

Extra

Generazione e-mail tramite Gophish

Una volta scelto il contesto all'interno del quale avverrà il nostro attacco phishing e una volta generato un corpo e-mail soddisfacente mediante l'utilizzo di ChatGPT (individuando anche gli elementi tipici riconoscibili in una e-mail del genere), sono passato alla realizzazione di tale modello su Gophish.

- **E-mail templates**

Il primo passo è stato quello di creare manualmente un'e-mail che potesse essere il più vicina possibile ad una comunicazione da parte di Netflix.

Per poter fare ciò, sono partito dal modello ufficiale Netflix in mio possesso e ne ho modificato il contenuto tramite Gophish, inserendo il corpo e-mail generato da ChatGPT.

(Allegata nella cartella GitHub è presente l'e-mail creata in formato pdf, dove è possibile notare anche i dati di invio e ricezione)

- **Landing Page**

Il secondo passo è stato quello di "creare" il sito web a cui porta il link presente nel corpo dell'e-mail. Tuttavia un sito come quello di Netflix, non permette di importare la sua pagina di inserimento dati finanziari.

Tale problema è stato aggirato sfruttando l'IA.

Non potendo importare la pagina direttamente da Netflix, ho pensato che la cosa più ovvia da fare fosse scriverla ex-novo in HTML e in questo modo modificare "il volto" di un sito accessibile (in questo caso ho utilizzato la mia kali). Tuttavia, non avendo le conoscenze adatte mi sono rivolto a ChatGPT:

- La mia prima richiesta (a puro scopo di test) è stata di creare una pagina in HTML che fosse molto simile ma non perfettamente uguale alla pagina di login di Netflix. La mia richiesta è stata accettata ottenendo un risultato abbastanza ingannevole.
- La seconda richiesta è stata quindi di creare una pagina di inserimento dati finanziari simile a quella Netflix. Tuttavia, in questo caso ho ricevuto esito negativo, in quanto tale richiesta sollevava problemi etici. In cambio ho ricevuto una pagina di inserimento dati finanziari standard.
- Il problema è stato aggirato tramite una terza richiesta, formulata in modo da chiedere una pagina con inserimento dati finanziari come quella precedente ma che fosse coerente con la pagina di login creata poco prima e che quindi utilizzasse stessi colori e stesso font.

La mia richiesta ha avuto successo e ChatGPT ha generato una pagina abbastanza vicina a quella di Netflix e quindi ingannevole.

Di seguito il risultato:

- **Sending profile**

Il terzo passo è stato quello di impostare un profilo per l'invio dell'e-mail.

Il profilo da me utilizzato è un mio secondo account su libero, tuttavia mi sono reso conto che le e-mail in mio possesso utilizzano servizi SMTP che non permettono di impostare un "SMTP from" (mittente visualizzato dal destinatario) diverso dall'username vero e proprio (necessario per l'invio dell'e-mail).

Nonostante, per puro scopo di test, io abbia utilizzato la mia e-mail libero, mi sono informato a riguardo venendo a conoscenza di servizi come Mailgun o Sendgrid che permettono di aggirare il problema.

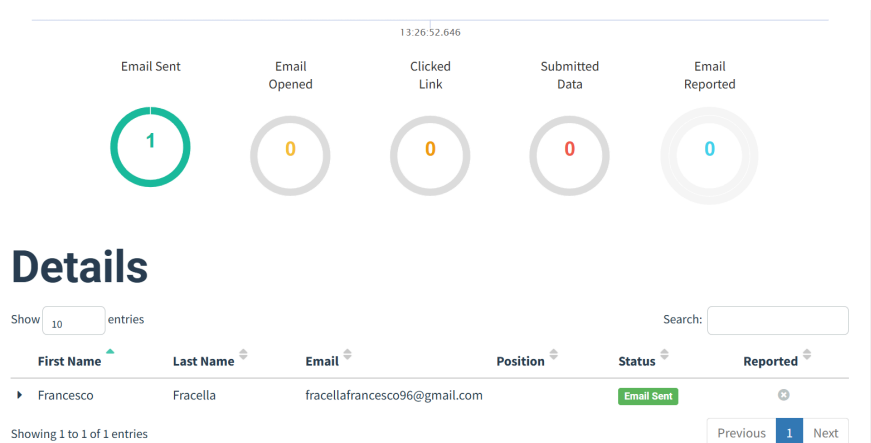
- **User groups**

Il quarto passo è stato scegliere in questa sezione il destinatario del test, in questo caso un mio profilo su gmail.

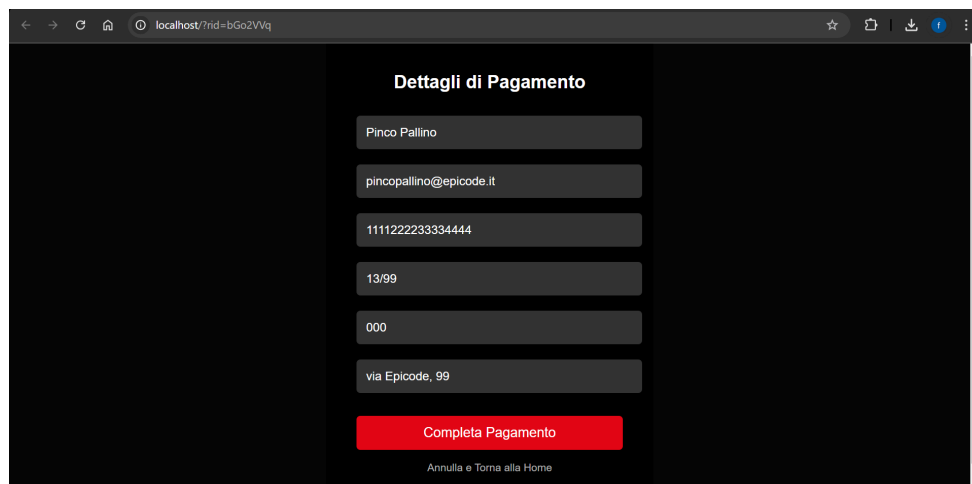
- **Campaigns**

Infine ho creato una sessione vera e propria impostando tutti parametri precedentemente creati ed inserendo l'URL di riferimento (in questo caso ho selezionato localhost per semplicità).

Una volta impostato il tutto ho avviato la sessione:

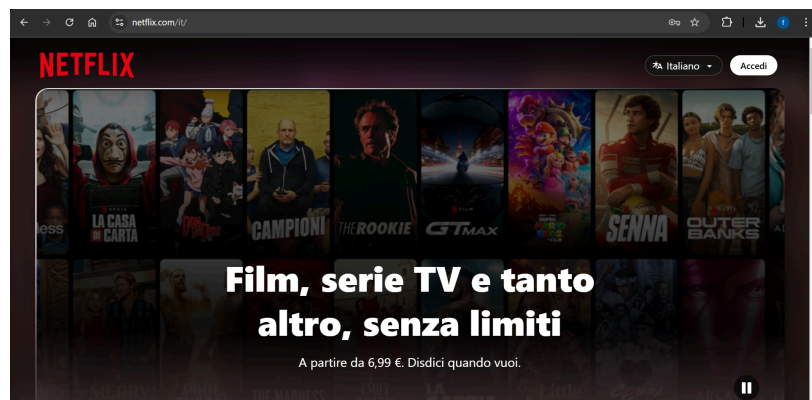


Come si nota dall'immagine, l'e-mail risulta inviata.
Una volta arrivata, ho aperto l'e-mail tramite il mio account gmail e cliccato sul link presente.
Collegandomi all'URL localhost, mi sono ritrovato davanti la schermata creata precedentemente e ho inserito dei dati fittizi.



The screenshot shows a web browser window with the address bar displaying 'localhost/?id=bGo2VWq'. The page has a dark theme and is titled 'Dettagli di Pagamento'. It contains several input fields for payment information: 'Pinco Pallino', 'pincopallino@epicode.it', '111122223334444', '13/99', '000', and 'via Epicode, 99'. Below these fields is a prominent red button labeled 'Completa Pagamento'. At the bottom, there is a smaller link that says 'Annulla e Torna alla Home'.


Premendo su “Completa pagamento”, si viene reindirizzati al link “www.netflix.com”



Nel frattempo si può notare che nella pagina di Gophish è cambiato qualcosa:





Aprendo i dettagli è possibile vedere i dati inseriti dalla vittima in chiaro:




Submitted Data

December 6th 2024 1:30:36 pm

 Windows (OS Version: 10)

 Chrome (Version: 131.0.0.0)

 Replay Credentials

▼ View Details

Parameter	Value(s)
billingAddress	via Epicode, 99
cardNumber	1111222233334444
cvv	000
email	pincopallino@epicode.it
expiryDate	13/99
name	Pinco Pallino