

W23D4 – Pratica

Epic Education Srl

Gophish

The Social-Engineer Toolkit (SET)

Analisi email phishing con l'IA

Simone Giordano

14/12/2025



Contatti:

Tel: 3280063044

Email: mynameisimone@gmail.com

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

Sommario

Gophish	3
The Social-Engineer Toolkit (SET)	6
Analisi email phishing con l'IA	7

Gophish

Ho inserito due indirizzi email come destinatari della campagna di phishing.

Edit Group

The screenshot shows the 'Edit Group' page. At the top, there's a 'Name:' field containing 'Esercizio Epicode'. Below it is a red button labeled '+ Bulk Import Users' and a link to 'Download CSV Template'. There are four input fields: 'First Name', 'Last Name', 'Email', and 'Position', followed by a red '+ Add' button. Underneath these are two search/filter controls: 'Show 10 entries' and a 'Search:' input field. A table then displays two imported users:

First Name	Last Name	Email	Position
Mario	Rosii	1983giordano@...	CEO
Simon	Giordano	mynameisimone...	CEO

At the bottom, it says 'Showing 1 to 2 of 2 entries' with navigation buttons for 'Previous', a blue '1', and 'Next'.

Ho importato il codice sorgente di un'email che ho ricevuto, in cui veniva comunicata l'avvenuta spedizione di un ordine Amazon ed era possibile monitorarne la spedizione.

Edit Template

The screenshot shows the 'Edit Template' page. It has a 'Name:' field with 'Amazon_1'. Below it is a red 'Import Email' button. The 'Envelope Sender:' field contains 'mynameisimone@gmail.com'. The 'Subject:' field has the message 'Il tuo ordine Amazon.it di "Cornice Bianca Cornice In..." è stato spedito.' Under the 'Text' tab, there's a rich text editor with the following content:

Il tuo ordine è stato inviato a:
Amazon Counter - Quiposte
Frascati

Totale ordine: EUR 14,99

Gli articoli sono stati inviati da Amazon Logistics. Il tuo numero di spedizione è: IT2767775764.

Ho importato la pagina di tracciamento delle spedizioni DHL per duplicarla e farla diventare la landing page malevola a cui si viene indirizzati.

Edit Landing Page

Name:

HTML



```
<!DOCTYPE html><html dir="ltr" lang="it-IT"><head>
<base href="https://www.dhl.com/it-it/home.html?locale=true"/><meta
charset="utf-8"/>
<title>Home page DHL - Logistica globale e spedizioni internazionali
Italia</title>
<link as="style" crossorigin="" href="/etc/clientlibs/dhl/clientlib-
all/css/bundle.38601f90d25907a1dc423fd714e290df.css" rel="preload"/>
<link as="font" crossorigin="" href="/etc/clientlibs/dhl/clientlib-
```

Capture Submitted Data ?

Capture Passwords

Ho configurato il profilo del mittente.

Edit Sending Profile

Name:

Interface Type:

SMTP From: ?

Host:

Username:

Password:

Ignore Certificate Errors ?

Email Headers:

Ho impostato la campagna.

New Campaign

Name:

Copy of Copy of Amazon2

Email Template:

Amazon_1

Landing Page:

Landing test

URL: [?](http://192.168.1.4)

192.168.1.4

Launch Date

Send Emails By (Optional) [?](#)

December 13th 2025, 11:06 pm

Sending Profile:

Esercizio Epicode

[Send Test Email](#)

Groups:

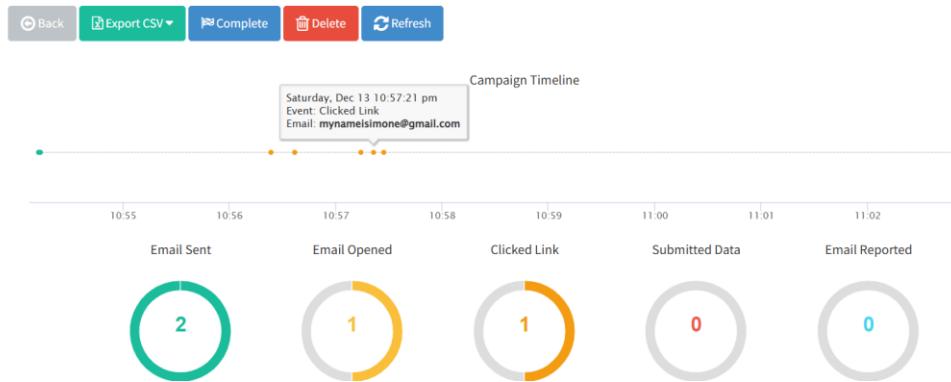
Select Group

L'email identica a quella di Amazon è stata inviata e ricevuta.

The screenshot shows an email from Amazon.it. The subject line is "Il tuo ordine Amazon.it di "Cornice Bianca Cornice In..." è stato spedito." The email is addressed to "mynameisimone@gmail.com" and was sent at 22:54 (12 minuti fa). The body of the email starts with "Ciao," and informs the recipient that their order has been shipped. It provides a link to manage orders on the Amazon website. Below this, a section titled "Conferma della spedizione" details the delivery information: arrival on "giovedì, dicembre 19" at "Amazon Counter - Quiposte Frascati". The tracking number is listed as "405-6761624-8245158". A yellow button labeled "Verifica lo stato della spedizione" is present. At the bottom, there is a small logo for "ESTANCIAS INCORNICIATE" and a link to "Cornice Bianca Cornice In Legno 29,7...".

La dashboard con i risultati mostra che l'email è stata inviata, aperta ed è stato fatto clic sul link.

Results for Copy of Amazon2



The Social-Engineer Toolkit (SET)

Una volta avviato The Social-Engineer Toolkit (SET), ho selezionato le seguenti opzioni:

- Website Attack Vectors
- Credential Harvester Attack Method
- Site Cloner
- set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 10.0.2.15 #con questo comando ho impostato l'IP della mia macchina per ospitare il sito che clonerò
- set:webattack> Enter the url to clone: <http://testphp.vulnweb.com/login.php> # con questo comando fornisco l'indirizzo del sito da clonare

Digitando il mio IP come URL del browser comparirà la pagina clonata, ora ospitata sul mio PC. Nella pagina inserisco le mie credenziali di accesso.

The screenshot shows a web browser with a green arrow pointing to the URL bar which contains "http://10.0.2.15". The page itself is a cloned version of the Acunetix Web Vulnerability Scanner login page. A green arrow points to the password input field, which contains the value "simone". The page includes a sidebar with links like "search art", "Browse categories", and "Signup". A message at the bottom says "Signup disabled. Please use the username test and the password test."

Una volta inserite le credenziali, SET le rileverà e le visualizzerà.

```

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:
10.0.2.15 - - [13/Dec/2025 17:24:40] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [13/Dec/2025 17:24:40] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output...
POSSIBLE PASSWORD FIELD FOUND: username=simone
POSSIBLE PASSWORD FIELD FOUND: pass=123456
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

```

Analisi email phishing con l'IA

Questo di seguito è il risultato dell'analisi del codice sorgente dell'email creata con gophish nel primo esercizio.

Risposta Perplexity

Il codice sorgente allegato contiene il codice sorgente di un'email di phishing che imita una conferma di spedizione Amazon.it per un ordine di "Cornice Bianca". L'indirizzo del mittente è mynameisimone@gmail.com (From e Return-Path), non autentico poiché Amazon utilizza domini verificati come @email.amazon.it o @amazon.it; l'header X-Mailer: gophish rivela l'uso di un framework phishing open-source.paste.txt

Elementi Sospetti

- **Incongruenze header:** Data futura (13 Dic 2025), SMTP Gmail con TLS ma contenuti spoofati; Message-Id legato a Gophish e hostname PCSimone.
- **Link malevoli:** Struttura href="192.168.1.4?rid=UFZpubw" (IP locale non Amazon), mascherati come amazon.it/gp/...; rischi includono furto credenziali, malware o phishing credential harvesting su server attaccante.paste.txt
- **Contenuti:** Ordine ID 405-6761624-8245158 e tracking ID 2767775764 inventati; encoding quoted-printable con caratteri UTF-8 corrotti (es. C3A8 per è).

Modelli Phishing Comuni

Formato multipart/alternative con HTML Rio (template Amazon clonato), stile professionale ma con logo/image da media-amazon.com legittimi. Corrisponde a tecniche note: spoofing brand (Amazon shipment), link IP locali (Gophish default) e payload rid= per tracciare clic/vittime.paste.txt

Pressione Psicologica

Frasi come "Il tuo ordine è andato a buon fine e non può più essere modificato" creano urgenza irreversibile; "In arrivo giovedì, 19 dicembre" e bottone "Verifica lo stato della spedizione" spingono azione immediata. Queste tattiche sfruttano FOMO (fear of missing out) e ansia perdita controllo per bypassare razionalità.paste.txt

Confronto con Email Legittime

Aspetto Email Sospetta	Email Amazon Legittima
Mittente mynameisimone@gmail.com	no-reply@email.amazon.it paste.txt
Link 192.168.1.4 (locale)	amazon.it/gp/css/... (HTTPS) paste.txt
Header X-Mailer: gophish	X-SES-CONFIGURATION-SET paste.txt
Tracking Non verificabile	Link diretto a dashboard paste.txt

Email autentiche Amazon usano SPF/DKIM, no IP locali e verifiche dirette su sito.paste.txt+1

Gestione Email Sospetta

- Non cliccare link né rispondere; elimina e svuota cancellati.
- Verifica ordini su amazon.it/login accedendo manualmente.
- Segnala a report@phishing.amazon.it o forward intero sorgente; blocca mittente.paste.txt

Scenario Formazione Phishing

Simulazione Addestramento: Immagina email "Aggiornamento Bancario Urgente" da fake@banca.it con link 192.168.1.x per "verifica conto". Domande: "Quali header controlli? Cosa fai prima di cliccare?". Risposta corretta: Analizza sorgente (no SPF, IP sospetto), accedi banca diretta. Ripeti con varianti (es. "Conto bloccato tra 24h") per insegnare urgenza tattica.paste.txt

1. <https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/137120591/c0bf1fdb-c11d-4bc1-8c7e-003f9d73e9c0/paste.txt>
2. <https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/137120591/0316b0b3-d768-4aee-a5eb-093fed896ab0/paste.txt>