

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. 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.).

Il contesto che ho pensato è una mail da parte di una banca che invita i clienti ad accedere e verificare che non vi siano state transazioni sospette nelle ultime 24 ore.

Il nostro obiettivo sarà ottenere i dati finanziari della nostra vittima.

**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).

Il prompt che ho dato a ChatGPT è il seguente:

***Sto facendo un corso di cybersecurity, potresti scrivermi una finta mail di phishing da parte di una banca finta dove invitiamo i clienti ad accedere per verificare transazioni sospette nelle ultime 24 ore con urgenza? Aggiungici anche qualche errore grammaticale come una vera mail di phishing.***

Ho ottenuto la seguente risposta:

**Oggetto:** Urgente: Verifica le tue transazioni sospette!

**Corpo del messaggio:**

Gentile Cliente,

Abbiamo rilevato delle attività sospette nel tuo conto bancario nelle ultime 24 ore. Per garantire la sicurezza del tuo conto, è necessario che tu acceda immediatamente al nostro sito per verificare queste transazioni.

Per favore, clicca sul link sottostante e segui le istruzioni per confermare la tua identità e proteggere il tuo conto:

[Verifica le tue transazioni](#)

Ricorda, è molto importante che tu agisca subito per evitare qualsiasi blocco del tuo conto o perdita di fondi. Non rispondere a questa email e non fornire informazioni personali se non tramite il link fornito.

Grazie per la tua collaborazione.

Cordiali Saluti,  
Servizio Clienti Banca Finta

*Nota: Questo è un messaggio automatico. Ti preghiamo di non rispondere a questa email.*

ChatGPT poi aggiunge:

### Errori grammaticali e stilistici inclusi:

- "Per favore, clicca sul link sottostante e segui le istruzioni per confermare la tua identità e proteggere il tuo conto" (la frase dovrebbe essere più precisa e corretta).
- "Ricorda, è molto importante che tu agisca subito per evitare qualsiasi blocco del tuo conto o perdita di fondi" (mancanza di chiarezza e fluidità).
- Uso di "Servizio Clienti Banca Finta" che non è un nome realista.

### 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.

Ho creato una campagna su GoPhish per mandare una mail tra miei due account gmail, il file mail sarà in allegato nella cartella di github.



## Details

Show  entries

Search:

| First Name | Last Name | Email                   | Position | Status     | Reported |
|------------|-----------|-------------------------|----------|------------|----------|
| ▶ Sim      | Ma        | simone94maion@gmail.com |          | Email Sent | ✕        |

Alla mail ho aggiunto l'indirizzo IP della mia macchina Kali come collegamento ipertestuale e ho usato il sito <http://testphp.vulnweb.com/login.php> per simulare il sito di login della banca:



simone.maion94@gmail.com

a me

\*\*\*

12:14 (1 minuto fa)



Gentile Cliente,

Abbiamo rilevato delle attività sospette nel tuo conto bancario nelle ultime 24 ore. Per garantire la sicurezza del tuo conto, è necessario che tu acceda immediatamente al nostro sito per verificare queste transazioni.

Per favore, clicca sul link sottostante e segui le istruzioni per confermare la tua identità e proteggere il tuo conto:

[Verifica le tue transazioni](#)

Ricorda, è molto importante che tu agisca subito per evitare qualsiasi blocco del tuo conto o perdita di fondi. Non rispondere a questa email e non fornire informazioni personali se non tramite il link fornito.

Grazie per la tua collaborazione.

Cordiali Saluti,  
Servizio Clienti Banca Finta

*Nota: Questo è un messaggio automatico. Ti preghiamo di non rispondere a questa email.*


Qui i dati dalla console di kali:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.51.102]: 192.168.51.102
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, th
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Inserendo le credenziali e dando conferma, la pagina verrà aggiornata mantenendo la stessa grafica:



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

**search art**  
   
[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)

**If you are already registered please enter your login information below:**  

Username :

Password :

E noi otterremo le credenziali inserite:

```
192.168.51.103 - - [13/Sep/2024 12:09:38] "GET /Flash/add.swf HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=mioutente
POSSIBLE PASSWORD FIELD FOUND: pass=miapassword
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

La mail di per se non contiene foto o banner di nessuna banca, ciò è uno degli elementi che potrebbe far scattare il campanello d'allarme a una persona attenta, insieme all'insistenza e alla fretta che la mail mette. Se una persona è dotata di home banking e App sullo smartphone, può tranquillamente verificare e capire che questa mail è falsa.

Se invece il ricevente è una persona meno "tecnologica" o meno attenta, leggendo che il suo account potrebbe essere bloccato o che potrebbe perdere dei fondi, potrebbe cliccare sul link e non accorgersi dell'indirizzo che è totalmente diverso da quello che normalmente vede, per poi inserire le credenziali, avere un refresh della pagina web e trovarsi la stessa landing page, questa volta veritiera. Collegandosi e non vedendo nessun movimento sospetto sul conto, potrebbe non insospettirsi e procedere normalmente nella sua giornata, mentre le sue credenziali sono state esposte.

Ovviamente, tutto ciò potrebbe essere ancora più credibile creando un indirizzo mail ad-hoc, che simuli quello di una banca di grande importanza (es: [sicurezzabancamediolanum@gmail.com](mailto:sicurezzabancamediolanum@gmail.com)), cosicché mandando a una lista di destinatari la nostra mail, vi siano più probabilità che qualcuno sia cliente della banca che stiamo usando per fare da esca, e che leggendo la prima parte dell'indirizzo caschi in trappola. Anche aggiungere delle immagini della banca al corpo della mail potrebbe aiutare in questo senso.