
S5-L5

Ingegneria sociale

Emanuele Benedetti | 10 gennaio 2025

Consegna

Obiettivo

Creare una simulazione di un'email di phishing utilizzando Chat GPT.

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.

Svolgimento

Scenario 1

Per svolgere la consegna, ho inizialmente creato un esempio di mail di phishing molto semplice da riconoscere. In particolare ho immaginato che un utente malevolo avesse l'obiettivo di rubare le credenziali degli account Amazon, sfruttando la disattenzione del malcapitato ricevente. Anche se in un primo momento un attacco di questo genere può risultare poco pericoloso, in realtà l'account amazon contiene molte informazioni (nome e cognome, indirizzi, ricerche ed interessi personali) ma soprattutto le carte di pagamento salvate nel sito.

Un semplice attacco di questo tipo può quindi generare un'ingente perdita di informazioni e di denaro!

Un attacco di phishing rientra nella categoria di attacchi di ingegneria sociale, ovvero una serie di tecniche utilizzate da malintenzionati per manipolare o influenzare le persone, con l'obiettivo di ottenere informazioni riservate, accesso a sistemi protetti o compiere altre azioni dannose.

L'ingegneria sociale sfrutta la psicologia umana per indurre le persone a fare qualcosa che non avrebbero intenzione di fare.

L'attaccante, in questo caso, sfrutta il fatto che amazon sia un servizio noto e dunque, distrattamente, si è portati a fidarsi delle informazioni contenute nella mail

Creazione email di phishing

NOTA BENE: *Gli attacchi di phishing mostrati sono effettuati in un ambiente di lavoro sicuro ed isolato, senza alcun interesse di danneggiare persone o cose. Si declina qualsiasi responsabilità di azioni illegali a seguito di emulazione di quanto mostrato nel report!*

Ho creato la mail malevola tramite **GoPhish**, una piattaforma open-source utilizzata per condurre campagne di phishing simulato. Il programma ha molte funzionalità ma in questo primo scenario ho sperimentato la funzionalità di creazione delle mail in plaintext, senza creare elaborate pagine HTML per facilitare la comprensione dell'attacco di phishing.

Il primo passaggio per la creazione della mail tramite GoPhish è stato creare la lista di indirizzi email target della campagna di phishing. Tramite la sezione *Users & Group* ho creato un nuovo gruppo aggiungendo il mio indirizzo email, che userò come ricevente delle campagne in tutti gli esempi.

Edit Group ×

Name:

Amazon phisng

[+ Bulk Import Users](#) [Download CSV Template](#)

First Name Last Name Email Position [+ Add](#)

Show entries Search:

First Name	Last Name	Email	Position
Emanuele	Benedetti	emanuelebene...	✕

Showing 1 to 1 of 1 entries [Previous](#) [1](#) [Next](#)

[Close](#) [Save changes](#)

Successivamente mi sono spostato nella sezione *Email Templates* ed ho creato il template ovvero il contenuto del messaggio. Ho inserito il nome del template, il nome del mittente, l'oggetto della mail.

Come da consegna, per il contenuto ho chiesto a ChatGPT di generare il testo della mail e dopo aver modificato e personalizzato il testo l'ho aggiunto al template.

x

Semplice

 Import Email

Amazon

Congratulazioni! Ecco un buono regalo per te!

HTML

Siamo lieti di comunicarti che sei il vincitore di un premio speciale di 50\$! 🎉

Grazie alla tua fedeltà hai guadagnato un buono regalo da utilizzare su una selezione di prodotti o servizi esclusivi*. Non vediamo l'ora che tu possa approfittare di questa occasione!

Per riscuotere il tuo premio, ti invitiamo a cliccare sul link qui sotto e seguire le semplici istruzioni:

[www.amazon.com](#)

Dopo aver impostato lo stile e le informazioni della mail ho configurato il programma con l'account utilizzato per l'invio delle email appena create.

×

Phishing

SMTP

promozioni@gmail.com

smtp.gmail.com

vanninugirgio@gmail.com

●●●●●●●●●●●●●●●●●●●●

☒ Ignore Certificate Errors ?

In questo momento tutto è impostato correttamente, dunque mi sono spostato nella sezione *Campaigns* per creare una nuova campagna di phishing, scegliendo dai menù a tendina del programma, le impostazioni appena configurate di mittente, riceventi e template dell'email.

New Campaign ×

Name:

Email Template:

Semplice

Landing Page:

Select a Landing Page

URL: ?

Launch Date

Send Emails By (Optional) ?

Sending Profile:

Phishing

✉ Send Test Email

Groups:

✖ Target telepass

Close ➦ Launch Campaign

Spiegazione ed analisi scenario 1

Passiamo ora all'analisi della mail ricevuta e ai consigli su come individuare i segnali di un attacco di phishing. L'immagine qui sotto, mostra l'email ricevuta.



Prima di analizzare il contenuto è bene notare che il client di posta (in questo caso Gmail) non è stato in grado di rilevarla come una mail di spam, ciò sta a significare che il programma utilizzato ha superato i controlli di sicurezza. Analizzando l'header del messaggio si può notare che i controlli SPF, DKIM e DMARC vengano superati senza alcun problema.

```
ARC-Authentication-Results: i=1; mx.google.com;  
  dkim=pass header.i=@gmail.com header.s=20230601 header.b=DMoDfzd+;  
  spf=pass (google.com: domain of vanninugirgio@gmail.com designates 209.85.220.65 as permitted sender)  
smtp.mailfrom=vanninugirgio@gmail.com;  
  dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com;  
  dara=pass header.i=@gmail.com
```

Ciò testimonia che bisogna sempre porre attenzione alle email che riceviamo e non possiamo fidarci dei filtri antispam e dei controlli integrati nei client di posta.

Dopo le prime considerazioni passiamo ora all'analisi del contenuto della mail.

Ci sono molti indicatori del fatto che la mail sia malevola:

1. Ciò che dovrebbe farci sin da subito dubitare è l'indirizzo email mostrato accanto al nome Amazon del mittente. Un'azienda leader come Amazon utilizza email professionali, mentre nel nostro caso troviamo un indirizzo non ben specificato di gmail
2. Nel testo sono presenti diversi errori lessicali e grammaticali, spesso frutto di una traduzione automatica errata ("buono regali", "la offerta" ecc.).
3. Nonostante il sito italiano di amazon utilizzi l'euro come valuta, riceviamo un buono in dollari senza alcun apparente motivo
4. Il punto più pericoloso della mail tuttavia è il link che siamo spronati a cliccare per ricevere il fantomatico premio. Anche se richiede maggiore attenzione, è facilmente riscontrabile che il link inserito sia www.amzzon.com e non il vero www.amazon.com (z al posto della a).

In questa tipologia di attacco possiamo aspettarci che l'attaccante abbia realizzato una copia simile del sito reale di Amazon, raggiungibile cliccando il link, per indurci a inserire nome utente e password che verrebbero mostrati al malintenzionato.

Nonostante possa sembrare difficile cadere in questo tipo di truffe, ci sono comunque delle caratteristiche della mail che ci spingono a cliccare sul link e inserire le informazioni per ricevere il buono regalo:

1. Il nome del mittente è Amazon, azienda che tutti conoscono e che spesso invia email di offerte o prodotti interessanti. E' proprio sul nostro interesse per il mittente e sul regalo che si basa l'attacco di phishing! Tuttavia come abbiamo visto il nome è stato astutamente modificato dal mittente malevolo.
2. Il mittente ha aggiunto il logo amazon per rendere l'email più verosimile
3. L'oggetto della mail cattura la nostra attenzione e fa leva sulla "bella notizia" ricevuta per farci subito aprire la mail senza notare i dettagli
4. Il testo della mail è semplice e sfrutta tecniche di manipolazione psicologica per compromettere la nostra capacità di analisi. Si esorta infatti a "non perdere tempo" poiché l'offerta "è valida fino a domani".

In questo caso è importante non cliccare sul link falsificato e non fornire alcuna credenziale di accesso. Qualora si volesse verificare la presenza di premi in palio è sempre meglio recarsi sul sito ufficiale tramite browser WEB senza cliccare sul link. E' importante tenere a mente che durante gli attacchi di social engineering ci sono spesso caratteristiche ricorrenti, in questo caso ad esempio troviamo: l'urgenza o la necessità di agire rapidamente (offerta limitata), sfruttamento della fiducia che le persone hanno verso gli altri (come aziende conosciute, colleghi di lavoro o amici) per ingannare le vittime, i messaggi sono spesso semplici, chiari e diretti, evitando tecnicismi che potrebbero far scattare sospetti. Riconoscere questi segnali può aiutarci a difenderci dagli attacchi di phishing!

Gli strumenti di intelligenza artificiale come ChatGPT possono aiutarci non solo a generare il testo della mail come simulato in precedenza, ma anche nell'analisi delle mail ricevute. Ho chiesto infatti a ChatGPT di analizzare l'email ed è riuscita ad indicarmi correttamente quali sono le criticità (già elencate) dell'email:

Questa email è un chiaro tentativo di phishing. Ecco i segnali principali:

- Mittente non ufficiale.
- Utilizzo di un dominio simile ma falso.
- Errori grammaticali e stilistici.
- Strumenti come "gophish" nel processo di invio.

Bisogna tenere a mente tuttavia che non sempre le analisi dei software di intelligenza artificiale sono da considerarsi complete o attendibili e pertanto la conoscenza degli attacchi e la revisione umana è fondamentale.

Scenario 2

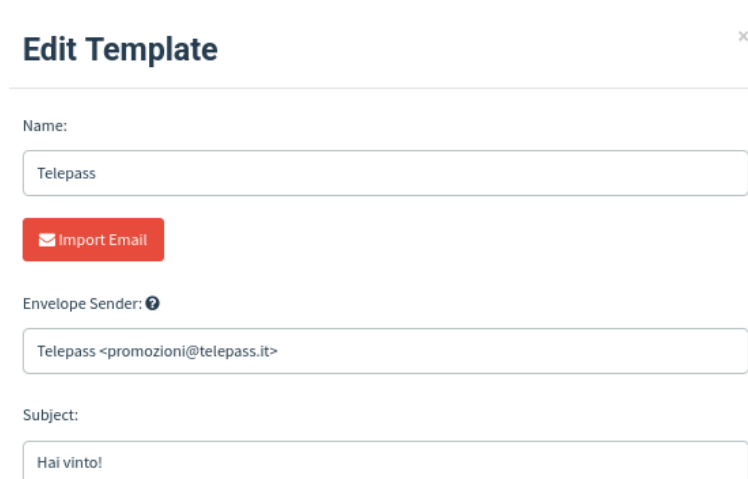
Il secondo scenario che ho ipotizzato è molto simile al precedente ma le caratteristiche della mail fanno sì che l'attacco richieda maggiore attenzione per essere riconosciuto. In questo caso l'attaccante ha creato una mail e un sito che assomigliano a quelli della società Telepass ma sono fraudolenti e tentano di rubare le credenziali di accesso agli account. Ho deciso di creare questo ulteriore esempio per mostrare che gran parte degli attacchi di phishing presentano caratteristiche comuni.

Creazione email di phishing

Anche in questo caso mi sono servito del tool GoPhish ma stavolta ho creato un codice HTML che viene renderizzato all'apertura della mail. In questo modo quando apriamo la mail non vedremo solamente un semplice testo con link (che dovrebbe farci insospettire) ma una pagina più strutturata che ricorda quella della società.

Ho eseguito gli stessi passaggi dell'esempio precedente, tuttavia, come mostra l'immagine, anziché inserire del testo in plaintext ho usato la versione HTML con il codice da me creato in precedenza e modificato oggetto e mittente della mail.


E' bene specificare che l'obiettivo non era effettuare una copia 1:1 del sito ma rendere la mail più credibile ad una lettura superficiale.




Edit Template ✕

Name:

Telepass

 Import Email

Envelope Sender: 

Telepass <promozioni@telepass.it>

Subject:

Hai vinto!

Ho dunque avviato una nuova campagna di phishing con le nuove impostazioni appena create.

Nota: tutte le mail create sono solamente a scopo didattico e indirizzate ad account sicuri e privati. Non emulare quanto mostrato nel report.

New Campaign ×

Name:

Email Template:

Landing Page:

URL: ?

Launch Date Send Emails By (Optional) ?

Sending Profile:
 Send Test Email

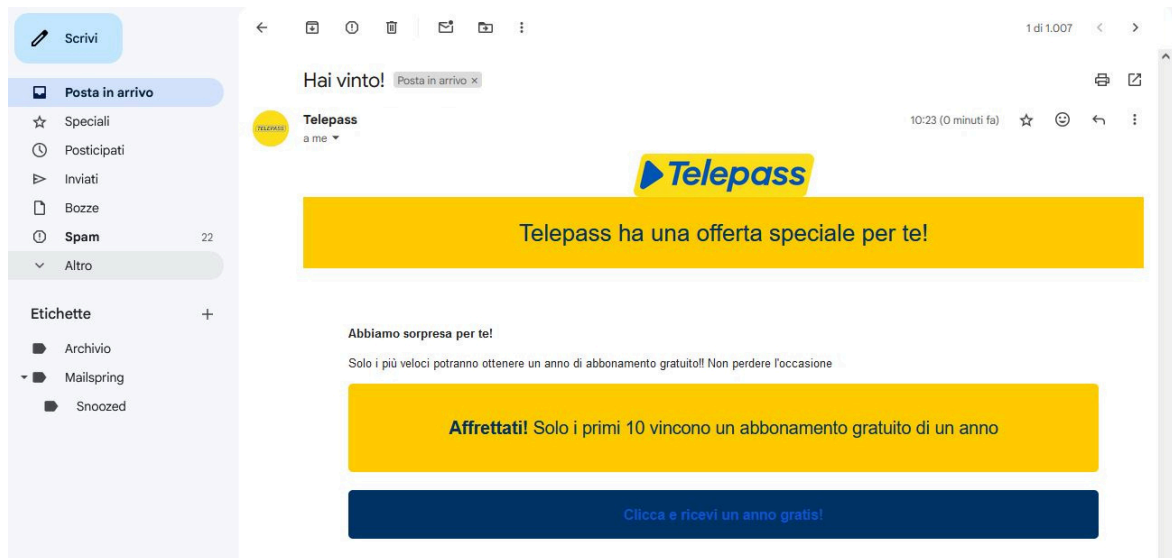
Groups:

Close Launch Campaign

Spiegazione ed analisi scenario 2

Come detto in precedenza, questo scenario non differisce molto dal precedente dunque mi limiterò ad evidenziare solo alcuni aspetti, sottolineando le caratteristiche comuni e come possiamo individuare i segnali di email non legittima.

Anche questa volta il programma è riuscito a superare i controlli di verifica del client, che non segnala alcun tipo di problematica nella mail ricevuta.



In questo caso l'attaccante è riuscito a camuffare meglio l'estetica della mail facendola somigliare ad una mail della società Telepass.

Ci sono diversi aspetti che possono indurci a credere che la mail sia legittima:

1. Nome Telepass mostrato dal client come mittente del messaggio
2. Logo Telepass correttamente visualizzato accanto al nome del mittente
3. Logo Telepass contenuto nel testo della mail
4. Il messaggio replica i colori dell'azienda facendo sembrare la mail più veritiera

Tuttavia anche qui sono presenti gli indicatori che dovrebbero far scattare un campanello d'allarme elencati precedentemente:

- Oggetto della mail gratificante che ci annuncia una fantomatica vittoria
- Il messaggio sfrutta la fiducia che abbiamo verso un brand noto per abbassare le nostre difese
- Nel testo viene evidenziato che l'offerta è riservata solo ai primi 10 clienti che cliccano il link (che stavolta è mascherato per renderne più difficile l'analisi)
- Il testo contiene piccoli errori, anche se più difficilmente individuabili rispetto al primo scenario

Un ulteriore indizio che possiamo notare è che in nessuno dei due casi vi sono informazioni personali specifiche sul ricevente, questo indica che la mail

probabilmente non era indirizzata solamente a noi, ma faceva parte di un attacco phishing su larga scala.

Anche in questo caso, tramite l'analisi di un software di intelligenza artificiale è possibile capire che si tratta di un tentativo di phishing. Questo il risultato di Microsoft Copilot:

Analisi phishing

- **Indirizzo email sospetto:** Anche se sembra provenire da Telepass, l'indirizzo è vanninugirgio@gmail.com, che non è un indirizzo ufficiale di Telepass.
- **X-Mailer:** L'email è stata inviata tramite "gophish", un noto strumento di phishing.
- **Link sospetto:** L'email contiene un link a "<https://www.tuosito.com/offerta>", che non è il dominio ufficiale di Telepass.

Conclusione: Questa email sembra essere un tentativo di phishing. Consiglio di non cliccare su nessun link e di segnalare l'email come spam o phishing.

Ancora una volta ci tengo a sottolineare che qualora l'attaccante riuscisse a recuperare le credenziali grazie alla disattenzione del malcapitato ricevente, gli account personali contengono molte delle nostre informazioni (nomi, indirizzi, carte di pagamento, contratti ecc.) che possono anche essere sfruttati per effettuare ulteriori attacchi mirati. Impostare password complesse in questo caso non impedisce l'attacco, è sempre importante prestare massima attenzione ed abilitare l'autenticazione a due fattori (2FA) o l'autenticazione a più fattori (MFA).

Saper riconoscere un attacco di phishing è una misura preventiva indispensabile per proteggere la propria sicurezza e quella degli altri. La conoscenza dei segnali di phishing e la capacità di saper agire correttamente sono strumenti potenti per evitare danni a livello personale e aziendale.

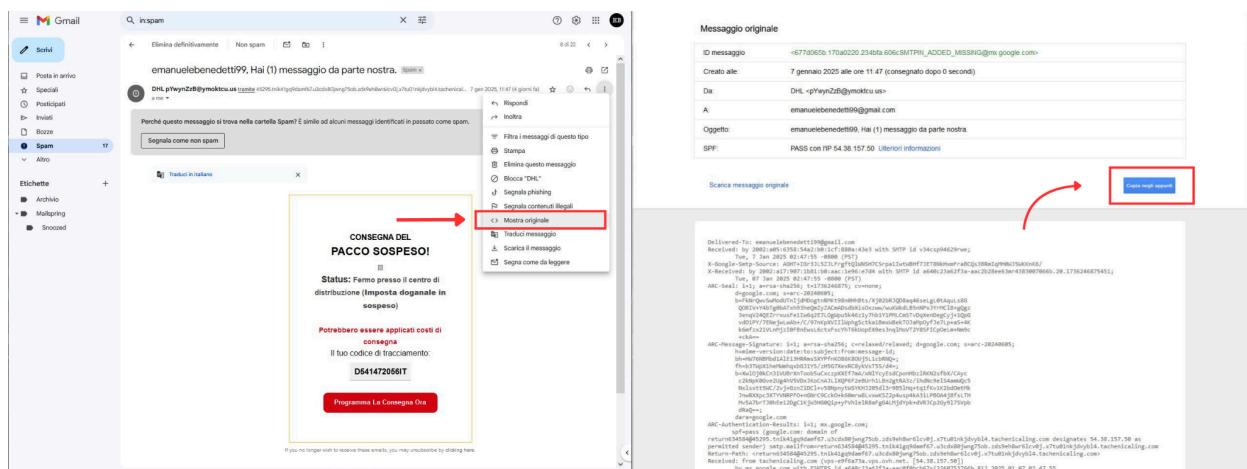
Bonus 1

Consegna

La prima consegna bonus chiedeva di creare un HTML copiando una mail di phishing già ricevuta.

Svolgimento


Per completare la consegna ho nuovamente utilizzato GoPhish, seguendo quasi completamente gli stessi passaggi usati per gli esempi precedenti. In questo caso però ho copiato il raw di un messaggio email ricevuto nella casella di posta privata. Le immagini mostrano i due passaggi per copiare l'HTML originale




Dopo aver copiato il messaggio originale, ho importato su GoPhish il template:

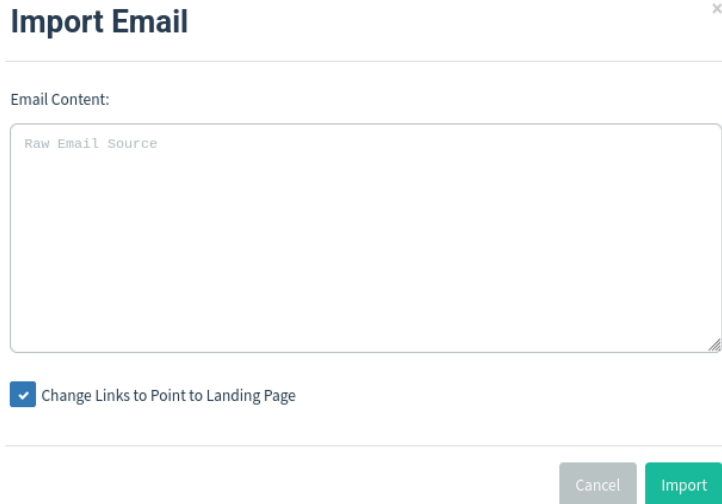
New Template

Name:

 Import Email

Envelope Sender: 

Cliccando su *Import Email* appare una nuova schermata che permette di incollare il messaggio copiato in precedenza.



Import Email ✕

Email Content:

Raw Email Source

☒ Change Links to Point to Landing Page

Cancel Import

Incolliamo qui il messaggio e spuntiamo la casella *Change Links to Point to Landing Page*.

In questo modo possiamo sostituire i link dell'originale messaggio di phishing con una landing page malevola da noi costruita.

L'esercizio si conclude con l'avvio di una nuova campagna di phishing. In questo modo l'email ricevuta sul nostro account è la stessa mail che abbiamo importato.

Bonus 2

Consegna

La consegna bonus chiedeva di creare una mail di phishing irriconoscibile.

Svolgimento

Scenario

Lo scenario che ho ipotizzato per eseguire la consegna è l'invio di un annuncio da parte del sito GitHub, che comunica agli utenti l'integrazione gratuita di Copilot nell'account GitHub. Ho appositamente scelto questo tipo di scenario poiché la mail esiste veramente e diversi clienti l'hanno ricevuta di recente.

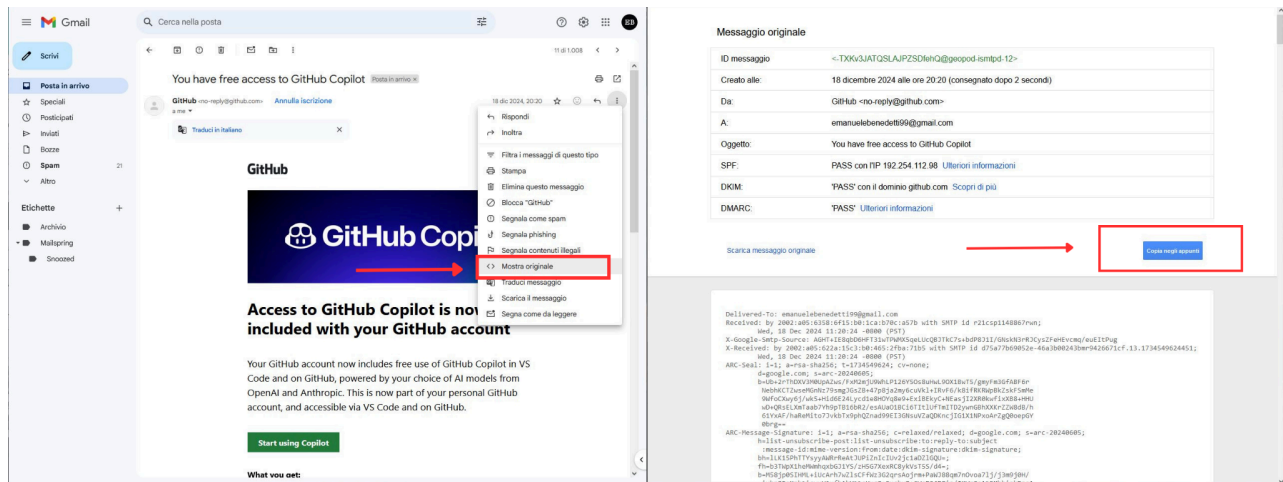
L'obiettivo è utilizzare la mail reale, modificarla appositamente per renderla pericolosa ed inoltrarla agli indirizzi email target per sottrarre le credenziali di accesso.

Creazione email

Per svolgere l'esercizio ho utilizzato il tool GoPhish, un software open-source utilizzato per creare e gestire campagne di simulazione di phishing.

Visto che ho già mostrato come ho impostato il tool per l'invio delle mail di phishing, mi limito a mostrare i nuovi passaggi che ho eseguito.

Per riuscire ad ottenere una mail irriconoscibile rispetto all'originale ho deciso di copiare un HTML di una mail reale che ho ricevuto. Come spiegato nello scenario, ho utilizzato il raw della mail di GitHub che annuncia la novità di Copilot integrata negli account. Per fare ciò ho seguito nuovamente i passaggi illustrati nel Bonus 1, fino ad importare il template nella sezione *Email Templates* di GoPhish.



Import Email

Name:

Envelope Sender:

Subject:

Email Content:

```

Ug60hiHnH8fLPbQ6LwVOYNeuxYle2LmBlomGcG00BwG2g0CVtHG3ZePhw-3D" alt="3D" wid=
th=3D"1" height=3D"1" border=3D"0" style=3D"height:1px !important;width:1px=
!important;border-width:0 !important;margin-top:0 !important;margin-bottom:=
:0 !important;margin-right:0 !important;margin-left:0 !important;padding-to=
p:0 !important;padding-bottom:0 !important;padding-right:0 !important;paddi=
ng-left:0 !important;"/></body>

</html>

--1e8ea70075ef9529425bb36f10ae49dd01941f07537077059efb7c713337--

```

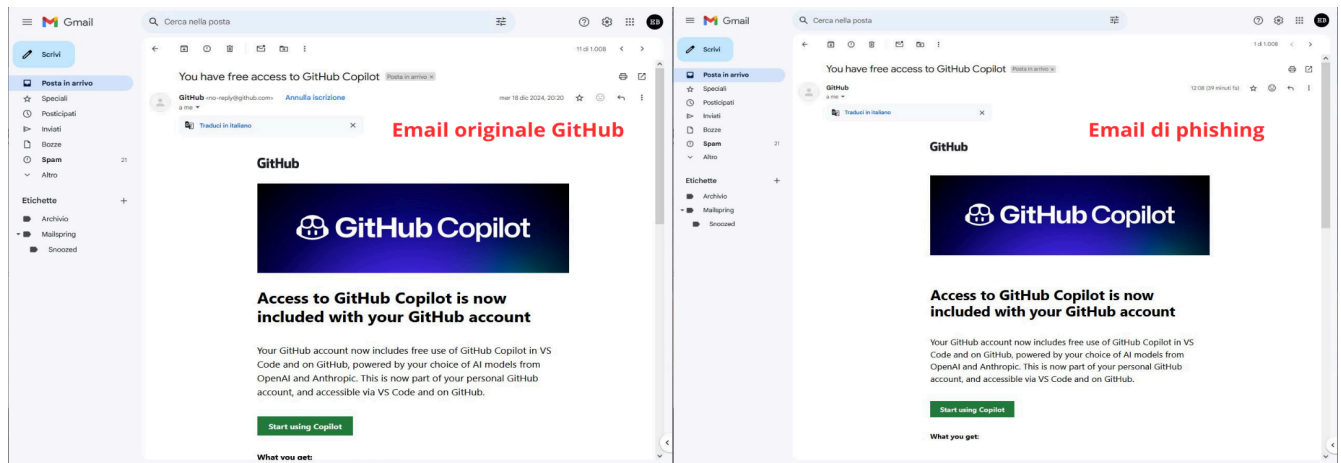
☒ Change Links to Point to Landing Page

Incolliamo il messaggio nella finestra *Import Email* e spuntiamo la casella *Change Links to Point to Landing Page*.

Questo passaggio è fondamentale per l'attaccante poiché permette di modificare tutti i link presenti all'interno della mail originale e sostituirli con link che puntano alla pagina web malevola creata nella landing page.

A questo punto non rimane altro che avviare la nuova campagna di phishing e osservare il risultato, confrontato alla mail originale.

Le due immagini che seguono mostrano una accanto all'altra le due email, l'originale e quella appena inviata tramite GoPhish:



Come ben evidenziato dalle due immagini affiancate, le email sono indistinguibili, il template viene interamente copiato e le immagini sono correttamente renderizzate dal client. In questo caso l'unica differenza visiva tra le email è data dalla presenza di un tasto fornito dal client di posta per disiscriversi dalla newsletter del sito reale, tuttavia la differenza emerge solamente affiancando le due email e attuando un'analisi approfondita del testo della mail.