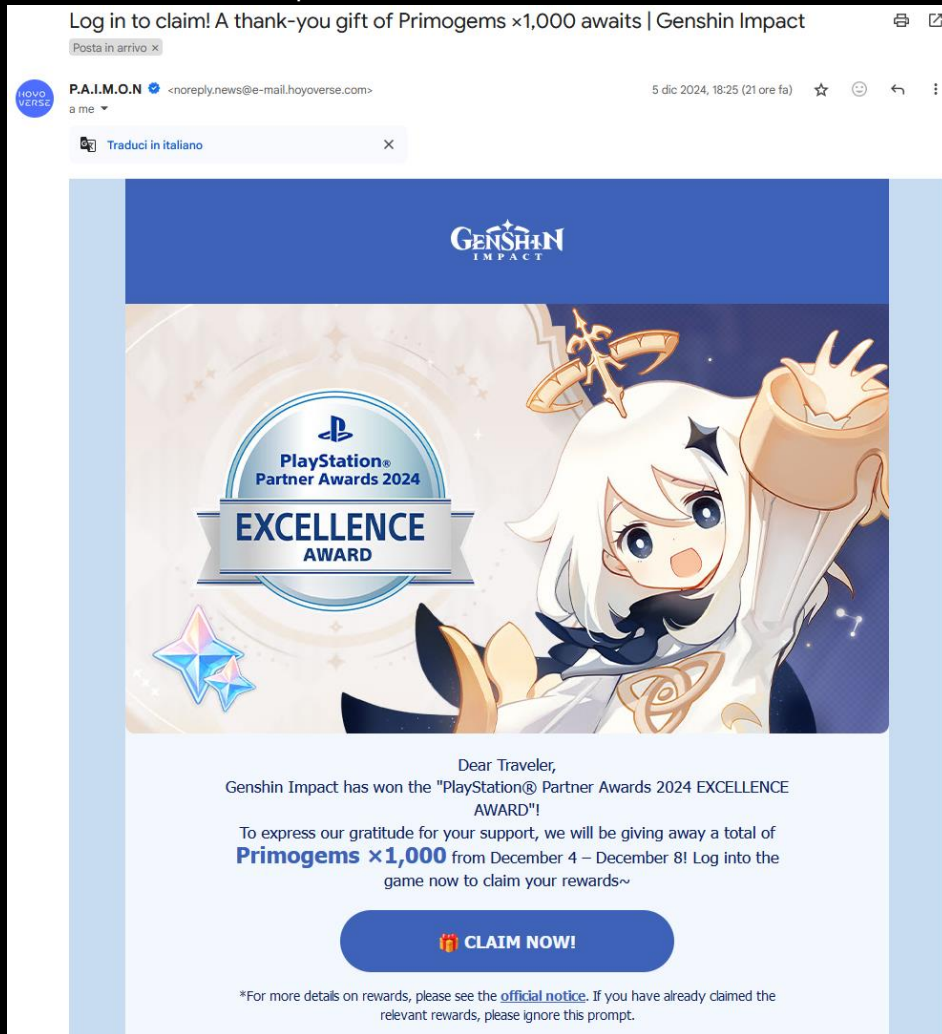


Relazione Test Email di Phishing

Per questa relazione, ispirato da una mail ricevuta riguardo un videogioco che ho giocato tempo fa, ho voluto ideare uno scenario ipotetico in cui un membro di un'azienda X, riceve questa mail, virtualmente identica a quella del gioco, ma che all'interno contiene un link malevolo (in questo caso sostituito da una cosa scherzosa per rimproverare il dipendente).

Per prima cosa, la mail di base che ho ricevuto

La mail che ho ricevuto è questa:



Ho preso il contenuto di questa mail e l'ho clonato, prendendo il file sorgente e sostituendo ogni link con un URL temporaneo (che sostituirò in seguito con un URL funzionante)

GoPhish

Dopo aver fatto questo, ho installato GoPhish sulla mia macchina, settando i vari parametri per permettere al servizio di inviare delle mail funzionanti, con un'email creata appositamente per risultare "simile" a quella originale, ma abbastanza diversa da renderla riconoscibile ad un occhio attento.

Di seguito le varie impostazioni:

Contenuto della mail

Edit Template

Name:

Hoyo1000Primo

Import Email

Envelope Sender: ⓘ

First Last <test@example.com>

Subject:

Log in to claim! A thank-you gift of Primogems x1,000 awaits | Genshin Impact

TextHTML

XUndoRedoBoldItalicLinkImageTableListGroupQuoteCodeAlignLeftAlignCenterAlignRightJustifyIndentDecreaseIndentIncreaseOutdentPrintSourceFullscreen

<html xmlns="http://www.w3.org/1999/xhtml" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:v="urn:schemas-microsoft-com:vml">
 <head>
 </head>
 <body bgcolor="#f7dcdf" style="background-color:#f7dcdf; margin-left:auto; margin-right:auto; width:100%; max-width:100%">
 <p class="alt" src="https://vphwzrk1.f.us-west-2.amazonaws.com/track/me/10/0101019397dbd4fb5bcdc7c-2389-47ad-a3ab-dde827671f26-000000/vMjQVnJl3KqIdIQjH579vbUeS5Y=404"></p>
</body>
</html>

Add Tracking Image

+ Add Files

Show10entriesSearch:

Name

No data available in table

Showing 0 of 0 entriesPreviousNext

Mittente

✕

Edit Sending Profile

Name:

Interface Type:

SMTP

SMTP From: ⓘ

Host:

Username:

Password:

☒ Ignore Certificate Errors ⓘ

Email Headers:

Show entries

Search:

Header ⓘ	Value ⓘ
No data available in table	

Showing 0 to 0 of 0 entries

Creazione pagina login

In seguito, ho creato una finta pagina di login dove l'utente ignaro veniva reindirizzato, invece del sito ufficiale, che ho in seguito hostato per testing su un indirizzo locale della macchina.

Edit Landing Page

Name:

COPY OF SCAMHOYO

Import Site

HTML

<!DOCTYPE html><html lang="it"><head>
 <base href="http://192.168.1.9:8080/site.html"/><meta charset="UTF-8"/><meta
name="viewport" content="width=device-width, initial-scale=1.0"/>
 <title>Login - Esempio</title>
 <style type="text/css">body {
 font-family: Arial, sans-serif;
 background-color: #f5f5f5;
 display: flex;

Capture Submitted Data

Capture Passwords

Warning:

Credentials are currently not encrypted. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

https://genshin.hoyoverse.com/crm/pc-launcher?lang=en-us&utm_source=email&utm_medium=crm&

Cancel

Save Page

Accedi al tuo account

Nome utente

Password

Accedi

Hai dimenticato la password?

Selezione target

Ho in seguito selezionato un target verosimile, in questo caso ho utilizzato me stesso, ed inserito quel target nella lista degli utenti a cui inviare mail

Edit Group

Name:

Test

+ Bulk Import Users

Download CSV Template

First Name

Last Name

Email

Position

+ Add

Show

10

entries

Search:

First Name

Last Name

Email

Position

Cristian

Girgenti

krissitzhere@g...

Player

Showing 1 to 1 of 1 entries

Previous

1

Next

Close

Save changes

Dopo aver fatto ciò, mi è rimasto soltanto da settare una campagna e cominciare ad inviare le mail

New Campaign

Name:

Hoyo

Email Template:

Hoyo1000Primo

Landing Page:

Copy of ScamHoyo

URL: ?

http://192.168.1.1

Launch Date

December 6th 2024, 4:16 pm

Send Emails By (Optional) ?

Sending Profile:

hoyoverse

Send Test Email

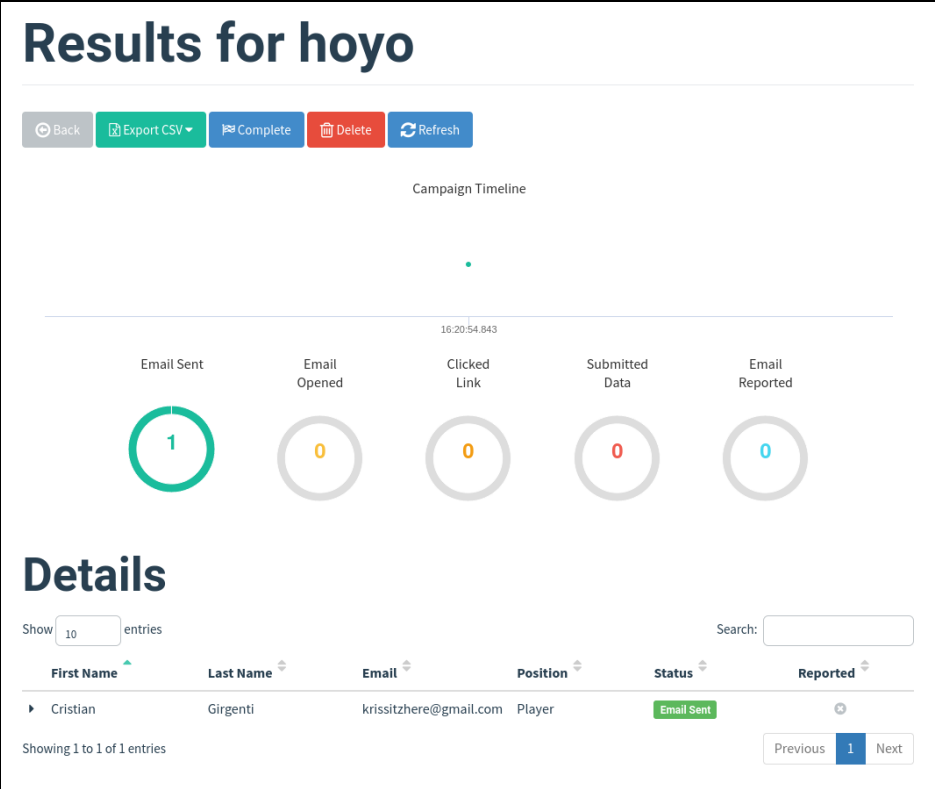
Groups:

× Test

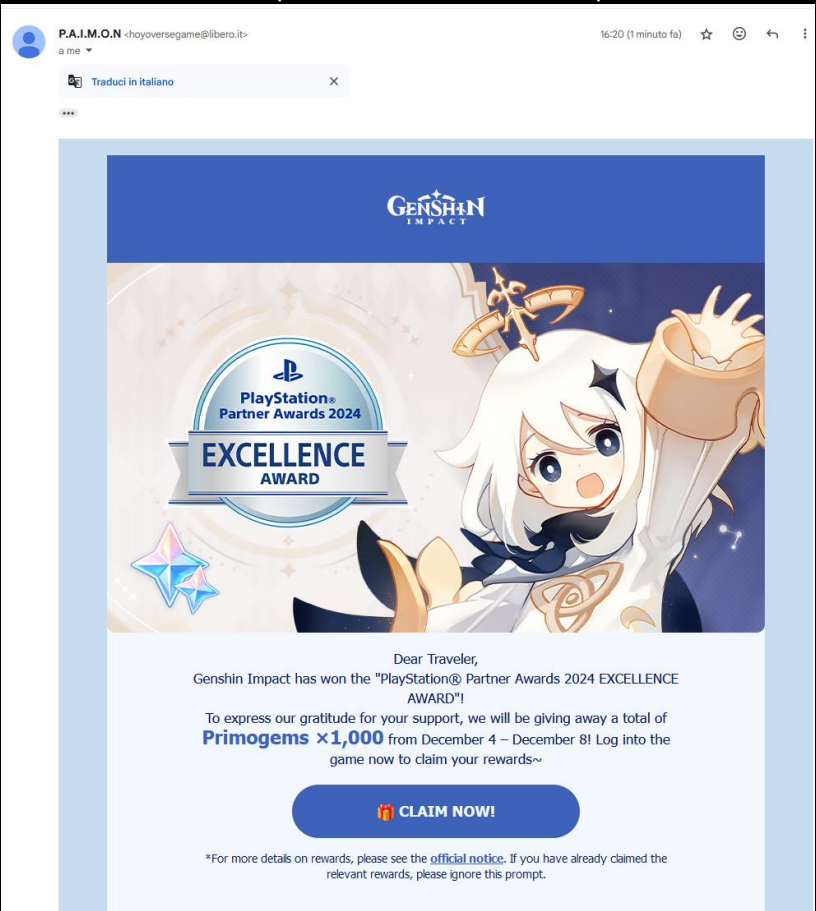
Close

Launch Campaign

Da questa schermata possiamo vedere che la mail è stata ricevuta



In seguito, controlliamo nella nostra mail e vediamo che è arrivato tutto tranquillamente, potremo anche notare che la mail risulta diversa, ed è quella che abbiamo scelto noi prima, nonostante il contenuto sia identico alla mail originale



Se l'utente clicca ingenuamente la mail, senza notare che la mail che lo invia non è credibile ed è diversa da quella originale, il risultato sarà questo:



Se l'utente decide di cliccare ed accedere per riscattare il bonus verrà reindirizzato a questo:

Accedi al tuo account

Nome utente

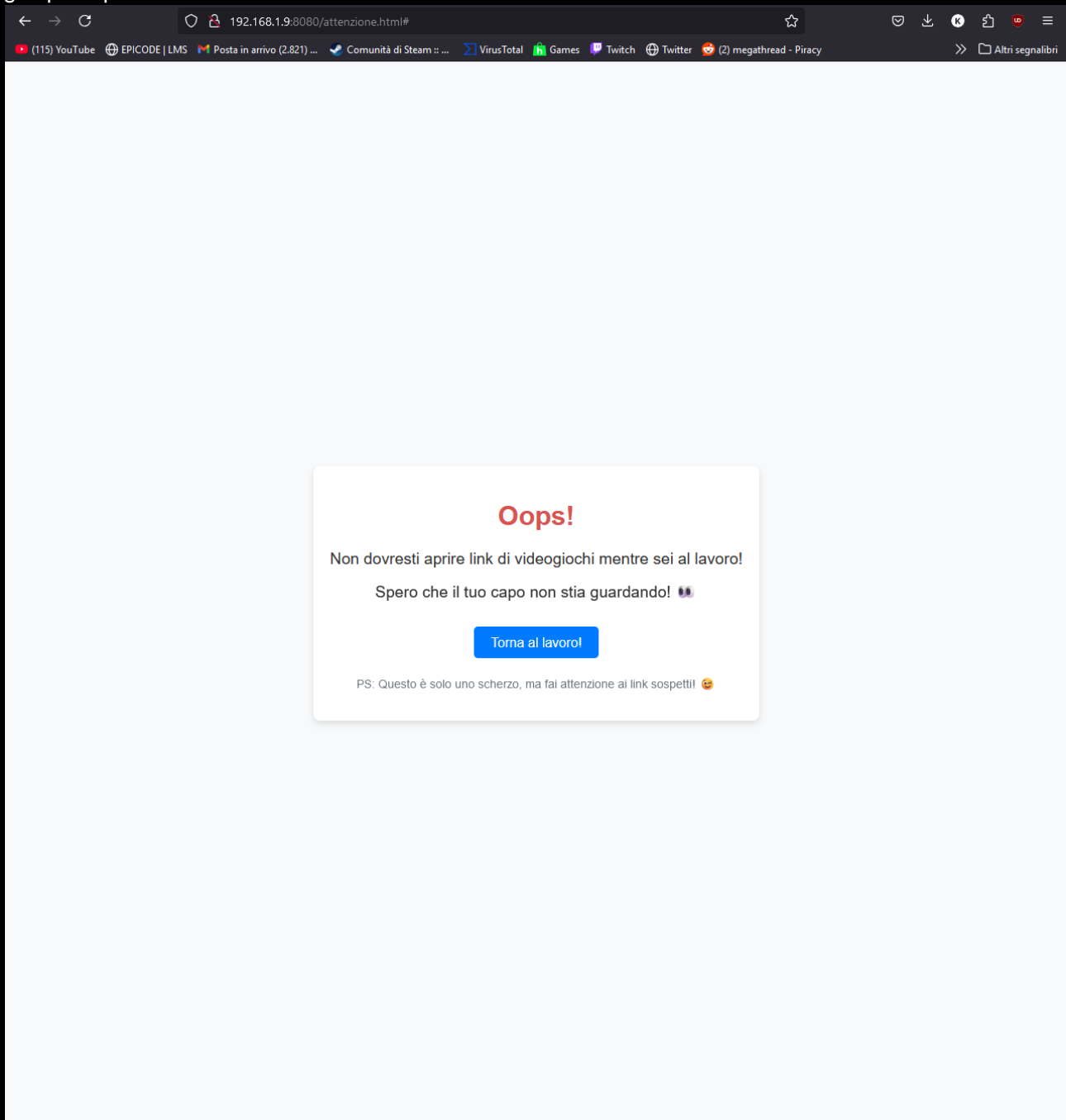
Password

Accedi

[Hai dimenticato la password?](#)

Un sito abbastanza evidente che non sia ufficiale, dovrebbe già far suonare tutti i campanelli d'allarme possibili. Ho testato con un indirizzo locale poiché non possedendo un dominio, creare un sito vero e proprio richiedeva molto più tempo per essere impostato bene, ed essendo solo un test va bene così

Infine, se l'utente decide di mettere password ed email, verrà reindirizzato ad una simpatica pagina che lo prende in giro per la poca cura che ha della sua sicurezza informatica



Grazie mille per l'attenzione!