

## 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.).

### 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).

### 3. Spiegare lo scenario:

- Descrivete lo scenario che avete creato.
- Spiegate perché l'email potrebbe sembrare credibile alla vittima.
- Evidenziate gli elementi della mail che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

## Creare uno scenario

Lo scenario a cui ho pensato è il seguente:

siamo in periodo pre-natalizio e la nota catena di supermercati EuroSpin vuole fare una campagna promozionale che consiste nel ricevere un buono di 50 Euro a fronte dell'acquisto di un coupon da 15 Euro.

L'utente ha solo 2 giorni per terminare l'acquisto dalla ricezione della mail (principio dell'urgenza).

Ovviamente per comprare il coupon le vittime dovranno compilare un form dove indicano numero di carta, scadenza e ccv oltre al loro nome e cognome.

Dopo aver chiesto gentile aiuto a ChatGpt con i giusti prompt per creare una mail di phishing ho ricevuto quanto segue:

**Oggetto dell'email:** 🎉 Festeggia il Natale con EuroSpin! Acquista un coupon da 15€ e ottieni 50€ in omaggio!

---

**Corpo dell'email:**

**EuroSpin Italia - Offerta Speciale di Natale** 🌲

Gentile Cliente,

In occasione del periodo natalizio, EuroSpin Italia ha deciso di ringraziarti per la tua fiducia con un'esclusiva **promozione natalizia!**

🎁 **Acquista un coupon del valore di 15€ e ricevi subito un buono da 50€!** 🎁

Siamo entusiasti di offrirti un'opportunità unica per rendere il tuo Natale ancora più speciale. Con l'acquisto di un coupon di 15€, riceverai direttamente nella tua mail un buono di 50€, utilizzabile in tutti i nostri punti vendita.

**Come funziona?**

- 1. Clicca sul pulsante qui sotto per richiedere il tuo coupon.
- 2. Compila il modulo con le informazioni richieste.
- 3. Ricevi il tuo buono e inizia a risparmiare da subito!

⚠️ **Attenzione:** Hai solo **2 giorni dalla ricezione di questa email** per richiedere il coupon! Non lasciarti sfuggire questa incredibile opportunità!

**RICHIEDI IL TUO COUPON ORA**

Ti auguriamo un felice Natale e ti ringraziamo per aver scelto EuroSpin!

Cordiali Saluti,  
**EuroSpin Italia - Servizio Clienti**

# Details

Show

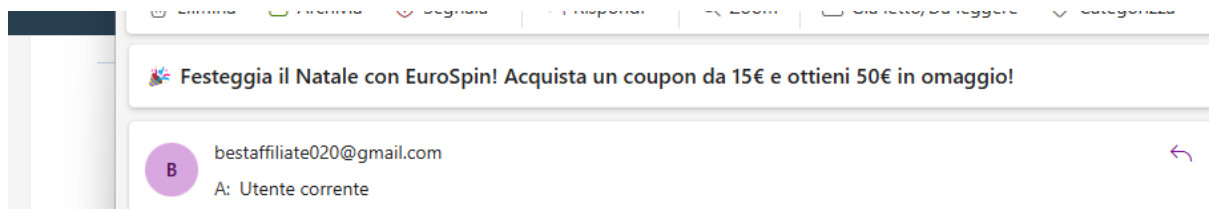
10

entries

Search

First Name	Last Name	Email	Position	Status
▶ Antonio	Bevilacqua	bigdixi@hotmail.com	Manager	Email Sent

Showing 1 to 1 of 1 entries



Abbiamo impostato Gophish per mandare una mail alla vittima con oggetto e corpo del messaggio.

Nel messaggio, dove l'utente clicca su "richiedi il tuo coupon ora" colleghiamo un link ad un link fake dal quale, grazie all'applicazione SET di KaliLinux, riusciremo a prendere i dati immessi dall'utente, in questo caso user e password.

Al posto del bottone ci potrebbe essere anche un QRCode: ovviamente dipende dalle situazioni e dal contesto; l'obiettivo è quello di mettere sempre la vittima a suo agio per indurla a fare ciò che vogliamo/vorremmo.

A screenshot of a login page for "EURO Spin". The page has a dark blue background. At the top center is the "EURO Spin" logo, which consists of a blue square with yellow stars and the text "EURO Spin" in white and yellow. Below the logo is the tagline "La Spesa intelligente". The login form includes two white input fields: "Email" with a person icon and "Password" with a lock icon. Below these fields is a yellow button labeled "ACCEDI". Underneath the button is the text "Password dimenticata?". Below that is a yellow box containing the text: "Ti sei già registrato ad altri servizi online di Eurospin? Usa le stesse credenziali per accedere, senza ripetere la registrazione." At the bottom of the form is another yellow button labeled "CREA IL TUO ACCOUNT". At the very bottom of the page, there is a language selector showing "Italiano" with a dropdown arrow.

```
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.178.51]: 192.168.178.51
[~] SET supports both HTTP and HTTPS
[~] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://eurospin.interviewweb.it/app.php?module=access&lang=it

[*] Cloning the website: https://eurospin.interviewweb.it/app.php?module=access&lang=it
[*] 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:
192.168.178.51 - - [03/Nov/2024 11:19:34] "GET / HTTP/1.1" 200 -
192.168.178.51 - - [03/Nov/2024 11:19:35] "GET /cdn-cgi/challenge-platform/scripts/jsd/main.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: FW=
PARAM: FWS=
PARAM: cid=
PARAM: FWM=
PARAM: file_id=
PARAM: ifrm=0
POSSIBLE USERNAME FIELD FOUND: login_email=bigdixi@hotmail.com
POSSIBLE USERNAME FIELD FOUND: login_password=Ciaoatuttibelliebrutti
POSSIBLE PASSWORD FIELD FOUND: login_password=Ciaoatuttibelliebrutti
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Una volta che la vittima ha fatto l'accesso, possiamo procedere al form per la richiesta dei dati della carta.

## Elementi del Phishing

In questo caso è facilmente intuibile che si tratta di phishing per i seguenti motivi:

- l'indirizzo mail da cui ci arriva la mail non è assolutamente un indirizzo ufficiale della compagnia EuroSpin;
- la pagina di accesso non è in https ed anche l'URL non risulterà quella ufficiale tipo [www.eurospin.it/login](https://www.eurospin.it/login) .....
- vige in principio di urgenza

**Gophish** ci dà la possibilità di avere traccia delle nostre campagne di phishing a 360 gradi; una volta impostato, il programma ci dirà anche quante mail sono state aperte, lette, click sul fake link ed inoltre possiamo utilizzare delle vere e proprie liste di destinatari da file .csv (se non paghi - il prodotto sei tu).

**SET** è uno strumento incluso in **Kali Linux** pensato per simulare attacchi di social engineering, come phishing, spear phishing e attacchi basati su malware. È particolarmente utile per realizzare campagne di phishing "custom" e specifiche per i test di sicurezza.

Ho chiesto, inoltre, consiglio a Chatgpt per stilare la relazione e oltre a spiegarmi nel dettaglio ciò che già ho fatto in precedenza ha aggiunto anche una conclusione:

## Conclusione

L'uso di strumenti come **SET** e **Gophish** può aiutare i professionisti della cybersecurity a simulare scenari realistici di attacco, testare la resilienza dell'organizzazione e migliorare la consapevolezza dei dipendenti riguardo ai rischi del phishing. Tali simulazioni evidenziano che l'anello debole della sicurezza è spesso l'essere umano; di conseguenza, una formazione continua e l'adozione di politiche di sicurezza forti sono essenziali per difendere efficacemente l'azienda dagli attacchi di social engineering.

Concludo personalmente affermando che, al giorno d'oggi, è sempre bene restare con gli "occhi aperti" sempre e dovunque.

Come per tutte le cose l'anello debole resta l'essere umano con i suoi bisogni (in questo caso quello di risparmiare qualche euro) e le sue necessità (quello, a prescindere, di fare la spesa) e rimane pertanto la parte più facilmente vulnerabile all'interno della Cyber Security.

Un bravo Cyber Security Specialist deve focalizzarsi sia sul lato hardware e software che su quello dell'essere umano e quindi è sempre consigliata la formazione dei dipendenti (e direi anche consapevolezza) delle aziende presso cui siamo chiamati per i nostri servizi.

Sono dell'idea che a livello hardware/software una porta può essere chiusa - aperta - modificato il numero - fare aggiornamenti frequenti - comprare il miglior firewall al mondo, ma riuscire a gestire un essere umano (che ha dei sentimenti e degli stati d'animo) sia la cosa più difficile e quindi più semplice a cui un hacker cercherà di fare breccia.

Grazie,  
**Antonio Bevilacqua**