

# Scenario di Simulazione: Phishing con Profilo Hackerato di Influencer Crypto

## Obiettivo del phishing:

L'obiettivo della simulazione è indurre le vittime a trasferire criptovalute a un indirizzo wallet fraudolento, facendogli credere che stiano partecipando a un'iniziativa promossa dall'influencer crypto (es. un *giveaway*).

---

## 1. Scenario Simulato

Immaginiamo che un hacker abbia compromesso l'account Instagram di un noto influencer nel mondo delle criptovalute, ad esempio "CryptoGuruPro". L'influencer è famoso per i suoi *giveaway* regolari e le promozioni di nuovi progetti blockchain. Gli hacker sfruttano questa fiducia costruita nel tempo per avviare una campagna di phishing.

- **Contesto realistico:** L'influencer invia un'email e pubblica un post su Instagram che promuove un "giveaway crypto". Le vittime devono cliccare su un link per partecipare, che conduce a una pagina fraudolenta.
  - **Target:** Seguaci dell'influencer, in particolare utenti già esperti nel settore crypto.
  - **Motivazione delle vittime:** La possibilità di ottenere un guadagno economico rapido (criptovalute gratuite).
- 

## 2. Email di Phishing Generata

### Oggetto:

Sei uno dei vincitori! 🎉 Richiedi subito i tuoi ETH gratuiti!

### Corpo dell'email:

---

**Da:** CryptoGuruPro <waricah804@rustetic.com>

**A:** [Email della vittima]

# Congratulazioni, sei stato selezionato!





Siamo felici di annunciarti che sei uno dei vincitori del nostro **Crypto Giveaway** per celebrare i 100.000 follower su Instagram!

Come parte della community di **CryptoGuruPro**, vogliamo premiarti con un regalo esclusivo: **2 BTC gratuiti**.

Per ricevere il tuo premio, segui questi semplici passi:

1. Clicca sul pulsante qui sotto per accedere al tuo account.
2. Inserisci il tuo indirizzo wallet BTC per ricevere il premio.
3. Conferma il tuo wallet inviando 0.1 BTC (necessario per autenticare la transazione).

 Richiedi il tuo premio ora

 **Nota:** Questa offerta è valida solo fino alle 23:59 di oggi. Non perdere questa opportunità unica!

Ricevi questa email perché sei iscritto alla nostra newsletter. Per qualsiasi dubbio, contattaci a [support@cryptogurupro.com](mailto:support@cryptogurupro.com).

© 2024 CryptoGuruPro. Tutti i diritti riservati.

---

### 3. Spiegazione dello Scenario

**Perché l'email potrebbe sembrare credibile?**

- **Autorità:** L'email proviene apparentemente da un influencer riconosciuto e affidabile nel settore.
  - **Urgenza:** La scadenza stringente spinge le vittime ad agire senza riflettere.
  - **Contesto realistico:** Giveaway e promozioni sono pratiche comuni nel mondo crypto.
  - **Fiducia consolidata:** L'influencer ha già un pubblico che lo segue regolarmente e conosce i suoi contenuti.
- 

**Elementi che dovrebbero far scattare un campanello d'allarme:**

1. **Dominio sospetto:** L'indirizzo email usa un dominio non ufficiale <http://localhost:8080/index.html> ( invece di un dominio verificato come [cryptogurupro.com](http://cryptogurupro.com)).
2. **Richiesta di pagamento anticipato:** I giveaway autentici non richiedono mai di inviare denaro per partecipare.
3. **Link sospetti:** Il link porta a un sito apparentemente legittimo ma non verificabile (es. l'URL non corrisponde al sito ufficiale).
4. **Urgency Bias:** La scadenza immediata è progettata per ridurre la capacità delle vittime di ragionare.
5. **Errori minimi:** Nonostante il linguaggio curato, piccoli dettagli possono rivelare l'inganno, come la richiesta di *inviare* criptovalute o il fatto di aver inserito nell'oggetto

dell'email un riscatto della criptovaluta ETH mentre nel corpo del messaggio si parla di BTC.

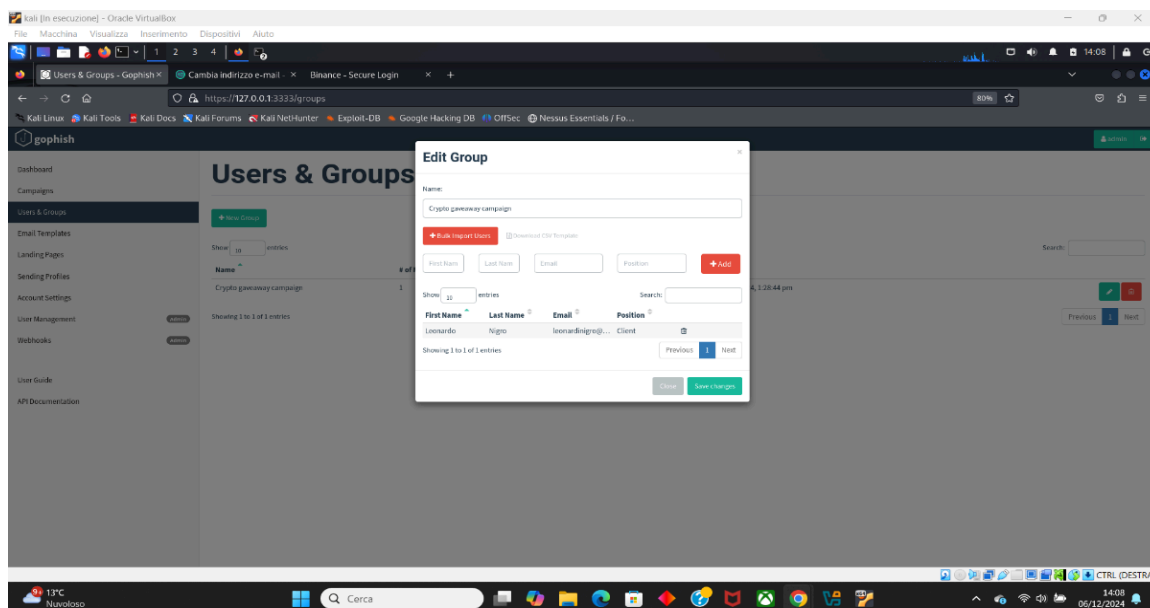
6. **Messaggio originale:** Se l'utente una volta ricevuta l'email controllasse il messaggio originale e il messaggio grezzo dell'email noterebbe che l'email in realtà è spedita da un indirizzo di posta elettronica non collegato a nessun account social del presunto influencer

## 5. Conclusioni e Misure Preventive

- Verificare il dominio del mittente.
- Non cliccare link non verificati.
- Non inviare denaro per partecipare a giveaway.
- Utilizzare strumenti di rilevamento di phishing
- Verificare il messaggio originale dell'email per cercare eventuali anomalie o incongruenze

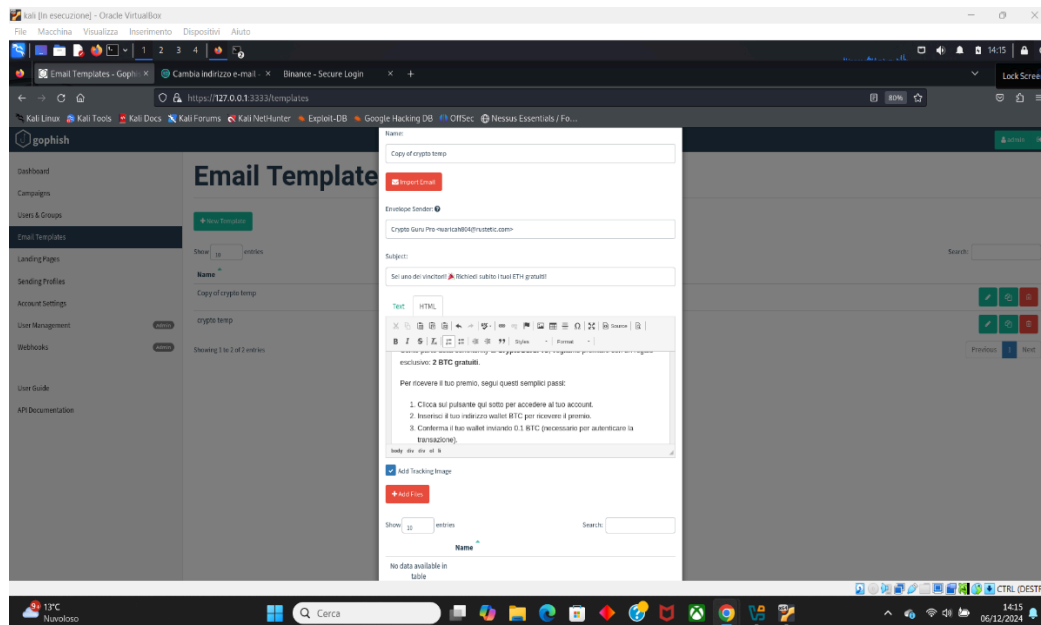
Di seguito allego delle foto di come ho configurato la campagna di phishing su gophish:

Per quanto riguarda l'utente o il gruppo sui quali effettuare la campagna di phishing o inserito una persona sola e come target per questa simulazione ho scelto me stesso:

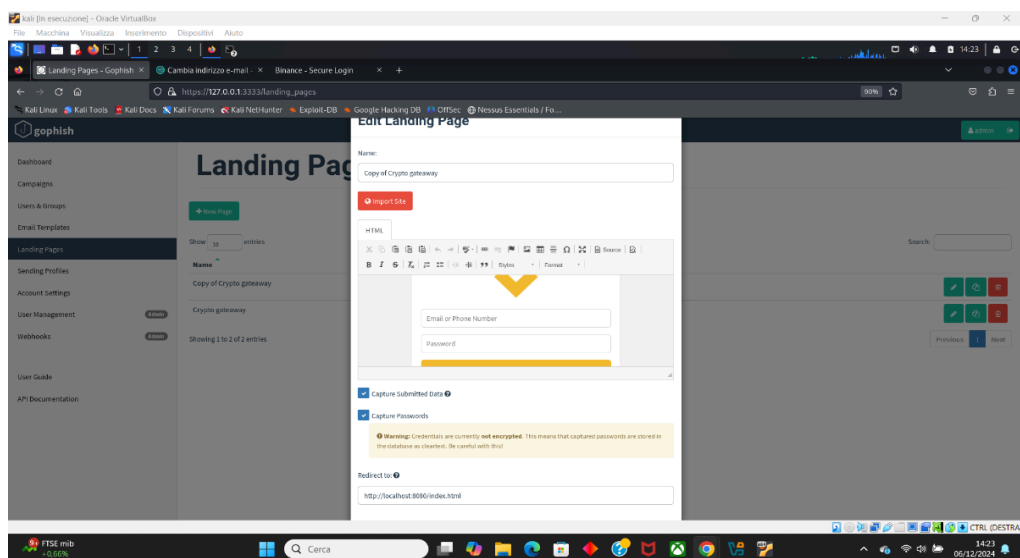
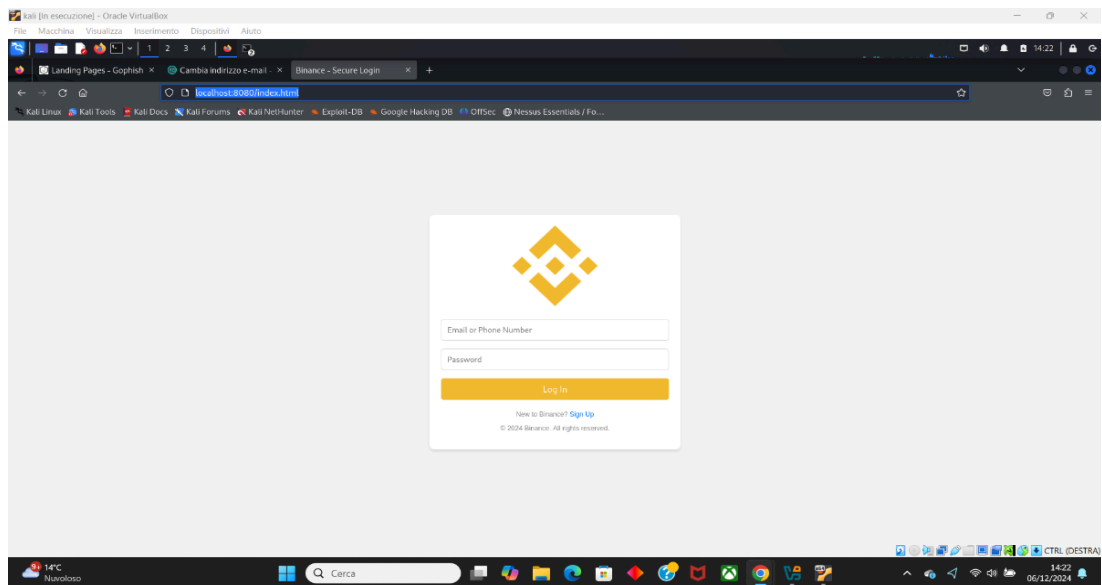


Per quanto riguarda il template dell'email, ho fatto generare a chatGPT un' email che simulasse l'offerta di gateway, per importarla su gophish ho chiesto a chat di fornirci il messaggio grezzo (raw) dell'email in maniera tale da esportarla, successivamente modificata da me per creare un ulteriore campanello d'allarme creando una sorta di incoerenza fra l'oggetto dell'email e il corpo del messaggio, per dare la possibilità a chi avesse una buona capacità di osservazione di accorgersi attraverso queste piccolezze di individuare subito la truffa.

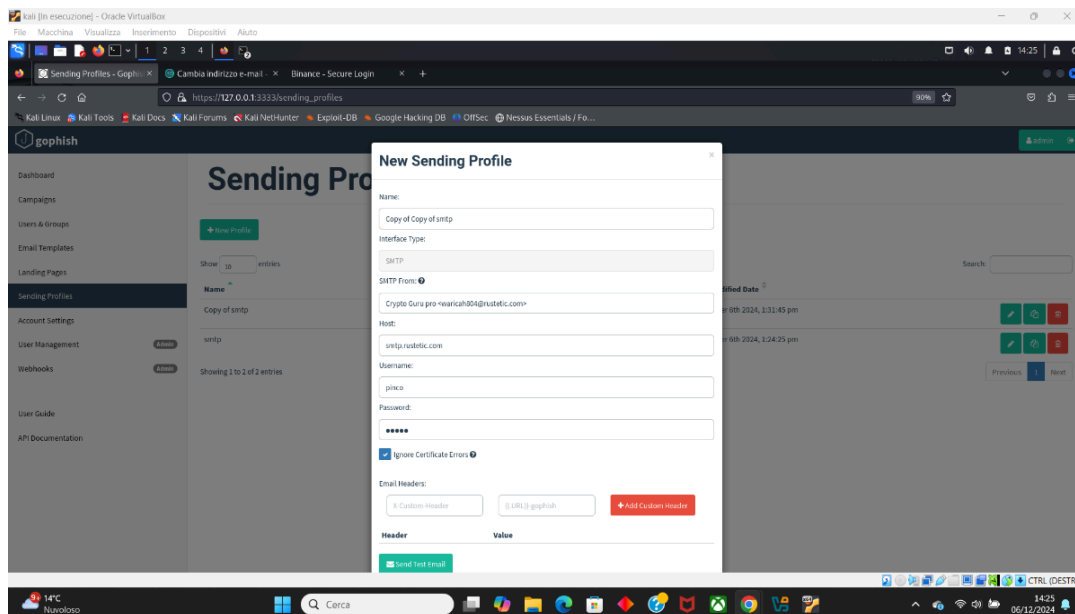
Per quanto riguarda l'indirizzo email del mittente del messaggio, ho usato una temp-mail



Per quanto riguarda la landing page ho fatto creare a chatGPT una pagina html simile alla pagina di login della piattaforma "Binance", ho salvato il codice html della pagina creata da chat in un file utilizzando l' editor di testo nano presente sulla macchina kali e salvato come index.html. Una volta fatto questo ho fatto partire un server web locale tramite python che ospitava la pagina html creata precedentemente, per fare questo ho utilizzato il seguente comando: `python3 -m http.server 8080`



Per quanto riguarda la sezione sendig profile l'ho configurata utilizzando l'email precedentemente creata con temp mail



Una volta finite queste configurazioni, ho configurato la sezione “Campaigns” inserendo le sezioni configurate nei passaggi precedenti e una volta finito anche questo passaggio ho lanciato la campagna di phishing:

