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. 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.

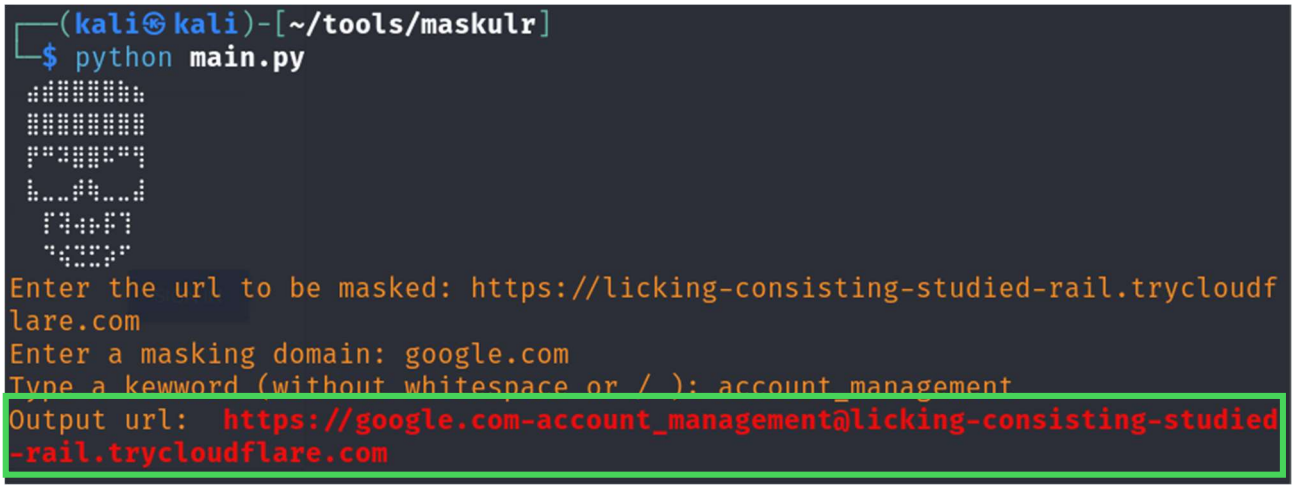
Bonus:

Bonus 1: fare mail irriconoscibile

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

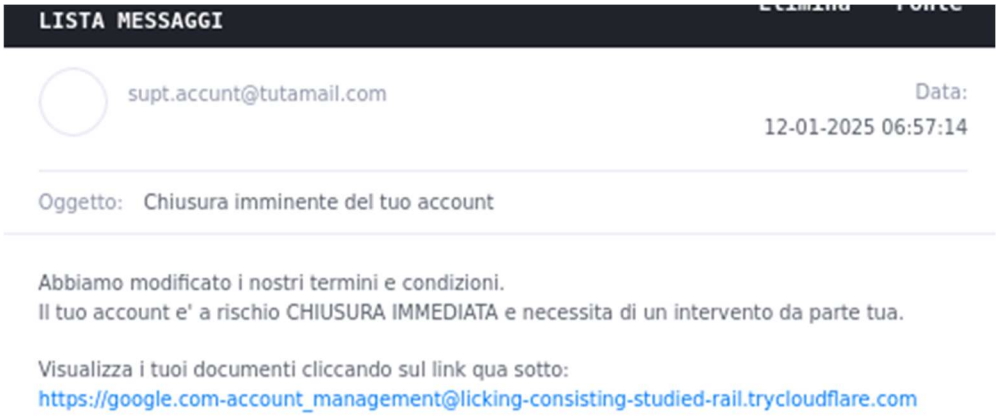
Per l'esercitazione, ho utilizzato un indirizzo e-mail temporaneo generato tramite il sito temp-mail.org. Successivamente, ho creato un link malevolo che reindirizzava a una falsa pagina di login di Google, sfruttando un tool disponibile su GitHub chiamato ZPhisher.

Poiché il link generato risultava sospetto, ho deciso di mascherarlo utilizzando un altro tool Python, anch'esso reperito su GitHub. Questo ha permesso di far apparire il link più credibile, includendo parole familiari come "google.com" e "account management", che potrebbero rassicurare la vittima.



Per inviare la mail, ho creato un account e-mail "supt.accunt@tuta.com" tramite il servizio SMTP gratuito **tuta.com**, il quale, diversamente da Gmail, non richiede un numero di telefono per la registrazione. Questo servizio consente di incollare direttamente il codice HTML personalizzato nel corpo della mail, un aspetto fondamentale per utilizzare un template già pronto.

Grazie a **ChatGPT**, ho elaborato il contenuto della mail di phishing, che è risultato come segue:



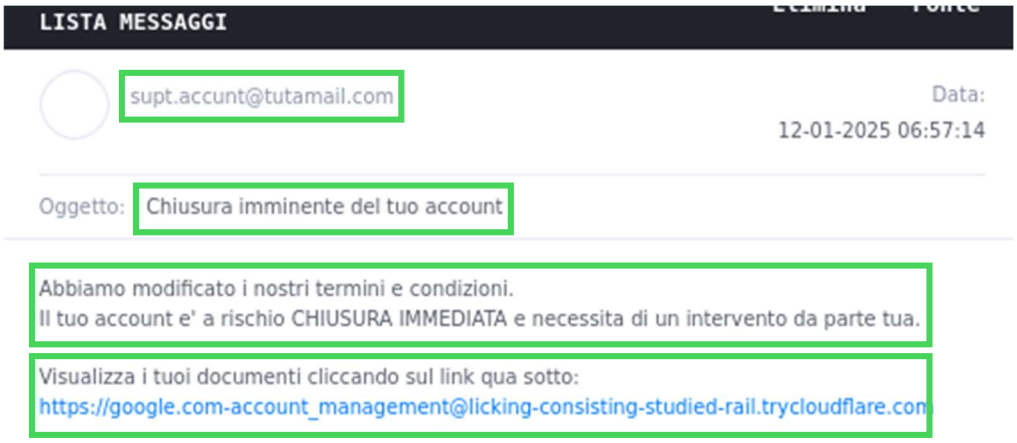
Prossimo notare molte cose che potrebbero far pensare che sia una mail di phishing.

Indirizzo e-mail del mittente: È evidente che non proviene da Google, poiché il dominio è "@tutamail.com" anziché il dominio ufficiale "@google.com". Le aziende ufficiali utilizzano sempre domini aziendali.

Oggetto: Formulato con l'unico scopo di generare urgenza, spingendo l'utente ad agire rapidamente senza riflettere.

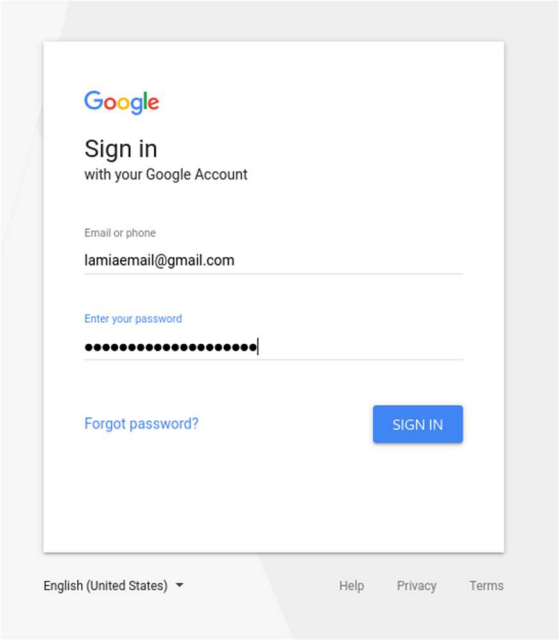
Corpo del messaggio: Trasmette un senso di urgenza senza fornire dettagli specifici sul servizio interessato. Nessun provider serio minaccerebbe di bloccare un account senza preavviso.

Link sospetto: Sebbene la prima parte sembri legittima, analizzando il link completo si nota che esso punta a "trycloudflare.com", un dominio non correlato a Google.

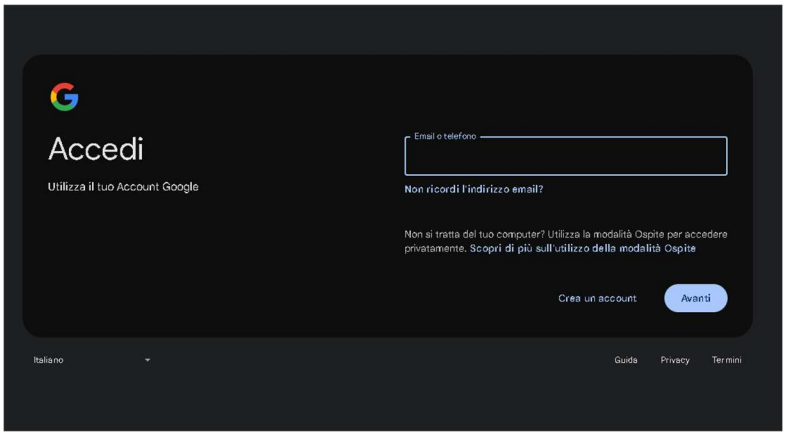


Una volta che la vittima clicca sul link, l'attaccante ottiene immediatamente l'indirizzo IP pubblico dell'utente senza che quest'ultimo se ne accorga.

Successivamente l'utente viene reindirizzato a una falsa pagina di login di Google che, a prima vista, appare identica a quella originale. Tuttavia, confrontando la URL con quella autentica di Google (https://accounts.google.com), si notano differenze.

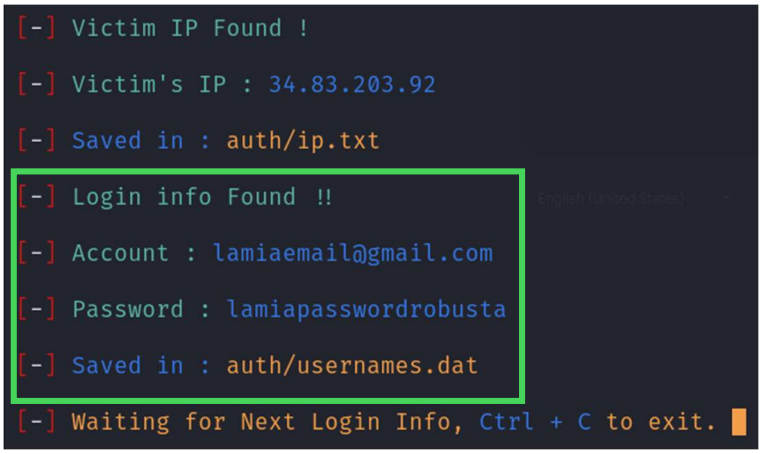


Pagina clonata



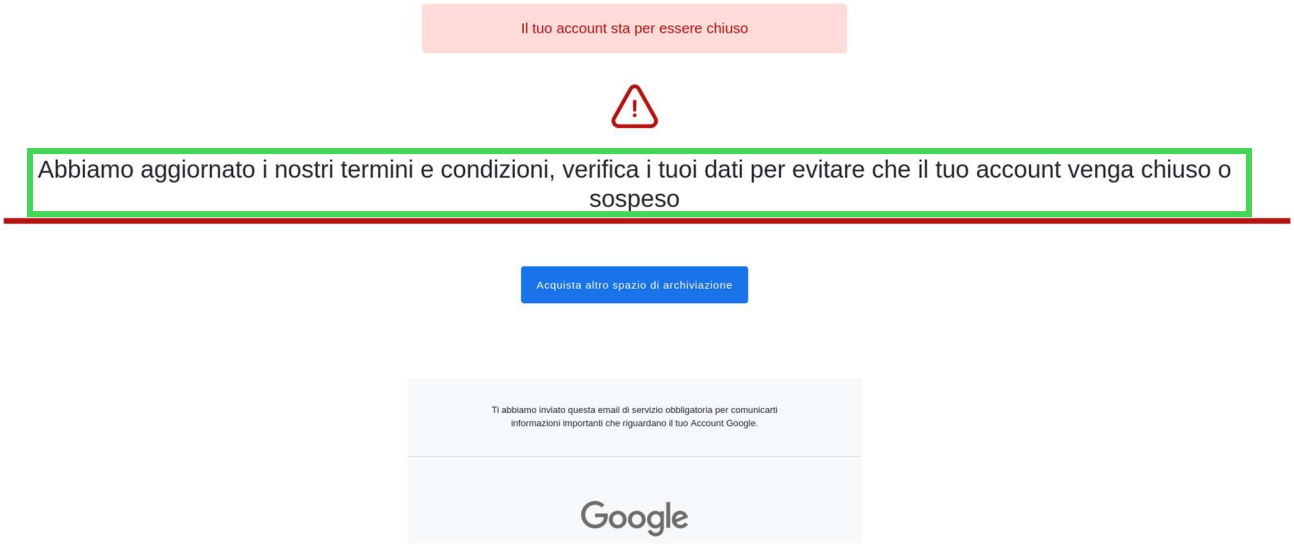
Pagina ufficiale di login Google

Inserendo le credenziali nella pagina clonata, queste vengono immediatamente inviate all'attaccante, mentre la vittima viene reindirizzata alla vera pagina di login di Google, attribuendo il tutto a un "errore di connessione".

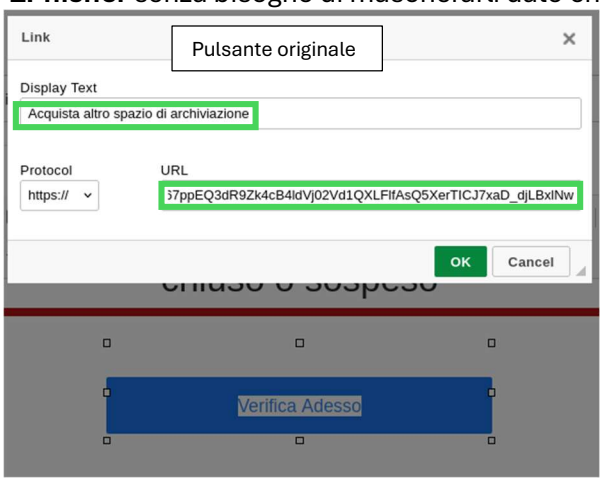


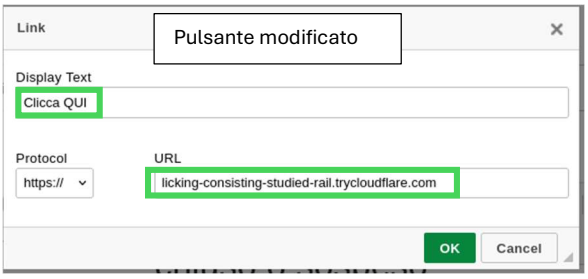
Per la seconda parte, ho preso come riferimento un template ricevuto da Google riguardante l'esaurimento dello spazio di archiviazione su Google Drive. Ho ottenuto il codice HTML originale utilizzando l'opzione "Mostra originale" e "copia negli appunti".

Ho poi importato il template in **GoPhish**, un tool che consente di modificare template HTML aggiungendo frasi allarmanti.
Permette anche l'invio e della mail ma per poterla inviare, e necessario mettersi in coda quindi per rapidità ho preferito utilizzare un altro servizio SMTP (tuta.com) gratuito per l'invio della mail.

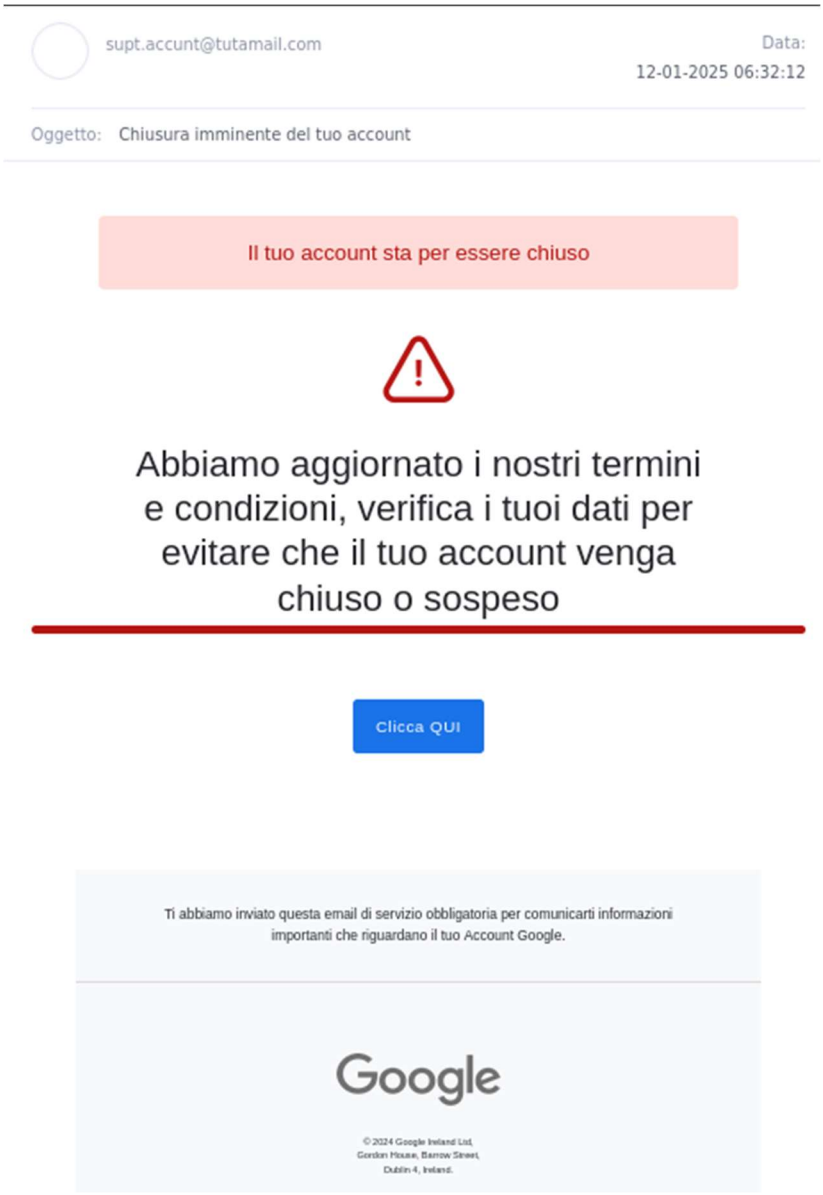


Ho modificato i pulsanti del template originale, sostituendo i link legittimi con quelli generati tramite **ZPhisher** senza bisogno di mascherarli dato che non viene mostrato.





A fine modifiche, la mail finale risulterà in questa maniera:



La mail finale risulta visivamente molto simile a una legittima comunicazione di Google, sfruttando lo stesso layout e le stesse icone. Tuttavia, analizzando i dettagli come l'indirizzo del mittente o il link incorporato nei pulsanti, è possibile identificare il phishing. Purtroppo, la maggior parte degli utenti medi non presta attenzione a tali dettagli, rendendo l'attacco particolarmente efficace.