# PROGETTO SETTIMANA 5

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

Consegna: 1. Creare uno scenario:
○ Pensate a un contesto realistico in cui un'email di phishing potrebbe essere inviata.
Può essere una notifica bancaria, un'email di un fornitore di servizi, un messaggio di un collega, ecc.
○ Definite chiaramente l'obiettivo del phishing
(ad esempio, 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 che contenga gli elementi tipici delle email di phishing
(ad esempio, 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 dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

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

Come prima cosa dobbiamo scegliere una mittente che invogli il destinatario a cliccare sul link malevolo che allegheremo nella mail.
Io ho scelto come mittente Instagram, facendo credere al destinatario che qualcuno stia cercando di entrare nel suo account.
Un ulteriore aspetto che dovrebbe spingere l'utente ad inserire i propri dati all'interno del nostro link è la paura che l'attaccante commetta azioni illegali sfruttando l'identità del malcapitato, che potrebbe dover rispondere di azioni illegali e dovrebbe fronteggiare un eventuale perdita di reputazioni dovuta ad una probabile pubblicazione di contenuti falsi e/o imbarazzanti nel suo profilo social.

la mia mail farà leva sulla perdita dell'account del social, inserendo anche un ultimatum di 24 ore così da mettere pressione all'utente e spingerlo ancora di più cliccare nel link ed inserire i suoi dati.

Per rendere la nostra mail di phishing riconoscibile andremo ad inserire volontariamente diversi campanelli d'allarme che dovrebbero far desistere l'utente dall'entrare nel link malevolo presente nella mail.
Io ho inserito:
Diversi errori grammaticali.
Immagini di bassa qualità.
Link che non è legato ad dominio ufficiale di Instagram.
Mancanza di certificazioni come la firma digitale.

oggetto: ⚠ Tentativo di accesso non autorizzato al tuo account Instagram

mittente: support-instaagram@gmail.com

Ciao @Username_ig,

Abbiamo rilevato un tentativo di accesso non autorizzato al tuo account Instagram da un dispositivo sconosciuto:

**Posizione**: Toronto, Canada
**Dispositivo**: iPhone 14 Pro
Per proteggere il tuo account, abbiamo temporaneamente bloccato l'accesso.
E' necessario confermare immediatamente la tua identità per riattivarlo.

➡ **Conferma la tua identità qui:**
https://secure-insta-support.com/login

⚠ Se non confermi entro 24 ore, il tuo account verra disattivato definitivamente.

Per ulteriori informazioni, contatta il nostro centro di supporto clienti.

Grazie,
Il Team di Sicurezza Instagram

**Attenzione: Questa email è stata inviata automaticamente. Non rispondere a questo messaggio.**

# Esercizio Bonus 1

Consegna: Mail irriconoscibile.

L'obbiettivo di questo esercizio è rendere la mail irriconoscibile

Per rendere la mail irriconoscibile dovremmo evitare gli errori inseriti di proposito nella prima mail, quindi dovremmo evitare errori grammaticali, riprodurre il più fedelmente possibile i toni e il design dio un mail legittima e camuffare il nostro link malevolo.
Dovremmo comunque fare leva sulla paura e su una possibile sospensione dell'account social.

**Oggetto**: Proteggi il tuo account: attività di accesso sospetta rilevata

**Mittente:** no-reply@instagram.com

Ciao @Username_ig,

Abbiamo rilevato un'attività insolita sul tuo account Instagram. È possibile che qualcuno abbia tentato di accedere da un dispositivo o una posizione non riconosciuti.

Posizione: Milano, Italia
Dispositivo: Samsung Galaxy S23
Ora: 10:42 CET, 11 gennaio 2025
Per garantire la sicurezza del tuo account, ti chiediamo di confermare immediatamente che sei stato tu. Se non confermi entro 48 ore, il tuo account potrebbe essere temporaneamente sospeso.

➡ Verifica attività di accesso:
https://instagram.com/security-check

Se non sei stato tu, ti consigliamo di cambiare subito la password e abilitare l'autenticazione a due fattori per maggiore protezione.

Grazie per la tua collaborazione.

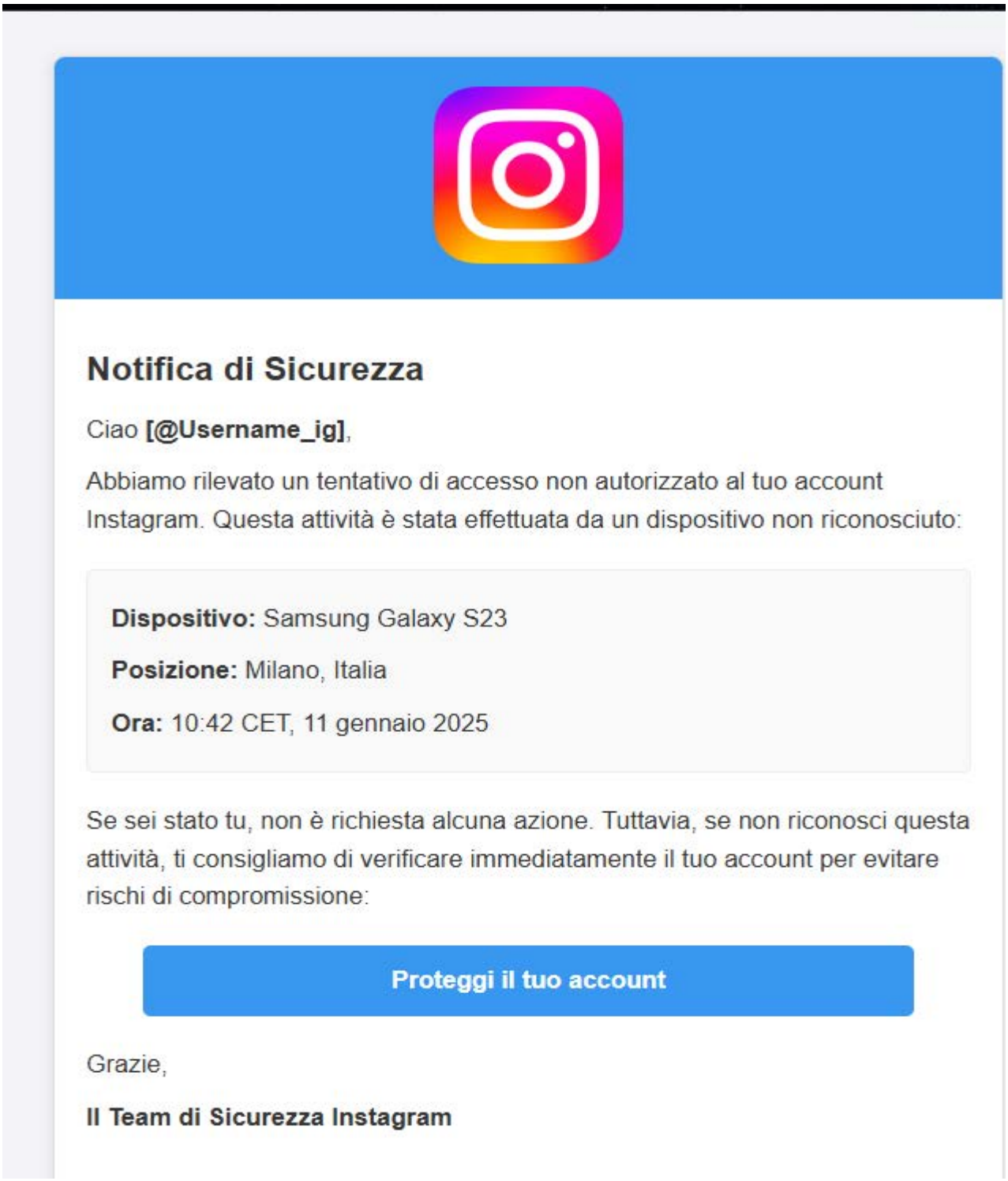
Instagram Security Team

Per ulteriori informazioni su come proteggere il tuo account, visita il nostro Centro assistenza: https://help.instagram.com

# Esercizio Bonus 2

Consegna: fare l'html copiando una mail di phishing

Come prima  cosa ho creato il codice html aiutandomi con ChatGPT, per poi andare a modificarlo secondo le mie esigenze, ho preso spunto dalla classica email di Instagram di protezione account e ho aggiunto un bottone con scritto "Proteggi il tuo account" ala paginal login vero e proprio di Instagram (ipoteticamente il furto delle credenziali dovrebbe avvenire in questa pagina)



Una volta che l'utente clicca nel tasto blu "Proteggi il tuo account" verrà indirizzato nella pagina di login dove dovrebbe avvenire il furto delle credenziali.