1. Creazione dello scenario:

- **Contesto:** Immagina che la vittima abbia recentemente acquistato un biglietto del treno online. Pochi giorni dopo, riceve un'email che sembra provenire dalla compagnia ferroviaria.
- **Obiettivo:** L'obiettivo del phishing è rubare le credenziali di accesso dell'utente al sito della compagnia ferroviaria, che potrebbero poi essere utilizzate per accedere a informazioni personali o dati finanziari.

2. Scrittura dell'email di phishing:

- **Oggetto:** "Avviso importante: verifica urgente del tuo account"
- **Corpo dell'email:**

Gentile Cliente,

Abbiamo rilevato un'attività sospetta sul tuo account. Per motivi di sicurezza, ti chiediamo di verificare immediatamente le tue credenziali di accesso.

Clicca sul seguente link per confermare il tuo account: italotreno.con

Ti ricordiamo che, in caso di mancata verifica entro 24 ore, il tuo account potrebbe essere sospeso.

Cordiali saluti,

Il team di supporto Italo S.b.a

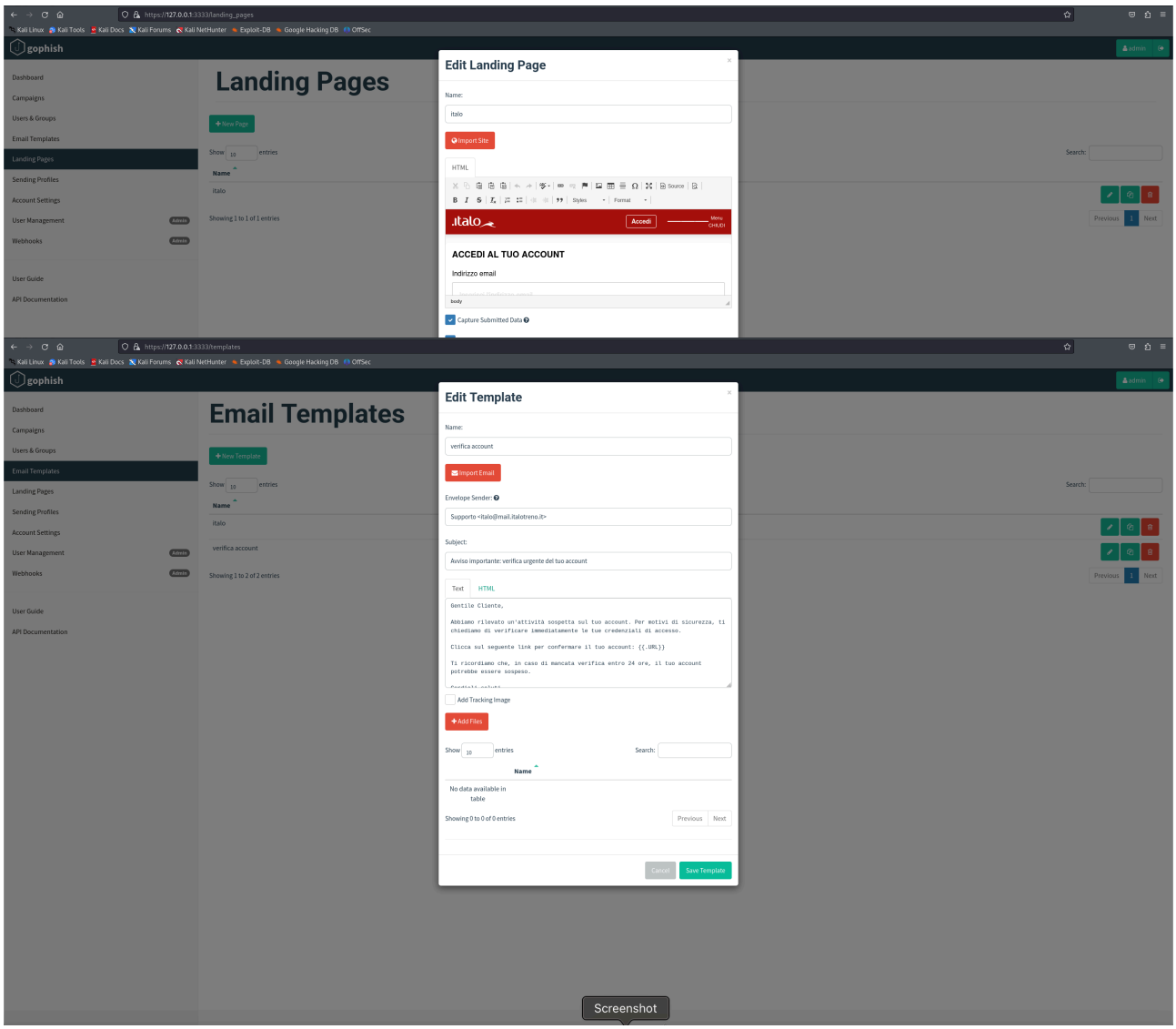
Nota: Questo messaggio è generato automaticamente dai nostri sistemi. Per ulteriori informazioni consulta italotreno.con. Se non vuoi più ricevere le nostre comunicazioni, puoi modificare in ogni momento i consensi Privacy da te forniti accedendo alla tua Area Personale nella sezione “Dati Personali e Preferenze”. L’eventuale modifica dei consensi forniti sarà effettiva sui nostri sistemi entro massimo 7 giorni. Puoi trovare l’informativa completa in materia di privacy, sul nostro sito italotreno.con. Invitiamo a non rispondere a questo messaggio, questa casella di posta elettronica non è abilitata alla ricezione.

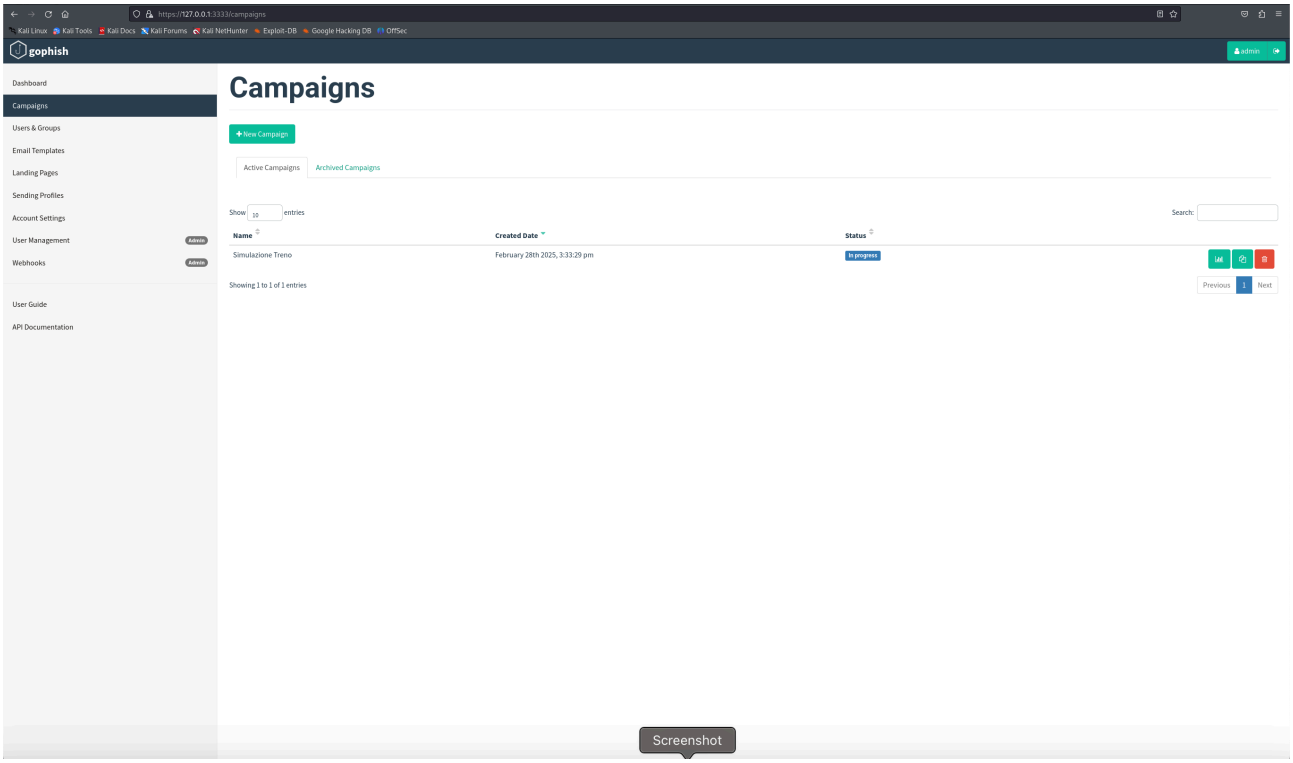
3. Spiegazione dello scenario:

- **Credibilità:** L'email potrebbe sembrare credibile perché:
  - La vittima ha recentemente interagito con la compagnia ferroviaria.

- L'email crea un senso di urgenza, spingendo la vittima ad agire rapidamente senza pensare.
- L'email utilizza un linguaggio formale e professionale.
- L’email finisce con Italo S.b.a che è certamente falso

- **Campanelli d'allarme:**
  - Il link è sospetto: prima di cliccare, la vittima dovrebbe controllare l'URL per assicurarsi che sia legittimo.
  - L'email contiene errori grammaticali o di ortografia.
  - L'email richiede informazioni sensibili tramite un link, invece di indirizzare la vittima al sito ufficiale.
  - L'email crea un senso di urgenza ingiustificato.
-




https://127.0.0.1:3333/campaigns
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
gophish
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Account Settings
User Management
Admin
Webhooks
Admin
User Guide
API Documentation
Campaigns
New Campaign
Active Campaigns
Archived Campaigns
Show 10 entries
Search:
Name
Created Date
Status
Simulazione Treno
February 28th 2025, 3:33:29 pm
In progress
Showing 1 to 1 of 1 entries
Previous
1
Next
Screenshot