

ESERCIZIO W23D4

Attacchi di Phishing

Mungiovì Fabio

TASK

Adesso ci concentreremo sull'aspetto pratico dell'ingegneria sociale utilizzando diversi strumenti:

1. **Gophish**, progettato per creare email di phishing, per condurre una campagna controllata di phishing;
2. Social Engineering Toolkit (**SET**), per clonare un sito web;
3. **ChatGPT**, per aiutarci a determinare se un'email è malevola o meno (**FACOLTATIVO**)

ESECUZIONE

GOPHISH

In questa esercitazione andremo a creare una campagna di phishing, a scopo didattico, con l'utilizzo del tool Gophish per Windows.

Dopo aver scaricato il tool dal sito ufficiale e avviato, colleghiamoci all'indirizzo indicato nella schermata, per accedere alla Dashboard dello strumento.

```
D:\EPICODE\Gophish\gophish x + v
time="2025-08-03T10:54:12+02:00" level=warning msg="No contact address has been configured."
time="2025-08-03T10:54:12+02:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2025-08-03T10:54:12+02:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-08-03T10:54:12+02:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-08-03T10:54:12+02:00" level=info msg="Starting IMAP monitor manager"
time="2025-08-03T10:54:12+02:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2025-08-03T10:54:13+02:00" level=info msg="Starting new IMAP monitor for user admin"
```

gophish

admin

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User ManagementAdmin

WebhooksAdmin

User Guide

API Documentation

Dashboard

Phishing Success Overview

% of Success

100

50

0

19:29:39.048

Email Sent

Email Opened

Clicked Link

Submitted Data

Email Reported

1

0

0

0

0

Recent Campaigns

View All

Show 10 entries

Search:

Name

Created Date

Status

Galaxus

August 1st 2025, 7:29:39 pm

1

0

0

0

0

In progress

Showing 1 to 1 of 1 entries

Previous

1

Next

CREAZIONE GRUPPO

Come primo passaggio per la nostra “campagna” creiamo un gruppo *Prova* dal menu *User & Group*

In questa sezione bisogna inserire i target della campagna di phishing.

È possibile inserire file contenenti liste di email da targettizzare.

Per l'esercitazione inserirò solo il mio indirizzo email personale.

Edit Group

Name:

Prova

+ Bulk Import Users

Download CSV Template

Fabio

Mungiovi

mungiovi.fabio@gr

Position

+ Add

Show

10

entries

Search:

First Name

Last Name

Email

Position

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

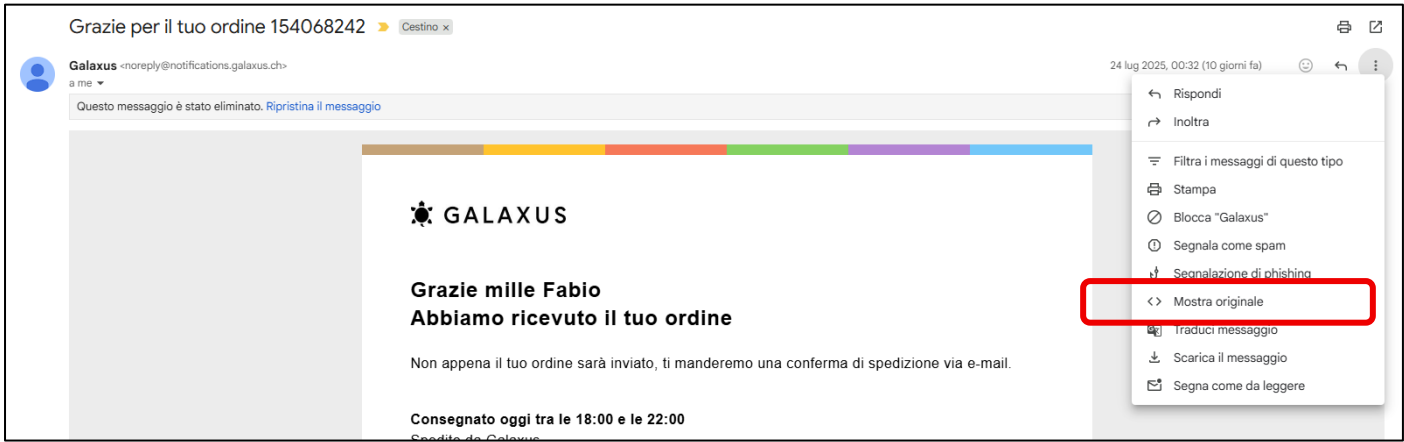
Close

Save changes

CREAZIONE TAMPLATE EMAIL

Ora andremo a creare una copia di una email autentica da utilizzare per la campagna.

Selezioniamo da Gmail una mail adatta, clicchiamo sui “3 puntini” a destra e selezioniamo *Mostra Originale*.



Copiamo quindi il codice HTML della mail cliccando su *Copia negli appunti*.

Messaggio originale

ID messaggio	<ZEHQHO7OQFqucvHAtTFPMQ@geopod-ismtpd-8>
Creato alle:	24 luglio 2025 alle ore 00:32 (consegnato dopo 1 secondo)
Da:	Galaxus <noreply@notifications.galaxus.ch>
A:	mungiovi.fabio@gmail.com
Oggetto:	Grazie per il tuo ordine 154068242
SPF:	PASS con l'IP 198.37.153.54 Ulteriori informazioni
DKIM:	'PASS' con il dominio notifications.galaxus.ch Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

[Scarica messaggio originale](#)[Copia negli appunti](#)

Delivered-To: mungiovi.fabio@gmail.com

Received: by 2002:a05:651c:b0e:b0:32c:a0eb:6b1b with SMTP id b14csp4105591jr;
Wed, 23 Jul 2025 15:32:13 -0700 (PDT)

X-Google-Smtp-Source: AGHT+IEECqspDKRIUgncxUNGZhiD/s7/J0+RHwSXSyh7vPht1wvIXNzLBbSynXJMuAXDLi9tt35E

X-Received: by 2002:a05:622a:4ac:b0:4ab:41a7:18da with SMTP id d75a77b69052e-4ae5b99f102mr144809581cf.26.1753309932912;
Wed, 23 Jul 2025 15:32:12 -0700 (PDT)

ARC-Seal: i=1; a=rsa-sha256; t=1753309932; cv=none;
d=google.com; s=arc-20240605;
b=PfSwerIA4seC0/bGDghHmPUaduJ+EU/VjyseKet4dzD47Nvz+br0G1U/7I6LK32Q/
zeVTDkGuTN533yTye/33UH70pgDSQItOhD6iyOzTsSg100dI1y/hIRqTxJvU8fUGuPnq
KFJ3608KBNLP0Cgx+qEWfd985p2NaeeJuv0AJE6wtTZYIorMdcAmyfLF0LRiTkL/D1L
gmer8y5xbF6vH5a0BneC237W40h06WbStkf2UP8E3Hmyxh/NcIjkAcguIZdVnx36PYfe
w+8fdkPN/kFge4hwM7AaeE1DIh2vQxd13PJvpmGizeUcMtW7KItw3k0cK6LH3oLi3A
4F20==

New Template

Name:

Galaxus

Import Email

Envelope Sender: ?

First Last <test@example.com>

Subject:

Grazie per il tuo ordine 154068242

Text HTML

GALAXUS

Grazie mille Fabio

Ora, su Gophish, entriamo nella sezione *Email Templates*.

A questo punto incolliamo il contenuto copiato nella sezione *Import Email*

Da questa sezione è possibile modificare il contenuto della email per adattarla agli scopi, lavorando sul codice HTML.

Una volta completate le operazioni, clicchiamo su *Salva*.

CREAZIONE LANDING PAGE

Creiamo ora la pagina a cui si vuole far entrare la vittima tramite la mail che stiamo preparando.

Andiamo nella sezione *Landing Pages*, tramite il tasto *Import Site*, incolliamo l'URL del sito che desideriamo copiare.

Import Site

URL:

https://www.post.ch/it/ricezione/monitorare-gli-invi

Cancel Import

Clicchiamo su *Import* e poi su *Salva* per terminare l'importazione.

CREAZIONE EMAIL FITTIZIA

Per l'esercizio è stata creata una email fittizia che dal nome possa trarre in inganno più facilmente il ricevente, galaxusnoreply@gmail.com.

È un passaggio facoltativo.

CREAZIONE PROFILO DI INVIO

Ora andremo a creare il profilo di invio delle email, cliccando su *Sending Profiles*

Questa è la schermata di configurazione di un profilo.

Analizziamo la **Panoramica dei Campi**

Edit Sending Profile

Name: Fabio

Interface Type: SMTP

SMTP From: galaxusnoreply@gmail.com

Host: smtp.gmail.com:465

Username: galaxusnoreply@gmail.com

Password: *****

☒ Ignore Certificate Errors

Email Headers:

X-Custom-Header {{.URL}}-gophish +Add Custom Header

Show 10 entries Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries Previous Next

Send Test Email

Cancel Save Profile

Name: Nome per l'identificazione del profilo.

Interface Type: Questo campo definisce il protocollo di invio. Generalmente, il valore predefinito è **SMTP**, che è il protocollo standard per la trasmissione della posta elettronica.

SMTP From: Qui devi inserire l'indirizzo email che apparirà come mittente per i destinatari della tua email di phishing.

Host: È l'indirizzo del server SMTP che Gophish utilizzerà per inviare le email. Va inserito nel formato indirizzo_server:porta. È univoco per ogni provider. Per esempio, `smtp.gmail.com:587` è il server di Gmail.

Username e Password: Questi sono i dati di accesso (credenziali) per autenticarsi sul server SMTP specificato in "Host". La password, per le politiche di sicurezza di Google non è quella dell'account. In seguito la spiegazione su come generarla.

Ignore Certificate Errors: Questa opzione, se selezionata, permette di ignorare eventuali errori relativi al certificato SSL/TLS del server SMTP. Va usata con cautela perché può esporre a rischi di sicurezza, ma a volte è necessaria per connettersi a server con certificati auto-firmati o non validi.

Email Headers: Qui puoi aggiungere delle intestazioni personalizzate all'email. Per esempio, `{{.URL}}-gophish` è un'intestazione speciale che Gophish utilizza per tracciare le campagne.

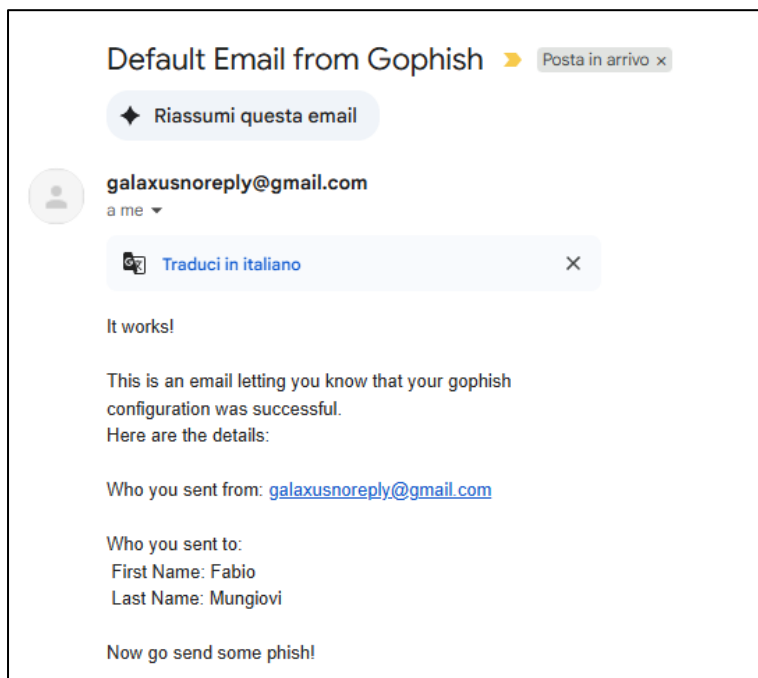
CAMPO PASSWORD

A causa delle politiche di sicurezza di Google, non è possibile utilizzare la password del proprio account principale in applicazioni di terze parti come Gophish.

Per far funzionare l'invio di email con Gophish e un account Google, devi abilitare la **verifica in due passaggi** sul tuo account e generare una **password per le app**.

Una password per le app è una password unica e di 16 cifre che viene creata appositamente da Google per consentire ad applicazioni meno sicure (o che non supportano l'accesso tramite "Accedi con Google") di accedere al tuo account. In questo modo, l'applicazione non ha accesso diretto alla tua password principale, mantenendo il tuo account più sicuro.

In sintesi, nella sezione Password di Gophish, bisogna inserire la password per le app che hai generato, e non quella che si usa per accedere al tuo account Google.



Una volta configurato il profilo, possiamo verificare la correttezza della configurazione, inviando una email di prova, cliccando su *Send Test Email*.

Nell'immagine la mail di test ricevuta all'indirizzo indicato.

AVVIO CAMPAGNA

New Campaign

Name:


Galaxus Campaign

Email Template:

Galaxus

Landing Page:


Post

URL: 

http://192.168.1.1


Launch Date

August 3rd 2025, 3:28 pm

Send Emails By (Optional) 

Sending Profile:

Fabio

 Send Test Email

Groups:

✕ Prova

Close

Launch Campaign

Possiamo ora avviare la campagna di phishing verso il nostro target.

Su Gophish clicchiamo ora nella sezione *Campaigns*

Creiamo una nuova campagna inserendo i dati richiesti.

Clicchiamo poi su *Launch Campaign* per avviarla

La vittima ora riceverà la mail che abbiamo configurato.



Social Engineering Toolkit (SET)

Ora andremo a vedere SET (Social Engineering Toolkit), uno dei programmi più usati dagli attaccanti per creare campagne di ingegneria sociale.

Daremo una dimostrazione di quanto sia facile ingannare una persona con i giusti strumenti.

1. Creazione di un Sito Fake
 - Creeremo un sito fake che sembri autentico.
2. Invio dei Link alla Vittima
 - Invieremo il link di questo sito alla vittima designata.
3. Raccolta delle Credenziali
 - La vittima, pensando che il sito sia autentico, inserirà il suo username e la sua password.
 - Noi potremo vedere le credenziali inserite.

SET è un toolkit presente di default su Kali, avviamo quindi la macchina ed il tool.

```
.M""bgd `7MM""YMM MMP""MM""YMM
,MI ""Y MM `7 P' MM `7
MMb. MM d MM
YMMNq. MMMMM MM
MM MM Y MM
Mb dM MM ,M MM
P"Ybmd" .JMMmmmmMM .JMLL.

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> █
```

Per lo scopo della nostra esercitazione ci avvaleremo del tool *Site Cloner*.

Per raggiungerlo selezioniamo in ordine le seguenti opzioni nell'interfaccia di SET:

- 1 – Social engineering attacks
- 2 – Website Attack Vectors
- 3 – Credentials Harvester Attack Method
- 2 – Site Cloner

Inseriamo, come prima cosa, l'indirizzo IP dove vogliamo che venga eseguita la copia del sito.

In questo caso inseriamo l'indirizzo della nostra macchina Kali

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.23]: 192.168.1.23 █
```

Dopodichè l'interfaccia ci chiederà di inserire l'URL del sito da clonare, utilizzeremo un sito dedicato a questi scopi scopi didattici:

<http://testphp.vulnweb.com/login.php>

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.23]: 192.168.1.23
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php
```

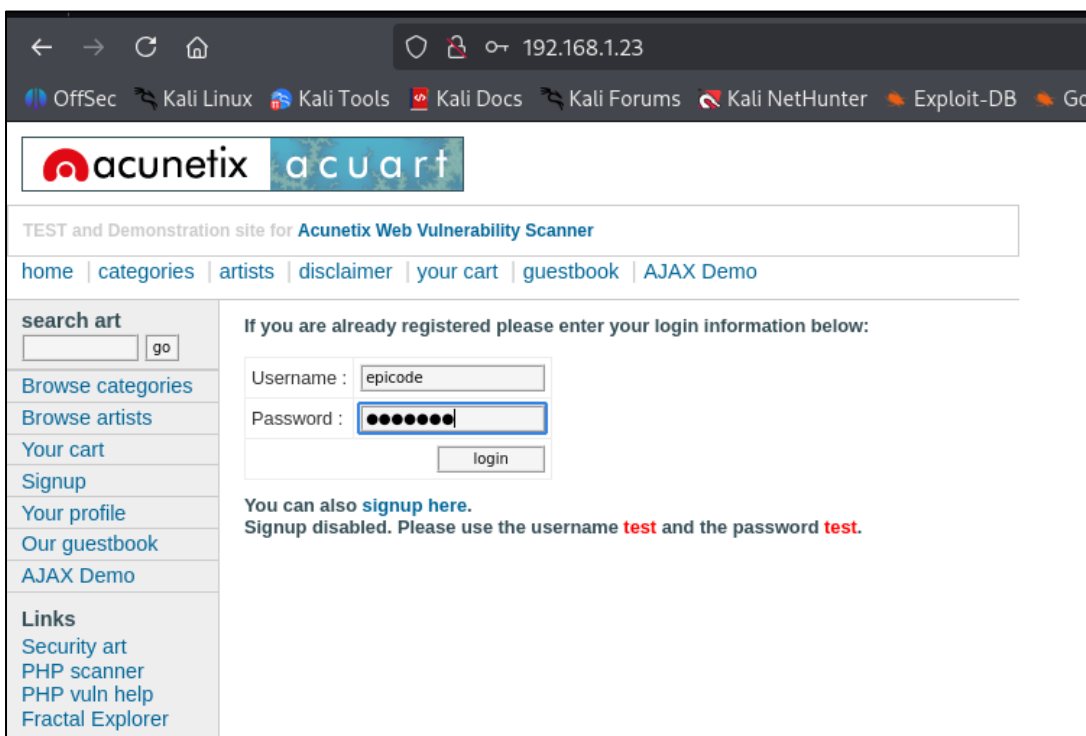
Una volta avviato riceveremo questa schermata, con il messaggio che ci ricorda che l'utilizzo ideal di questo tool è quello di intercettare le credenziali, dato che il tool caturerà tutte le richieste POST inviate al sito.

```
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, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Testiamo quindi il funzionamento, da browser colleghiamoci all'IP indicato in precedenza, per visualizzare il sito "copiato".



Inseriamo qualcosa nel campo delle credenziali, ad esempio *epicode*.

Clicchiamo su *login* per inviare la richiesta.

Tornando sulla schermata di SET ci verrà mostrato un messaggio che ci avviserà che la richiesta intercettata, con anche già identificati i campi di user e password intercettati.

```
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=epicode
POSSIBLE PASSWORD FIELD FOUND: pass=epicode
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Analizziamo, con l'ausilio di **Chat GPT**, la mail di phishing creata in precedenza con Gophish in cerca di evidenze che la identifichino come malevola.

Messaggio originale	
ID messaggio	<1754227773423060100.424.5553013304706880426@Lenovo>
Creato alle:	3 agosto 2025 alle ore 15:29 (consegnato dopo 0 secondi)
Da:	galaxusnoreply@gmail.com Tramite gophish
A:	Fabio Mungiovi <mungiovi.fabio@gmail.com>
Oggetto:	Grazie per il tuo ordine 154068242
SPF:	PASS con l'IP 209.85.220.41 Ulteriori informazioni
DKIM:	'PASS' con il dominio gmail.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni
Scarica messaggio originale	

Da un'analisi approfondita dell'email, si può confermare che si tratta di un'email malevola. L'email è un tentativo di **phishing**, una pratica ingannevole che cerca di carpire dati sensibili.

Ecco i motivi per cui l'email è da considerarsi un attacco malevolo:

- **Mittente non autentico:** L'email è stata inviata da "galaxusnoreply@gmail.com". Sebbene il nome sembri legittimo, l'indirizzo email non appartiene al dominio ufficiale di Galaxus, che è "galaxus.ch". Un'azienda seria userebbe sempre il proprio dominio per le comunicazioni ufficiali. * **Intestazioni ingannevoli:** Le intestazioni (headers) dell'email contengono informazioni che indicano come sia stata creata per ingannare i filtri antispam e gli utenti. Si nota la dicitura **"Tramite gophish"**, che è un toolkit di phishing open-source, spesso usato proprio per creare questo tipo di email fasulle.
- **Record SPF/DKIM/DMARC manipolati:** Anche se i risultati SPF, DKIM e DMARC indicano "PASS", ciò accade perché il messaggio è stato inviato correttamente da un server Gmail (209.85.220.41) per un mittente che usa anch'esso il dominio gmail.com. Questo è un trucco comune per superare i controlli di sicurezza, ma non certifica l'autenticità del mittente Galaxus. È una valida autenticazione per l'invio da Google, non per la fonte apparente del messaggio.
- **Metodo di pagamento e dettagli plausibili ma falsi:** I dati presenti nel corpo dell'email, come l'indirizzo di consegna e l'indicazione di un metodo di pagamento come "TWINT", sono generati per sembrare credibili. Questo fa parte della strategia per rendere l'email più convincente e spingere l'utente a cliccare sui link per verificare l'ordine.
- **Link malevoli:** Se si esaminano gli URL a cui puntano i collegamenti ("Vai all'ordine", "Galaxus Assistant", ecc.), si può notare che non conducono al sito ufficiale di Galaxus. Tutti i link nell'email reindirizzano a un URL che inizia con **"?rid=3DVIaw1HU"**, il quale è un parametro di tracciamento tipico delle campagne di phishing. Cliccare su questi link potrebbe portare a siti falsi progettati per rubare credenziali o installare malware.

In sintesi, la combinazione di un indirizzo email non ufficiale, la presenza di "gophish" nelle intestazioni e i link di reindirizzamento sospetti sono tutti indicatori inequivocabili di un tentativo di phishing. Si consiglia sempre di verificare l'autenticità di un'email controllando l'indirizzo del mittente e i dettagli dei link prima di intraprendere qualsiasi azione.