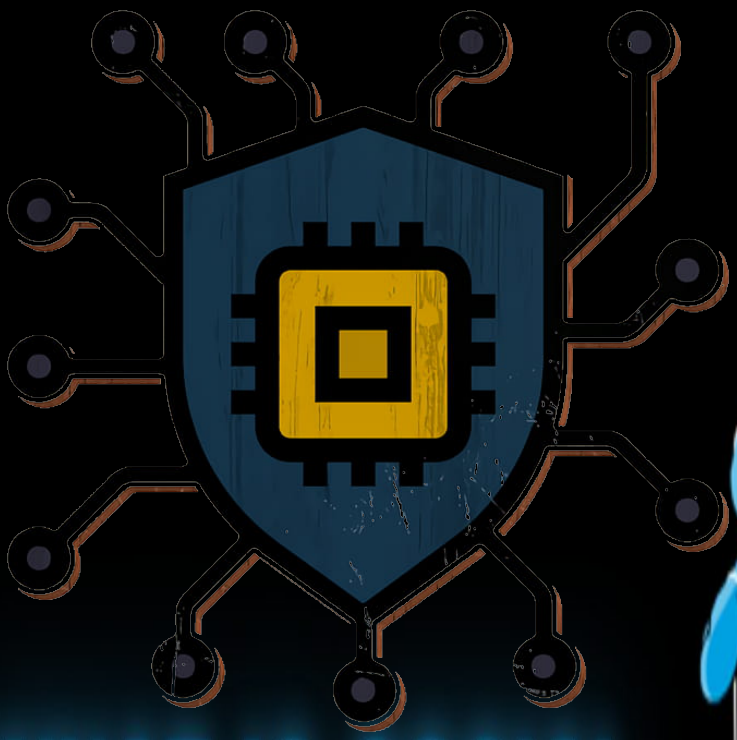
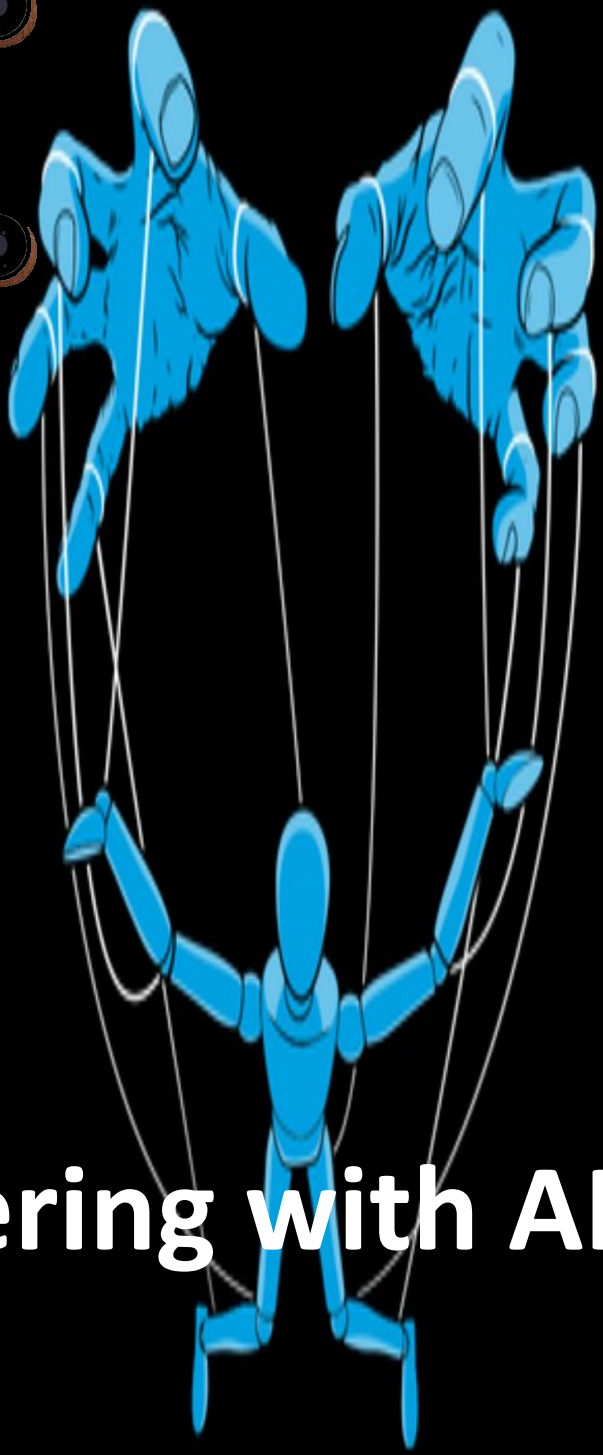


WHAT IS SOCIAL ENGINEERING



Social Engineering with AI

Cybersecurity & Ethical Hacking

Matteo Mattia

INDICE GENERALE

INTRODUZIONE

PARTE I: [OFFICIAL] Attacchi di Phishing

1. Gophish
2. SET - Social Engineering Toolkit

PARTE II: [FACOLTATIVO] ChatGPT - Analisi Email di Phishing

CONCLUSIONE

INTRODUZIONE

In questo laboratorio ho esplorato le tecniche di ingegneria sociale utilizzate dagli attaccanti per compromettere la sicurezza informatica.

Ho utilizzato strumenti professionali come **Gophish** e **SET (Social Engineering Toolkit)** per comprendere come vengono condotte le campagne di phishing e quanto sia facile ingannare gli utenti con i giusti strumenti.

PARTE I: [OFFICIAL] Attacchi di Phishing

Il phishing e una delle tecniche di attacco piu diffuse e pericolose.

Consiste nell'ingannare la vittima facendole credere di interagire con un servizio legittimo, quando in realta sta fornendo le proprie credenziali a un attaccante.

Gli elementi chiave di un attacco di phishing includono:
- Email convincenti che imitano comunicazioni ufficiali
- Landing page false che replicano siti web autentici
- Tecniche di social engineering per creare urgenza o fiducia

1. Gophish

Gophish e un framework open-source per la simulazione di campagne di phishing.

L'ho installato su Windows 10 e configurato per creare una campagna di test.

Installazione e Configurazione

Durante l'installazione ho riscontrato un errore sulla porta 80, che ho risolto modificando il file di configurazione:

```
 Directory di C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit

14/12/2025  12:29    <DIR>          .
14/12/2025  12:29    <DIR>          ..
14/12/2025  12:29               460 config.json
14/12/2025  12:29    <DIR>          db
14/12/2025  12:29           122.880 gophish.db
14/12/2025  12:29        34.590.314 gophish.exe
14/12/2025  12:29             1.115 LICENSE
14/12/2025  12:29             3.285 README.md
14/12/2025  12:29    <DIR>          static
14/12/2025  12:29    <DIR>          templates
14/12/2025  12:29                 7 VERSION
               6 File     34.718.061 byte
               5 Directory  18.541.088.768 byte disponibili

C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>cd %USERPROFILE%\Desktop\gophish-v0.12.1-windows-64bit

C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>notepad config.json

C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>gophish.exe
time="2025-12-14T12:32:02+01:00" level=warning msg="No contact address has been configured."
time="2025-12-14T12:32:02+01:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2025-12-14T12:32:02+01:00" level=info msg="Please login with the username admin and the password cbdfe2beb436f6df"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting admin server at http://127.0.0.1:3333"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting IMAP monitor manager"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting new IMAP monitor for user admin"
time="2025-12-14T12:32:02+01:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-12-14T12:32:02+01:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-12-14T12:32:02+01:00" level=fatal msg="listen tcp 0.0.0.0:80: bind: Tentativo di accesso al socket con modalità non consentite dalle rispettive autorizzazioni di accesso."

C:\Users\user\Desktop\gophish-v0.12.1-windows-64bit>
```

Ho modificato il file `config.json` per utilizzare la porta 8080 invece della 80:

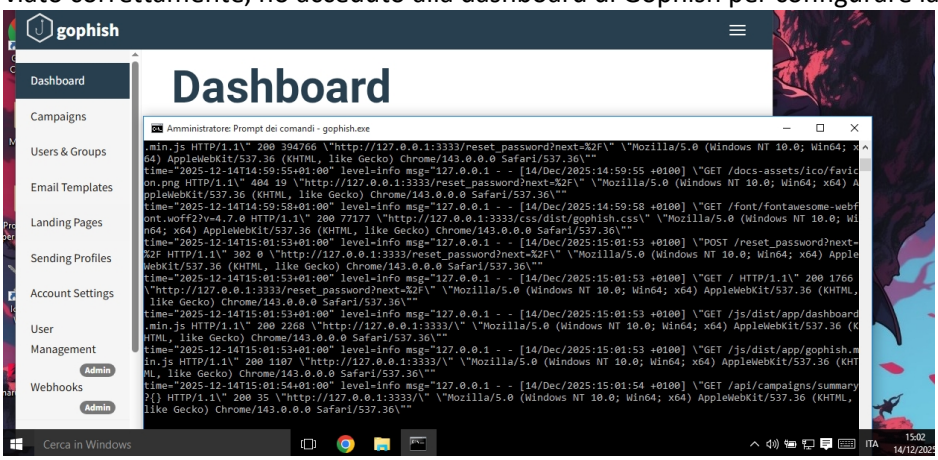
config.json - Blocco note

File Modifica Formato Visualizza ?

```
{
        "admin_server": {
                "listen_url": "127.0.0.1:3333",
                "use_tls": false,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key",
                "trusted_origins": []
        },
        "phish_server": {
                "listen_url": "0.0.0.0:8080",
                "use_tls": false,
                "cert_path": "example.crt",
                "key_path": "example.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}
```

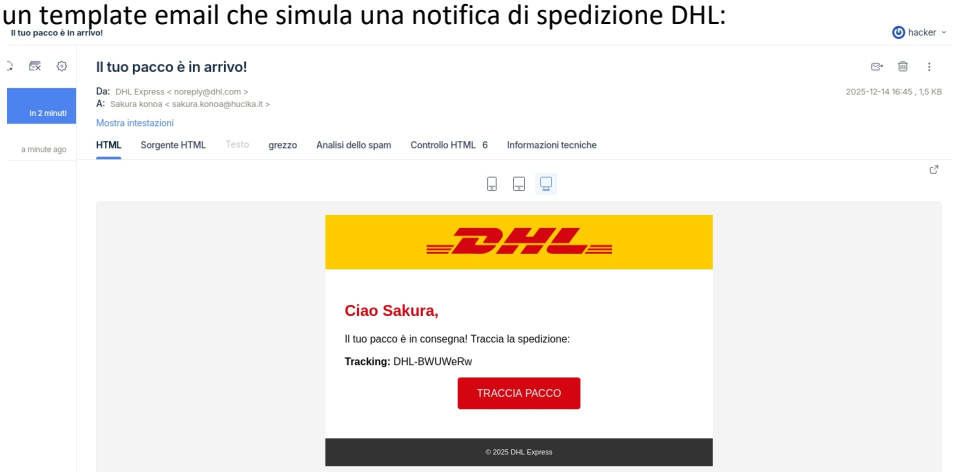
Dashboard e Creazione Campagna

Una volta avviato correttamente, ho acceduto alla dashboard di Gophish per configurare la campagna:



Email di Phishing Creata

Ho creato un template email che simula una notifica di spedizione DHL:



L'email e stata inviata con successo tramite Mailtrap e ricevuta nella inbox.

2. SET - Social Engineering Toolkit

SET e uno degli strumenti piu potenti per condurre attacchi di ingegneria sociale.

L'ho utilizzato su Kali Linux per clonare un sito web e catturare le credenziali.

Avvio di SET Ho avviato SET dal terminale di Kali Linux con il comando: `sudo setoolkit`

Passaggi di Configurazione

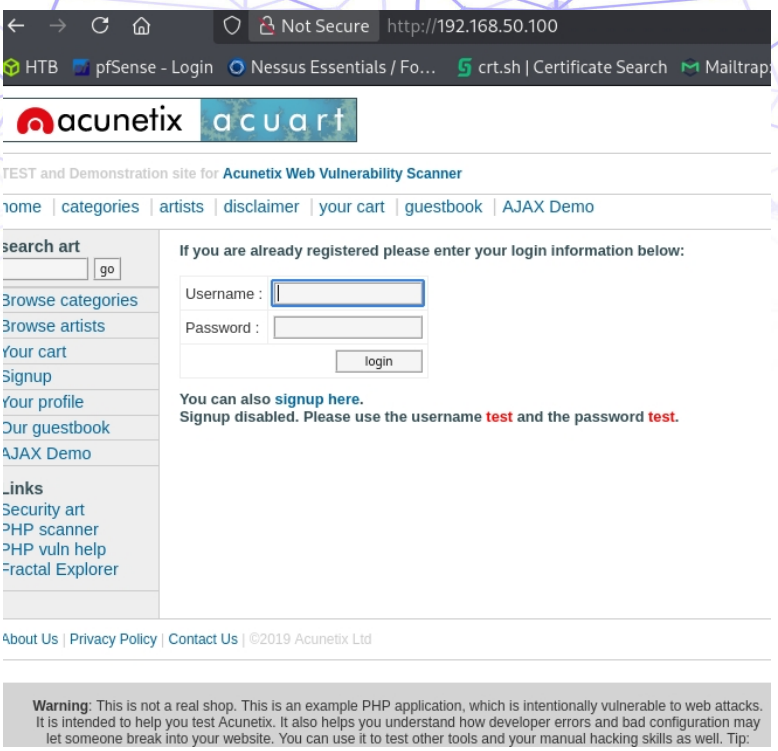
Ho seguito questi passaggi per configurare l'attacco:

1. **Menu principale** - Ho selezionato `1) Social-Engineering Attacks`
2. **Tipo di attacco** - Ho selezionato `2) Website Attack Vectors`
3. **Metodo di attacco** - Ho selezionato `3) Credential Harvester Attack Method`
4. **Modalita** - Ho selezionato `2) Site Cloner`
5. **Indirizzo IP** - Ho inserito il mio IP locale: `192.168.50.100`
6. **URL da clonare** - Ho inserito: `http://testphp.vulnweb.com/login.php`

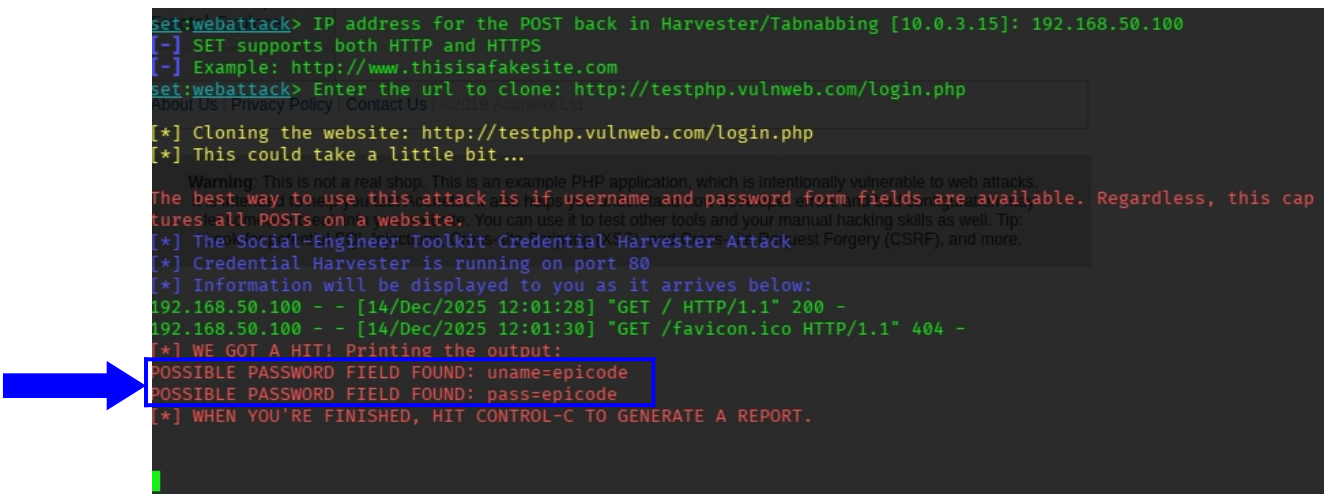
```
set> 1
set> 2
set:webattack> 3
set:webattack> 2
set:webattack> IP address for the POST back in Harvester/Tabnabbing:
192.168.50.100
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/
login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Una volta completata la configurazione, SET ha clonato il sito di test:



Quando la "vittima" ha inserito le credenziali nel sito clonato, SET le ha catturate immediatamente:



Come si puo vedere, le credenziali inserite (username: **`epicode`** , password: **`epicode`**) sono state intercettate con successo.

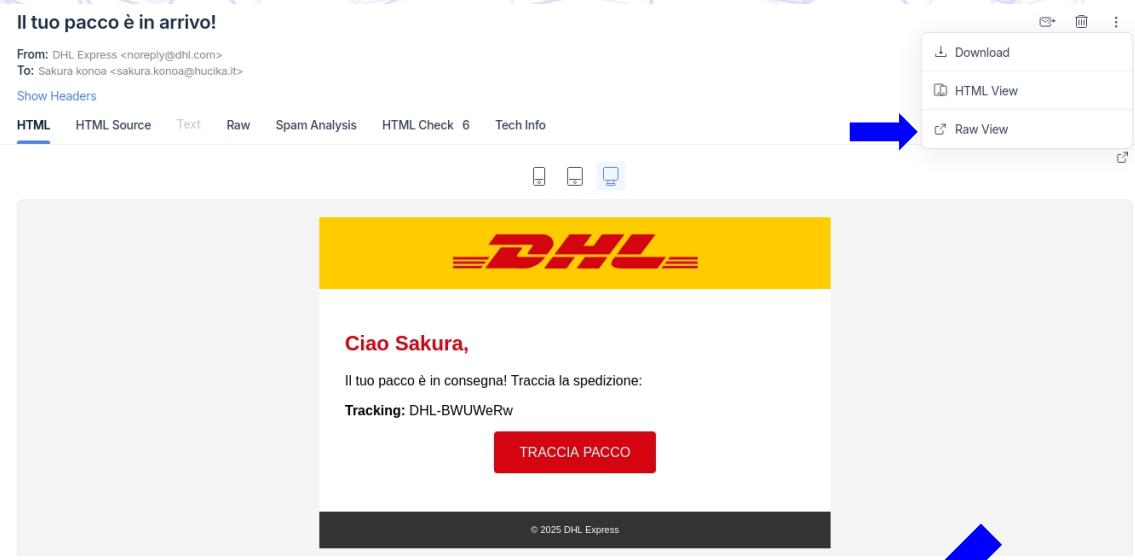
PARTE II: [FACOLTATIVO]

ChatGPT - Analisi Email di Phishing

Come richiesto dalla traccia, ho analizzato l'email di phishing utilizzando ChatGPT.

Codice Sorgente dell'Email

Ho estratto il codice sorgente raw dell'email da Mailtrap:

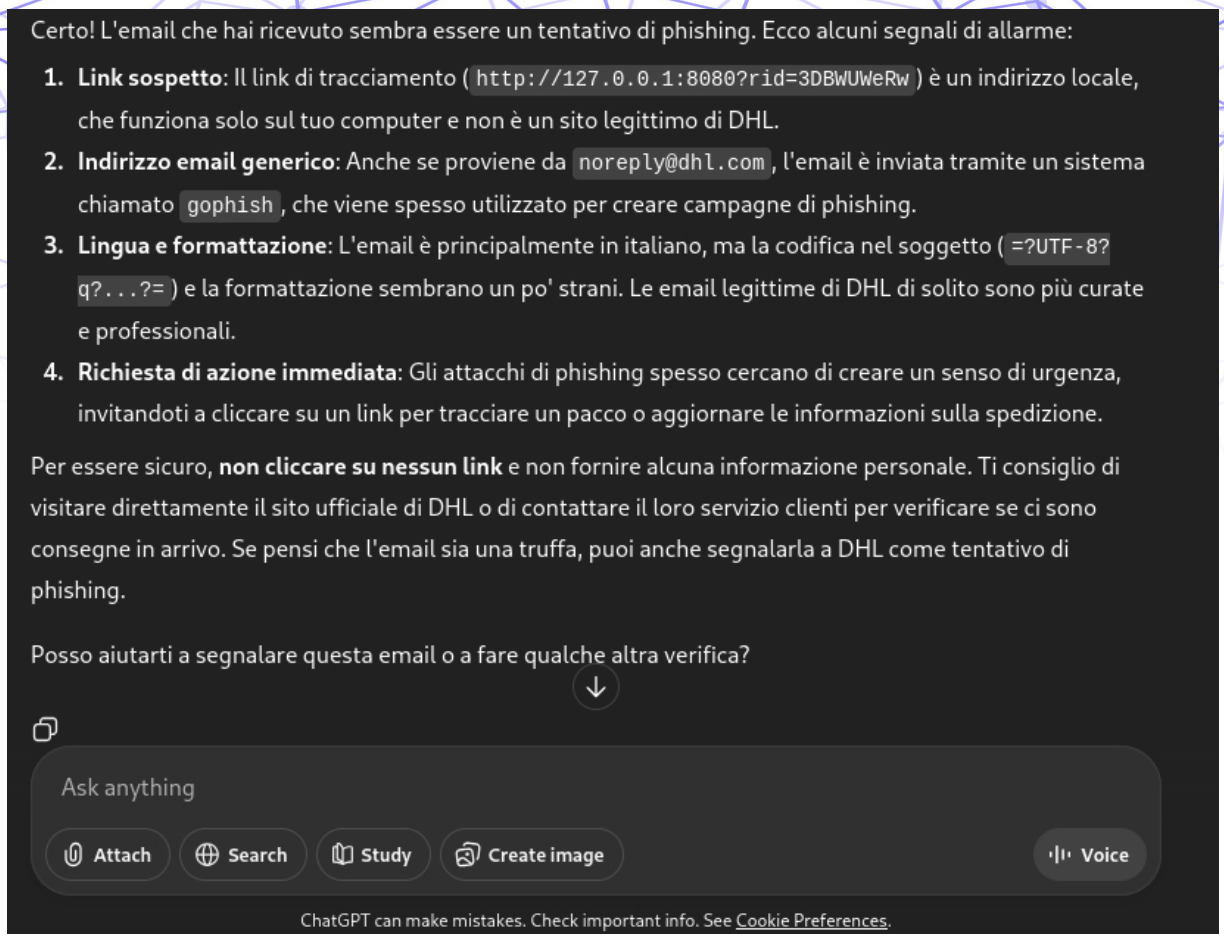



```
Mime-Version: 1.0
Date: Sun, 14 Dec 2025 17:45:56 +0100
From: "DHL Express" <noreply@dhl.com>
X-Mailer: gophish
Message-Id: <1765730755783955800.5788.18366647967735046 44@DESKTOP-9K1O4BT>
Subject: =?UTF-8?q?Il_tuo_pacco_=C3=A8_in_arrivo!?=
To: "Sakura konoa" <sakura.konoa@hucika.it>
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE html>
<html>
<body style=3D"font-family: Arial; margin: 0; padding: 0; background: #f4f4=
f4;">
    <div style=3D"max-width: 600px; margin: 20px auto; background: white;">
        <div style=3D"background: #FFCC00; padding: 20px; text-align: cente=
r;">
            <img src=3D"https://www.dhl.com/content/dam/dhl/global/core/ima=
ges/logos/dhl-logo.svg" height=3D"40">
        </div>
        <div style=3D"padding: 30px;">
            <h2 style=3D"color: #D40511;">Ciao Sakura,</h2>
            <p>Il tuo pacco =C3=A8 in consegna! Traccia la spedizione:</p>
            <p><strong>Tracking:</strong> DHL-BWUWeRw</p>
            <p style=3D"text-align: center; margin: 30px;">
                <a href=3D"http://127.0.0.1:8080?rid=3DBWUWeRw" style=3D"ba=
ckground: #D40511; color: white; padding: 15px 30px; text-decoration: none;=
 border-radius: 4px;">TRACCIA PACCO</a>
            </p>
        </div>
        <div style=3D"background: #333; color: white; padding: 15px; text-a=
lign: center; font-size: 11px;">
            =C2=A9 2025 DHL Express
        </div>
    </div>
<img alt=3D'' style=3D'display: none' src=3D'http://127.0.0.1:8080/track?ri=
d=3DBWUWeRw'/></body>
</html>
```

Analisi di ChatGPT

Ho fornito a ChatGPT l'email di phishing e questa e stata la sua risposta:



ChatGPT ha identificato correttamente i seguenti segnali di allarme:

1. **Link sospetto** - L'URL http://127.0.0.1:8080 e un indirizzo locale, non un sito DHL
2. **Indirizzo email generico** - L'uso di gophish come sistema di invio
3. **Lingua e formattazione** - Codifica UTF-8 sospetta nell'oggetto
4. **Richiesta di azione immediata** - Tipica tecnica di phishing per creare urgenza

La Mia Analisi

Analizzando gli header dell'email, ho identificato i seguenti indicatori di phishing:

Elemento	Valore	Indicatore di Rischio
X-Mailer	gophish	Tool noto per campagne phishing
From	noreply@dhl.com	Mitente falsificato (spoofing)
Message-ID	DESKTOP-9K1O4BT	Inviato da PC personale, non server aziendale
URL nel Body	Http://127.0.0.1:8080	Indirizzo locale, non sito DHL reale
Tracking pixel	Presente	Usato per tracciare apertura email

Conclusione dell'analisi

Questa email presenta tutti gli indicatori tipici di un attacco di phishing.

L'utilizzo di Gophish come X-Mailer, il Message-ID anomalo e i link che puntano a localhost sono prove evidenti della natura malevola del messaggio.

CONCLUSIONE

Questo laboratorio mi ha permesso di comprendere quanto sia semplice per un attaccante creare campagne di phishing convincenti.

Con strumenti come Gophish e SET, e possibile clonare siti web, creare email ingannevoli e catturare credenziali in pochi minuti.

La lezione piu importante e che la formazione degli utenti rimane la prima linea di difesa contro questi attacchi.

Tecnologie come SPF, DKIM e DMARC possono aiutare, ma come dimostrato, possono essere aggirate.

La consapevolezza e l'attenzione critica verso email sospette sono fondamentali per proteggersi.