PROGETTO S5

INGEGNERIA SOCIALE

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 dell'email che dovrebbero far scattare un campanello d'allarme sulla sua autenticità.

Svolgimento

Per generare il contenuto dell'email ho usato Copilot, questo è il testo generato:

Da: support@paypal-cares.com

Oggetto: URGENTE: Verifica immediata sul tuo account!

Caro cliente,

Abbiamo notato delle attività sospette sul tuo account PayPal e per proteggere il tuo saldo, ti chiediamo di aggiornare subito le tue informazioni. Clicca sul link seguente per verificare il tuo account:

www.pay-pal.org/aggiornamento-dati

Se non rispondi entro 24 ore, il tuo account sarà essere sospeso definitivamente. Non ignorare questa email!

Grazie per la tua imediata attenzione.

Cordiali saluti,

Il team di sicurezza PayPal

Scenario:

Con questa email un ipotetico phisher cerca di sfruttare la paura del target/vittima di perdere l'accesso a qualcosa di importante, come un conto PayPal. Lo scenario che tenta di creare è che hai qualche problema con il tuo account, e devi agire velocemente per sistemarlo, altrimenti potrebbe accadere qualcosa di negativo, come la sospensione del tuo account.

Questo scenario è progettato per manipolare psicologicamente il destinatario, creando un senso di urgenza e paura per indurlo a fornire

informazioni personali senza pensarci troppo. Per questo potrebbe risultare credibile ad una vittima che non è attenta a ciò che legge.

Detto ciò, ci sono comunque segnali che ci fanno capire che si tratta di un email di phishing, andiamo ad analizzarli:

Analisi dell'email:

- **Mittente:** L'indirizzo "support@paypal-cares.com" sembra simile a quello ufficiale ma non è autentico.
- **Oggetto:** Non è scritto in modo consono, la presenza della scritta "URGENTE" in maiuscolo e la presenza del punto esclamativo ci dovrebbe subito far scattare un campanello di allarme.
- **Saluto:** L'utilizzo di un saluto generico come "caro cliente" senza il nome dell'utente è un altro segnale che ci fa capire che c'è qualcosa che non va.
- **Urgenza e pressione:** Così come nell'oggetto la parola "URGENTE", l'email ci mette fretta e pressione dicendo "Se non rispondi entro 24 ore". Sono frasi che creano un senso di urgenza irrealistico, tipico dei tentativi di phishing.
- **Errori grammaticali:** Si deve prestare attenzione ad eventuali errori grammaticali o di sintassi. Ad esempio in questa e-mail nella frase: "Grazie per la tua imediata attenzione" la parola immediata è scritta senza una "m". Oppure in: "Se non rispondi entro 24 ore, il tuo account sarà essere sospeso definitivamente. Non ignorare questa email!" è palese l'utilizzo di un traduttore.
- **Link sospetto:** il link: "www.pay-pal.org/aggiornamento-dati" non è veritiero poiché si scrive "PayPal" e non "pay-pal", per non parlare del ".org" al posto di ".com".

La combinazione di questi segnali ci può aiutare a distinguere un'email di phishing da una reale. Comunque è sempre meglio procedere con cautela e verificare ulteriormente l'email prima di interagire con essa, oppure verificare che tipo di e-mail ci può mandare un determinato servizio così da evitare a priori di cascare in queste truffe.

BONUS 1

Creazione di un'e-mail più veritiera

Da: notifications@paypal.com

Oggetto: Verifica del conto necessaria

VERIFICA IL TUO ACCOUNT

Gentile [Nome vittima],

Abbiamo rilevato delle attività sospette sul tuo account PayPal. Per proteggere il tuo conto e garantire la tua sicurezza, ti chiediamo gentilmente di completare una breve verifica entro 24 ore.

Verifica il mio account----> non visibile (http://www.pay-pal.com/signin)

Se non prenderai provvedimenti entro il tempo stabilito, potremmo dover limitare temporaneamente l'accesso al tuo account per proteggere le tue informazioni personali.

Grazie per la collaborazione.

Cordiali saluti,

Il Team di Sicurezza PayPal

Questa è una notifica automatica, si prega di non rispondere a questo messaggio. Per qualsiasi domanda, visita il nostro Centro Assistenza.

Analisi dell'email:

- In questo caso il mittente sembra legittimo, "notifications@paypal.com" è molto simile a un indirizzo autentico di PayPal.

- Il saluto è personalizzato, l'aggiunta del nome aumenta la credibilità, i phisher possono utilizzare tecniche per ottenere il nome della vittima e rendere l'email più convincente.

- Il linguaggio è più rassicurante e convincente, sembra un e-mail formale e professionale.

- Non c'è una richiesta aggressiva, l'aggiunta di "e garantire la tua sicurezza", "gentilmente" o "potremmo dover limitare temporaneamente" evita appunto di sembrare una richiesta aggressiva.

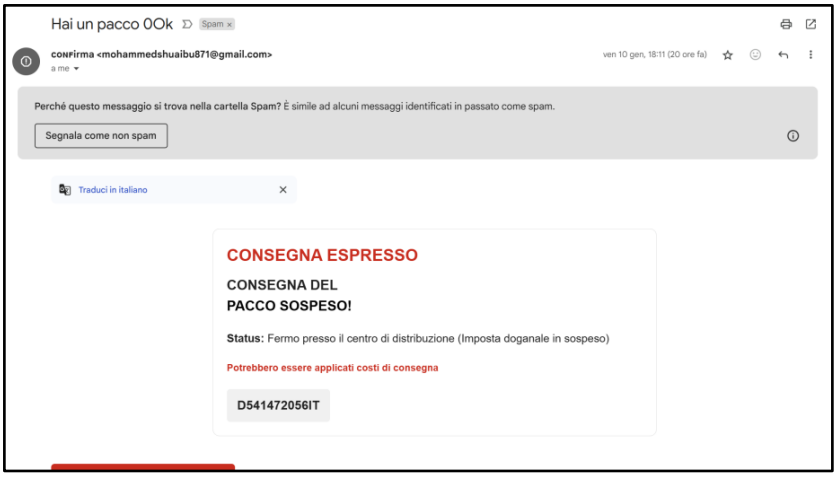
- Assenza di un link in chiaro che faccia insospettire la vittima, ma la presenza di "*Verifica il mio account* " *che ci permette di nascondere alla vista della vittima l'URL malevola (anche in questo caso "pay-pal" è scritto in modo errato) rendendo il tutto più veritiero*.

- Presenza di informazioni su assistenza*, che* Include un riferimento al Centro di Assistenza PayPal per aumentare la autenticità.

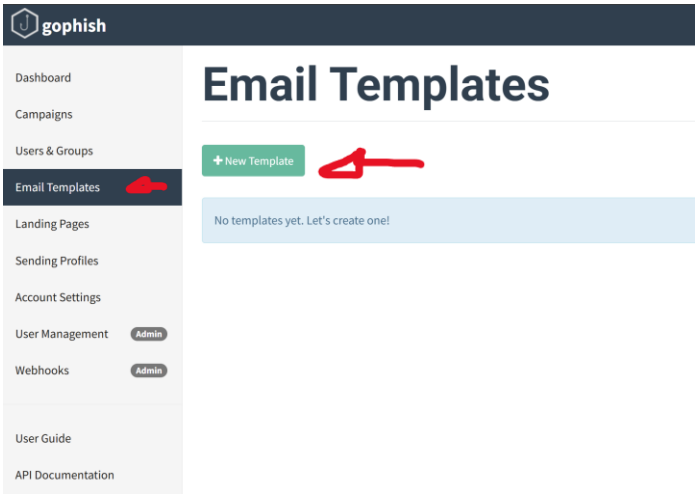
- Presenza di un identificativo del servizio, in questo caso il logo di PayPal posizionato in alto a sinistra.

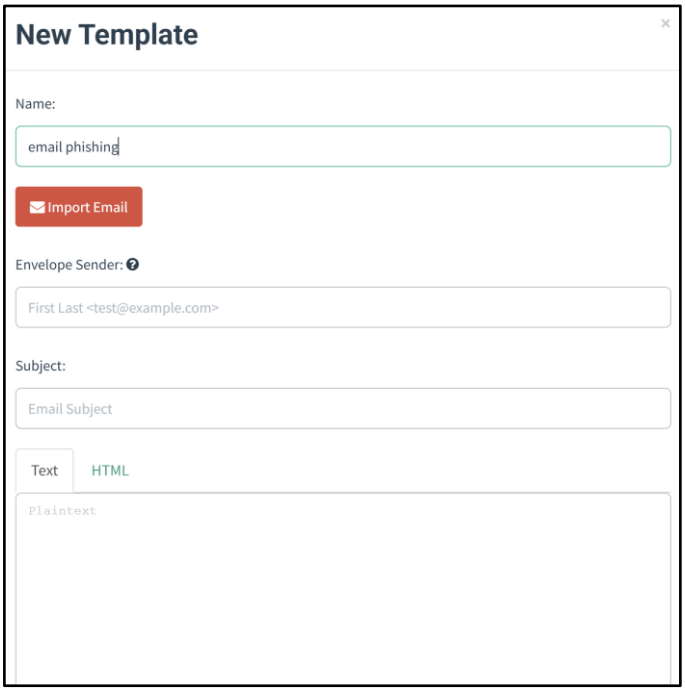
BONUS 2

Il bonus 2 chiedeva di creare l'html di un email phishing, io ho scelto un email tra gli spam:



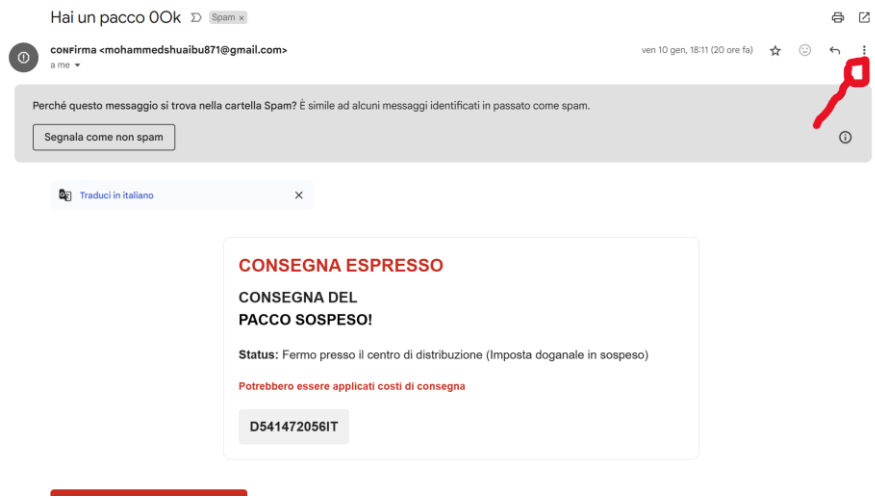
Per prima cosa ho aperto gophish e ho creato un nuovo email template:



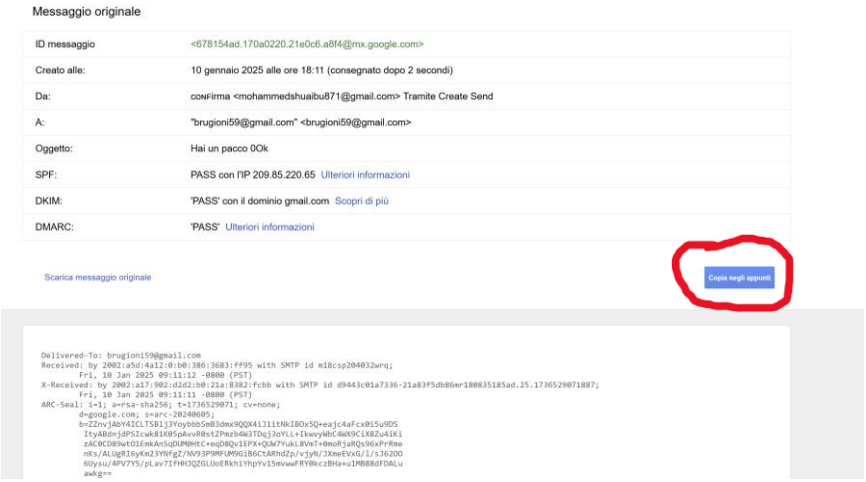


Inserisco un nome e clicco su “import email”

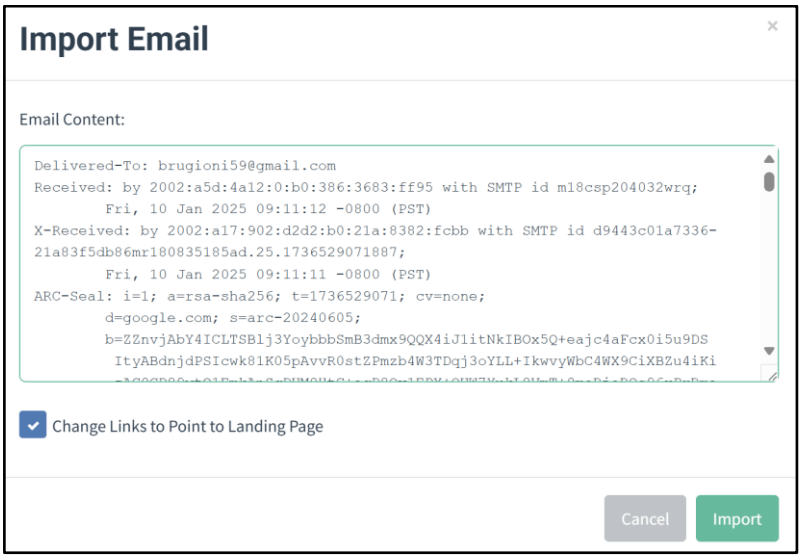
Torno nella mia casella postale e vado nell’email che ho scelto



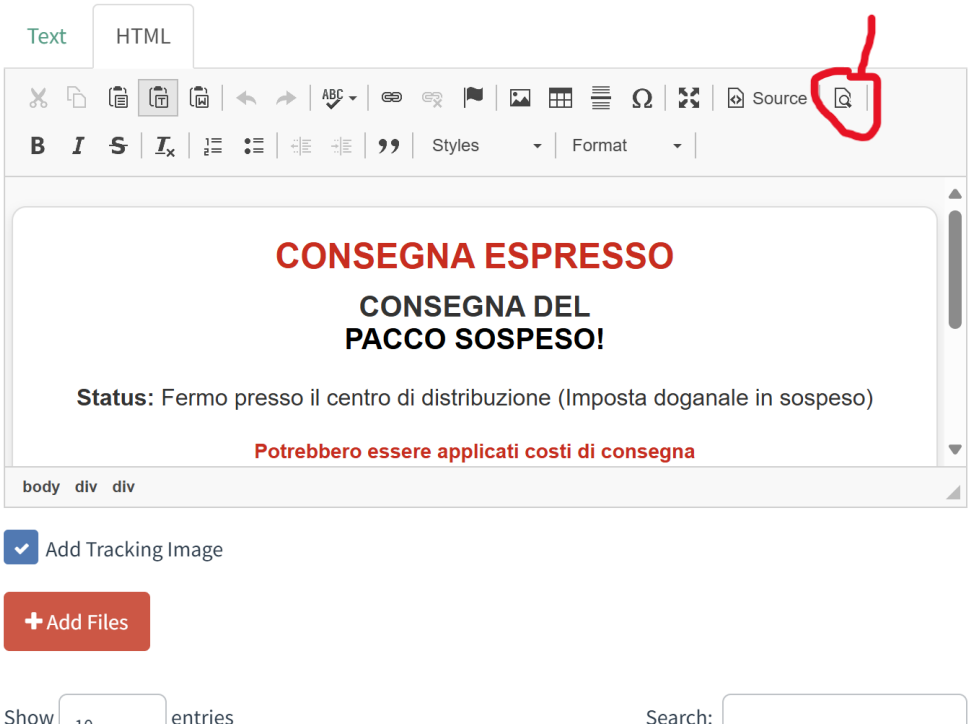
Clicco sui 3 puntini in alto a destra, -----> mostra originale e mi copio il contenuto negli appunti



Torno su gophish e importo il contenuto dell’email



Clicco su import



Come possiamo vedere l'email è stata copiata e ora abbiamo l'HTML.
Clicchiamo su preview per verificare