell'email del mittente non è esattamente quello ufficiale.
- La richiesta urgente e il tono allarmistico sono tipici delle email di phishing.
- Il link sospetto non corrisponde al dominio ufficiale della banca.
- Sono presenti due errori grammaticali, uno nell'oggetto e uno nella firma della banca
- Non ci sono riferimenti specifici al cliente, come il nome completo o il numero di conto, che una banca autentica includerebbe.

Ecco altri scenari possibili che possono essere utilizzati

- **Fattura non pagata da un fornitore di servizi.**
- **Conferma di un ordine mai effettuato.**
- **Aggiornamento password da parte di un servizio conosciuto.**
- **Messaggio da un "collega" in azienda.**
- **Rimborso fiscale falso.**
- **Premio vinto in un concorso.**
- **Messaggio di un corriere (es. DHL, FedEx, Poste Italiane).**
- **Offerta di lavoro da una grande azienda.**
- **Avviso di account sospeso (es. PayPal, Netflix, Amazon).**
- **Notifica di accesso non autorizzato a un account.**
- **Aggiornamento software richiesto (es. Microsoft, Adobe).**
- **Richiesta di donazioni per una causa benefica.**
- **Avviso di violazione di copyright o multa online.**
- **Notifica di vincita della lotteria internazionale.**
- **Richiesta di pagamento urgente per un dominio o servizio web.**

## **Bonus 1: fare una mail irriconoscibile**

Per effettuare questo esercizio utilizzeremo l'email spoofing, una tecnica utilizzata per falsificare l'indirizzo email del mittente, facendo sembrare che l'email provenga da una fonte legittima o affidabile (ad esempio una banca, un collega, o un fornitore di servizi), quando in realtà proviene da un attaccante.

### **Come Funziona?**

Gli attaccanti sfruttano la struttura del protocollo **SMTP** (Simple Mail Transfer Protocol), che è alla base dell'invio delle email. SMTP non verifica l'autenticità del mittente, quindi è possibile:

1. Modificare il campo "From" per far sembrare che l'email provenga da un altro indirizzo (es. support@banca.com).

2. Utilizzare server di posta non configurati correttamente o vulnerabili per inviare email con un mittente falsificato.
3. Nascondere la vera identità del mittente utilizzando proxy o reti anonime come Tor.

Esistono diverse tecnologie e standard che possono mitigare i rischi legati all'email spoofing. Alcuni esempi includono:

1. **SPF (Sender Policy Framework)**: Autorizza specifici server di posta a inviare email per conto di un dominio.
2. **DKIM (DomainKeys Identified Mail)**: Aggiunge una firma digitale alle email per garantirne l'integrità.
3. **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**: Combina SPF e DKIM per verificare l'autenticità delle email e fornire istruzioni su come trattare quelle non conformi.
4. **Email filtering avanzato**: Strumenti come i filtri di spam, i gateway email sicuri e gli antivirus aiutano a rilevare e bloccare email malevoli.

Ecco il testo della mail con email address spoofed, testo senza errori e più credibile.

È possibile usare database di leaked informations, dove sono presenti nomi associati indirizzi email per un determinato servizio. In questo caso è possibile adattare la mail associando SERVIZIO, NOME COGNOME e indirizzo email, rendendo la mail pressoché irriconoscibile da quella reale.

**Oggetto:** Importante: Aggiornamento obbligatorio per il tuo account Banca Intesa

**Mittente:** notifiche@bancaintesa.it

**Corpo dell'email:**

Gentile Cliente,

Abbiamo aggiornato i nostri Termini di Servizio e le nostre Norme sulla Privacy per migliorare la tua esperienza e garantire la sicurezza del tuo account. Tuttavia, abbiamo bisogno della tua collaborazione per continuare ad accedere ai nostri servizi senza interruzioni.

Ti chiediamo di confermare le informazioni relative al tuo account cliccando sul seguente link:

 [Conferma le tue informazioni ora](#)

Per motivi di sicurezza, ti preghiamo di completare questa operazione entro **48 ore**. Se non rispondi entro il termine indicato, il tuo account potrebbe essere limitato.

Grazie per la tua collaborazione.

Cordiali saluti,

**Il Team di Supporto Clienti**

Banca Intesa Sanpaolo

**Nota:** Non rispondere a questa email, è stata inviata automaticamente dal nostro sistema.

### **Elementi che sembrano autentici:**

1. **Mittente apparentemente legittimo:** L'indirizzo email include il nome del servizio e un formato professionale.
2. **Tono professionale:** L'email usa un linguaggio formale e chiaro, simile alle vere email di aziende.
3. **Richiesta di azione:** L'urgenza (es. scadenza di 48 ore) spinge la vittima ad agire velocemente senza riflettere.
4. **Dettagli specifici:** L'inserimento del nome della vittima (anche generico) e riferimenti ai "Termini di Servizio" danno un'apparenza di credibilità.

### **Campanelli d'allarme:**

1. **Dominio sospetto nel link:** Non è il dominio ufficiale del servizio.
2. **Richiesta di dati sensibili tramite link:** Un servizio autentico non richiede mai la conferma di dati personali attraverso email non sicure.
3. **Errori sottili:** Il linguaggio è credibile, ma potrebbe contenere piccole anomalie o mancare di dettagli personalizzati.

### **Bonus 1: fare anche l'html copiando una mail di phishing**





Gentile Cliente,

Abbiamo aggiornato i nostri **Termini di Servizio** e le nostre **Norme sulla Privacy** per migliorare la tua esperienza e garantire la sicurezza del tuo account. Tuttavia, abbiamo bisogno della tua collaborazione per continuare ad accedere ai nostri servizi senza interruzioni.

Ti chiediamo di confermare le informazioni relative al tuo account cliccando sul seguente link:

[Conferma le tue informazioni ora](#)

Per motivi di sicurezza, ti preghiamo di completare questa operazione entro **48 ore**. Se non rispondi entro il termine indicato, il tuo account potrebbe essere limitato.

Grazie per la tua collaborazione.

Cordiali saluti,

**Il Team di Supporto Clienti**

Banca Intesa

Nota: Non rispondere a questa email, è stata inviata automaticamente dal nostro sistema.

Il logo è centrato e dimensionato automaticamente con un massimo di **150px** di larghezza per adattarsi al design.

A seguire il codice HTML  
<!DOCTYPE html>

```
<html lang="it">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Importante aggiornamento obbligarorio</title>
</head>
<body style="font-family: Arial, sans-serif; line-height: 1.6; color: #333; margin: 0; padding: 0;">
    <table width="100%" style="background-color: #f8f8f8; padding: 20px;">
        <tr>
            <td align="center">
                <table width="600px" style="background-color: #ffffff; padding: 20px; border-radius: 8px; box-shadow: 0 2px 4px rgba(0,0,0,0.1);">
                    <!-- Logo -->
                    <tr>
                        <td align="center" style="border-bottom: 2px solid #0073e6; padding-bottom: 10px;">
                            
                        </td>
                    </tr>
                    <!-- Corpo dell'email -->
                    <tr>
                        <td style="padding: 20px;">
                            <p>Gentile Cliente,</p>
                            <p>
                                Abbiamo aggiornato i nostri <strong>Termini di Servizio</strong> e le
                                nostre <strong>Norme sulla Privacy</strong> per migliorare la tua esperienza e garantire la
                                sicurezza del tuo account.
                            </p>
                            Tuttavia, abbiamo bisogno della tua collaborazione per continuare ad
                            accedere ai nostri servizi senza interruzioni.
                            </p>
                            <p>Ti chiediamo di confermare le informazioni relative al tuo account
                            cliccando sul seguente link:</p>
                            <p style="text-align: center; margin: 20px 0;">
                                <a href="http://www.bancaintesa-verifica.com"
                                    style="background-color: #0073e6; color: #ffffff; text-decoration: none;
                                    padding: 10px 20px; border-radius: 5px; font-size: 16px;">
                                    Conferma le tue informazioni ora
                                </a>
                            </p>
                            <p>
                                Per motivi di sicurezza, ti preghiamo di completare questa operazione
                                entro <strong>48 ore</strong>.
                            </p>
                            Se non rispondi entro il termine indicato, il tuo account potrebbe essere
                            limitato.
                            </p>
                            <p>Grazie per la tua collaborazione.</p>
                        </td>
                    </tr>
                    <!-- Footer -->
                </table>
            </td>
        </tr>
    </table>
</body>
```

```
<tr>
    <td style="padding: 20px; background-color: #f0f0f0; text-align: center; font-size: 12px; color: #777;">
        <p>Cordiali saluti,</p>
        <p><strong>Il Team di Supporto Clienti</strong><br>Banca Intesa</p>
        <p style="margin-top: 20px; font-size: 10px;">Nota: Non rispondere a questa email, &#9677; stata inviata automaticamente dal nostro sistema.</p>
    </td>
</tr>
</table>
</td>
</tr>
</table>
</body>
</html>
```