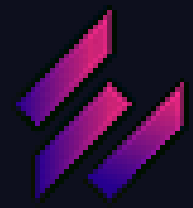


# REPORT

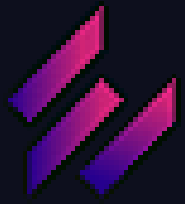
## Creazione email di phishing

By Xian Long Qiu



# Indice

- Panoramica pag. 3
- Scenario phishing pag.5
- Email di phishing pag.6
- Motivazione della credibilita' pag.7
- Elementi d'allarme pag.9
- Metodi di protezione pag.11
- Conclusione pag.13



# Panoramica

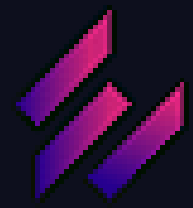
Creare una simulazione di un'email di phishing utilizzando ChatGPT.

## Scopo

Capire perché l'email potrebbe sembrare credibile alla vittima. Analizzare gli elementi dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

## Origine traccia

Il presente report è relativo al Modulo 2 - Settimana 1 - lezione 5  
del corso sulla piattaforma Epicode



# Strumenti

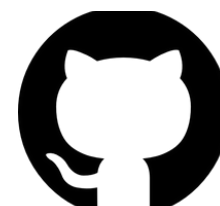


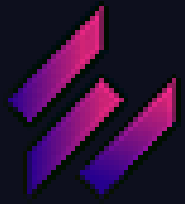
-ChatGPT è un modello di linguaggio basato sull'intelligenza artificiale sviluppato da OpenAI, progettato per comprendere e generare testo in modo naturale e fluido. Può essere utilizzato come strumento di assistenza per una vasta gamma di compiti.

## Fonte

Repository

<https://github.com/XLQcyber/CS0225>





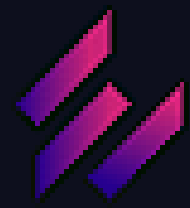
# Creare scenario phishing

**Contesto realistico:** email inviato dalla polizia postale

**L'obiettivo principale** è indurre la vittima a cliccare sul link per:

1. Rubare dati sensibili, come credenziali personali attraverso un falso sito web di verifica dell'identità.
2. Installare malware nel dispositivo della vittima tramite un sito trappola o un download automatico.
3. Estorcere denaro, ad esempio con minacce di azioni legali fasulle che portano a una falsa "multa online" o pagamento immediato per evitare la denuncia.

Oggetto: ⚠ Notifica urgente: violazione rilevata sul suo indirizzo IP  
Mittente: Polizia Postale [sicurezza@poliziapostale-info.it](mailto:sicurezza@poliziapostale-info.it)




# Email di phishing creata da ChatGPT

Gentile cittadino,

il nostro sistema ha rilevato attività anomale provenienti dal suo indirizzo IP nelle ultime 48 ore. Queste attività potrebbero essere collegate alla distribuzione non autorizzata di contenuti digitali protetti.

Ai sensi dell'articolo 171 della legge sul diritto d'autore, è necessario che lei collabora immediatamente per evitare procedimenti giudiziari.

Clicchi sul link sottostante per visualizzare il rapporto completo e confermare la sua identità:

 [Visualizza notifica ufficiale](#)

Se non riceveremo una risposta entro 24 ore, la sua posizione verrà inoltrata all'autorità giudiziaria competente per ulteriori accertamenti.

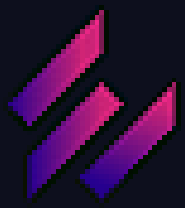
Per eventuali chiarimenti, la preghiamo di non rispondere a questa email, ma utilizzare il portale dedicato.

**Servizio Anticrimine Informativo**

Polizia Postale e delle Comunicazioni

[www.poliziadistato.it](http://www.poliziadistato.it)

Usiamo il prompt per inviare la richiesta di creazione email con le informazioni dello scenario. Il seguente e' il risultato email phishing.



# Motivazione alla credibilita' dalla parte della vittima.

Questa email di phishing è credibile per la vittima per una serie di motivi ben studiati che sfruttano elementi psicologici e visivi:

## ✓ 1. Apparenza istituzionale

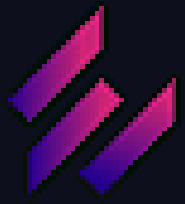
- L'email si presenta come proveniente da un'autorità conosciuta e temuta: la Polizia Postale.
- Include un linguaggio formale e riferimenti a leggi reali (es. art. 171 della legge sul diritto d'autore), aumentando il senso di legittimità.

## ✓ 2. Tono autorevole e minaccioso

- L'uso di frasi come "procedimenti giudiziari" o "inoltrata all'autorità giudiziaria" sfrutta la paura e l'ansia di conseguenze legali.
- Questo tono mette sotto pressione la vittima e riduce il tempo per riflettere.

## ✓ 3. Urgenza temporale

- L'imposizione di una scadenza ("entro 24 ore") fa leva sulla fretta, spingendo la vittima ad agire immediatamente senza verificare l'autenticità del messaggio.



#### ✓ 4. **Contenuto plausibile**

- L'accusa è generica ("attività anomale", "contenuti protetti"), ma verosimile: chiunque potrebbe temere di aver scaricato qualcosa di illegale involontariamente.

#### ✓ 5. **Link apparentemente normale**

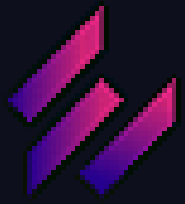
- Il link contiene parole come "verifica", "identità" e "polizia", che lo fanno sembrare coerente con la comunicazione e non immediatamente sospetto per occhi inesperti.

#### ✓ 6. **Uso del "noi" istituzionale**

- L'uso di frasi come "il nostro sistema ha rilevato" dà l'impressione di un controllo informatico centralizzato, aumentando la credibilità tecnica del messaggio.

Questi elementi insieme rendono l'email **altamente persuasiva** per un utente.



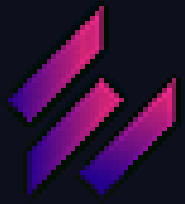


# Elementi d'allarme



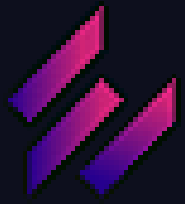
Elementi che fanno scattare l'allarme (campanelli di allarme)

1. **Mittente sospetto**: Anche se appare come "Polizia Postale", l'indirizzo email reale non è ufficiale né appartenente a un dominio governativo (come .gov.it o .poliziadistato.it).
2. **Errori grammaticali e sintattici**: Frasi scorrette come “è necessario che lei collabora” e “inoltrata all'autorità giudiziaria” indicano una traduzione automatica o una scrittura approssimativa, comune nei messaggi di phishing.
3. **Tono minaccioso e urgente**: L'email impone un'azione rapida (“entro 24 ore”) e minaccia conseguenze legali. Le autorità non inviano mai notifiche giudiziarie via email in questo modo.
4. **Richiesta di cliccare su un link**: Le forze dell'ordine non chiedono mai di “confermare la propria identità” tramite link non ufficiali.



5. **Link non istituzionale:** Il link contenuto nell'email porta a <http://polizia-verifica-identita.net/rapporto>, un dominio palesemente falso.
6. **Firma ingannevole:** Anche se la firma riporta "Polizia Postale e delle Comunicazioni" e un link al sito reale, l'intero contenuto è in contrasto con le modalità ufficiali di comunicazione della Polizia.
7. **ManCANZE di informazioni:** dati personali sensibili (nome, il numero dei documenti), indirizzo IP del dispositivo, nome del servizio usato illegalmente e numero di protocollo.

Questi indicatori combinati devono **insospettire** la vittima e spingerla a non cliccare, non rispondere e segnalare immediatamente il messaggio come tentativo di phishing.



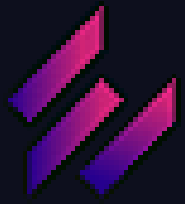
# Metodi di protezione

## 1. Formazione e Sensibilizzazione:

- Educare i dipendenti sui rischi e le tecniche di ingegneria sociale attraverso corsi di formazione regolari e aggiornamenti.
- Simulare attacchi di ingegneria sociale per testare la prontezza del personale.

## 2. Politiche e Procedure di Sicurezza:

- Implementare politiche di sicurezza rigorose per la gestione delle informazioni e l'accesso ai sistemi.
- Stabilire protocolli di verifica per le richieste di informazioni sensibili, come richiedere conferme attraverso canali separati.

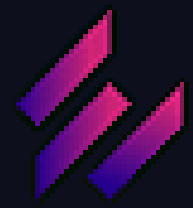


### 3. Tecnologie di Protezione:

- Utilizzare software di sicurezza per filtrare e-mail sospette e rilevare attività anomale.
- Implementare l'autenticazione a due fattori (2FA) per aggiungere un ulteriore livello di sicurezza.

### 4. Gestione degli Accessi:

- Limitare l'accesso alle informazioni sensibili solo a chi ne ha effettivamente bisogno per svolgere il proprio lavoro.
- Monitorare e registrare l'accesso ai dati critici per rilevare comportamenti sospetti.



# Conclusione

L'email analizzata rappresenta un tipico esempio di phishing ben costruito, progettato per sfruttare la fiducia nelle istituzioni e la paura di conseguenze legali. Nonostante l'apparenza iniziale credibile, essa presenta numerosi segnali d'allarme che, se riconosciuti, permettono di identificarla come fraudolenta.

Per difendersi da questo tipo di minacce, è fondamentale adottare un approccio proattivo basato su formazione continua, politiche di sicurezza aziendale, e tecnologie di protezione.

L'implementazione di strumenti può ridurre significativamente il rischio di attacchi riusciti. Solo attraverso la consapevolezza e la prevenzione è possibile contrastare efficacemente l'ingegneria sociale e proteggere dati e identità digitali.