

**Esercizio S5L5**

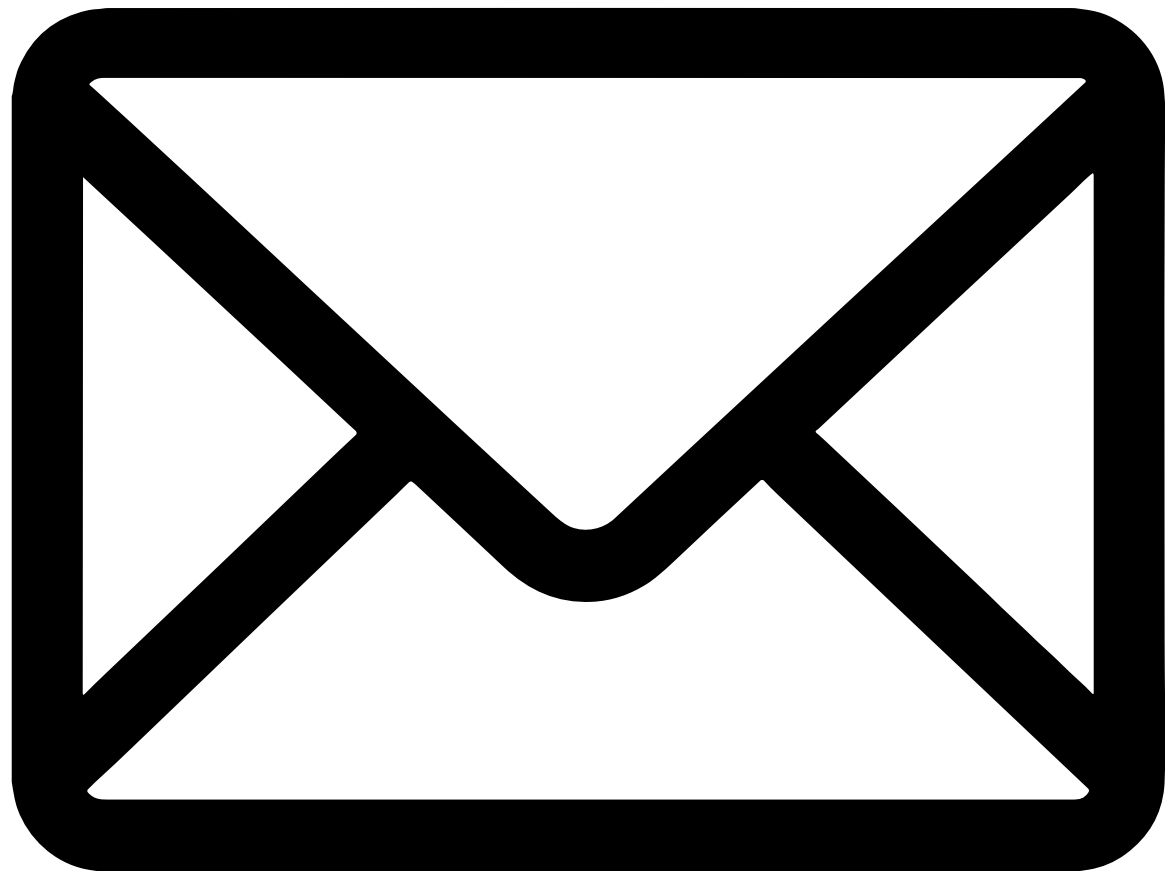
# **Simulazione**

---

# **Phishing**

---

Oggi, abbiamo imparato a riconoscere, creandole, delle email truffa per rubare dati sensibili, come nel nostro caso username e password. Questo sarà molto utile alle aziende per istruire i propri dipendenti nel trattare i propri dati in modo sicuro per non compromettere l'azienda, e la creazione di queste email sarà anche un nostro compito in azienda.



## Obiettivo dell'esercizio

- Sensibilizzare sul rischio del phishing mirato (spear phishing)
- Simulare un attacco realistico e plausibile
- Valutare la reazione degli utenti

## Scenario scelto

- Mittente: HR dell'azienda
- Target: Dipendente Mario Rossi
- Tema: Selezione per un viaggio premio aziendale in Spagna
- Obiettivo dell'attaccante: Raccolta di credenziali (username e password)

### Congratulazioni! Sei stato selezionato per un Weekend in Spagna



Ufficio Risorse Umane <hr@azienda-italiana.it>

To Mario Rossi

Caro Mario Rossi,

Con grande piacere ti informiamo che sei stato selezionato, insieme ad altri 10 dipendenti, per partecipare all'iniziativa **"Weekend di Benessere Aziendale"**, promosse dal nostro dipartimento HR.

→ Il premio consiste in **un weekend tutto pagato in Spagna (Barcellona)** dal 20 al 22 settembre 2025, comprensivo di volo, hotel 4\* e attività di team building!

Per confermare la tua partecipazione, ti chiediamo di accedere al Portale HR Aziendale entro e non oltre il 5 agosto 2025.

**Accedi ora al portale:** <https://intranet.azienda-italiana.it-premio2025>

(accesso richiesto con le tue credenziali aziendali)

In caso di dubbi,  
contatta il tuo.

Elena Bianchi

Ufficio Risorse Umane



Per raggiungere l'obiettivo mi sono avvalsa di Gophish per la creazione virtuale di una email phishing, e di Chat gpt per ricreare immagini e aiutarmi nello strutturare lo scenario.

Devo creare per un esercizio del corso a cui partecipo di cybersecurity, una finta email di phishing, immaginiamo un contesto dove un lavoratore di nome Mario Rossi riceve dalla sua azienda HR una email dove è stato selezionato insieme ad altri dipendenti per vincere un premio, ovvero un weekend in Spagna, creami anche una immagine di come potrebbe essere una email del genere. l'obiettivo sarà quello di prendere username e password della azienda, dato che l'email rimanderà ad un sito aziendale dove devono loggarsi

Perfetto, stai lavorando su un tipico scenario di **simulazione di phishing** con finalità educative, e hai scelto un approccio socialmente plausibile: un premio da HR per i dipendenti. Qui sotto ti propongo:

Oggetto: 🎉 Congratulazioni! Sei stato selezionato per un Weekend in Spagna 🇪🇸

Mittente: Ufficio Risorse Umane [hr@azienda-italiana.it](mailto:hr@azienda-italiana.it)

Caro Mario Rossi,

Con grande piacere ti informiamo che sei stato selezionato, insieme ad altri 10 dipendenti, per partecipare all'iniziativa "Weekend di Benessere Aziendale", promossa dal nostro dipartimento HR.

👉 Il premio consiste in un weekend tutto pagato in Spagna (Barcellona) dal 20 al 22 settembre 2025, comprensivo di volo, hotel 4★ e attività di team building!

Per confermare la tua partecipazione, ti chiediamo di accedere al Portale HR Aziendale entro e non oltre il 5 agosto 2025.

🔑 Accedi ora al portale:

👉 <https://intranet.azienda-italiana.it/hr-premio2025>

(accesso richiesto con le tue credenziali aziendali)



# Risultato di chat gpt

**Congratulazioni! Sei stato selezionato per un Weekend in Spagna**



**Ufficio Risorse Umane** <hr@azienda-italiana.it>

To Mario Rossi

Caro Mario Rossi,

Con grande piacere ti informiamo che sei stato selezionato, insieme ad altri 10 dipendenti, per partecipare all'iniziativa **"Weekend di Benessere Aziendale"**, promossa dal nostro dipartimento HR.

→ Il premio consiste in **un weekend tutto pagato in Spagna (Barcellona)** dal 20 al 22 settembre 2025, comprensivo di volo, hotel 4\* e attività di team building!

Per confermare la tua partecipazione, ti chiediamo di accedere al Portale HR Aziendale entro e non oltre il 5 agosto 2025.

**Accedi ora al portale:** <https://intranet.azienda-italiana.it-premio2025>

(accesso richiesto con le tue credenziali aziendali)

In caso di dubbi,  
contatta il tuo.

Elena Bianchi  
Ufficio Risorse Umane

## Portale HR Aziendale

Username

Password

accesso richiesto con le tue credenziali aziendali

Accedi

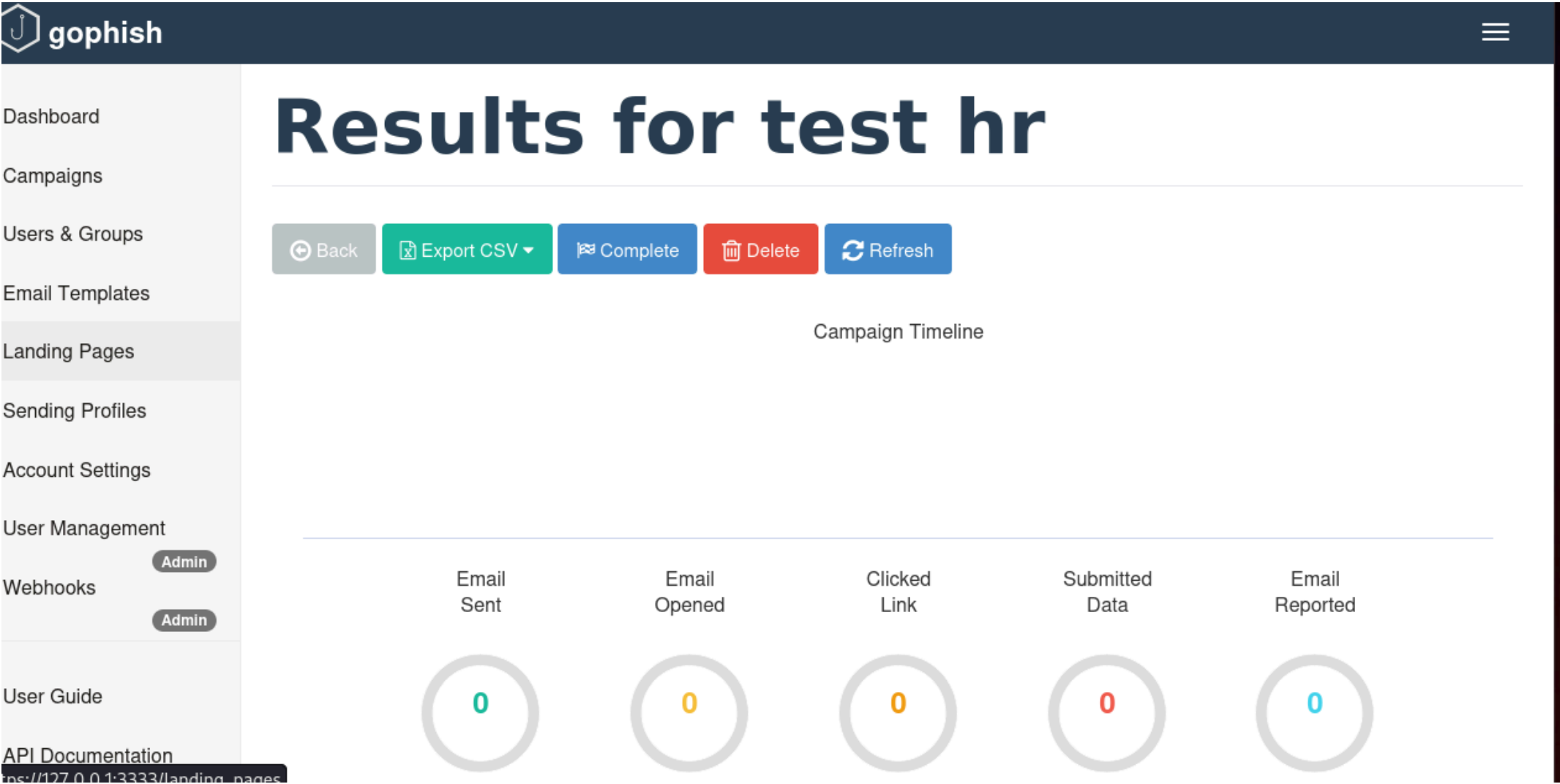
## Portale HR Aziendale



## Spiacenti, non hai vinto il Weekend di Benessere Aziendale

Ci dispiace informarti che la tua selezione, in seguito al processo di verifica, non è andata a buon fine.  
Ti auguriamo di avere miglior fortuna in futuro.

# Su Gophish



## Edit Group

Name:

gruppo test interno

[+ Bulk Import Users](#)

[Download CSV Template](#)

First Name

Last Name

Email

Position

[+ Add](#)

Show 10 entries

Search:

First Name

Last Name

Email

Position

Mario	Rossi	mario.rossi@a...	<a href="#">🗑️</a>
-------	-------	------------------	--------------------



Showing 1 to 1 of 1 entries

Previous

1

Next

Close

Save changes

## Edit Sending Profile

Name:

HR Fake Sender

Interface Type:

SMTP

SMTP From: ?

hr@azienda.local

Host:

smtp.fake.local

Username:

hr

Password:

●●●●●●●●

☒ Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{{.URL}}-gophish

[+ Add Custom Header](#)



## Edit Template

Name:

Concorso HR - Weekend Benessere

 Import Email

Envelope Sender: 

Ufficio HR <hr@azienda.it>

Subject:

 Sei stato nominato per il premio Dipendente del Mese!

Text

HTML

```
<html>
  <body style="font-family: Arial, sans-serif;">
    <p>Ciao <b>{{.FirstName}}</b>, </p>
    <p>Sei stato selezionato tra i candidati al <b>Dipendente del Mese</b>. </p>
    <p>Il premio: <b>Weekend benessere per 2 persone</b> presso il resort "Terme
di Armonia". </p>
    <p>
      <a href="{{.URL}}" style="background-color:#007BFF;color:#fff;padding:10px
20px;text-decoration:none;border-radius:5px;">
        Conferma la tua candidatura
      </a>
    </p>
  </body>
</html>
```

☐ Add Tracking Image

Dopo aver installato gophish sulla Kali, ho iniziato a settare lo scenario portando lo scenario creato su chatgpt, quindi ho messo una email fasulla, sia del mittente che del ricevente, successivamente ho creato grazie a chat gpt uno script per strutturare l'email con un oggetto, alla fine ho creato il lunch e mandato, ovviamente non ho risultati da mostrare purtroppo per problemi di dominio



# Come si può capire se si tratta di una email phishing

## 1. Falsa urgenza o opportunità imperdibile

Promessa di un premio importante (viaggio in Spagna)

Termine ravvicinato per confermare → crea pressione e fretta

## 2. Mittente apparentemente legittimo

L'indirizzo "hr@azienda-italiana.it" sembra plausibile

Ma potrebbe essere spoofato o leggermente alterato (es. con una lettera diversa tipo aziendaliana)

## 3. Link sospetto o manipolato

Il link mostrato sembra ufficiale → <https://intranet.azienda-italiana.it>

Ma potrebbe portare a un dominio simile ma malevolo (es. azienda-laliaha.it)

Sempre passare il mouse sul link prima di cliccare

## 4. Richiesta di credenziali aziendali

Nessuna comunicazione legittima dovrebbe chiedere di fare login per un premio

Le HR non dovrebbero mai chiedere l'accesso al portale in questi contesti

## 5. Stile e formato troppo generico

Mancanza di riferimenti ufficiali (loghi, firme verificate)

Nessuna conferma del regolamento del concorso o link a documentazione

## 6. Email personalizzata ma sospettosa

Uso del nome corretto ("Mario Rossi") → segno che l'attacco è mirato (spear phishing)

Proprio per questo più pericoloso e difficile da riconoscere

## Possibili contromisure

- Formazione continua per i dipendenti
- Simulazioni regolari di phishing
- Attivazione di MFA
- Analisi dei log d'accesso
- Segnalazione delle email sospette

## In conclusione

Questo esercizio mi ha mostrato l'importanza della consapevolezza che

Il phishing può assumere molte forme, è importante assumere delle contromisure e soprattutto mi ha sicuramente fatto capire che non devo mai inserire credenziali in link sospetti, anche se "credibili".