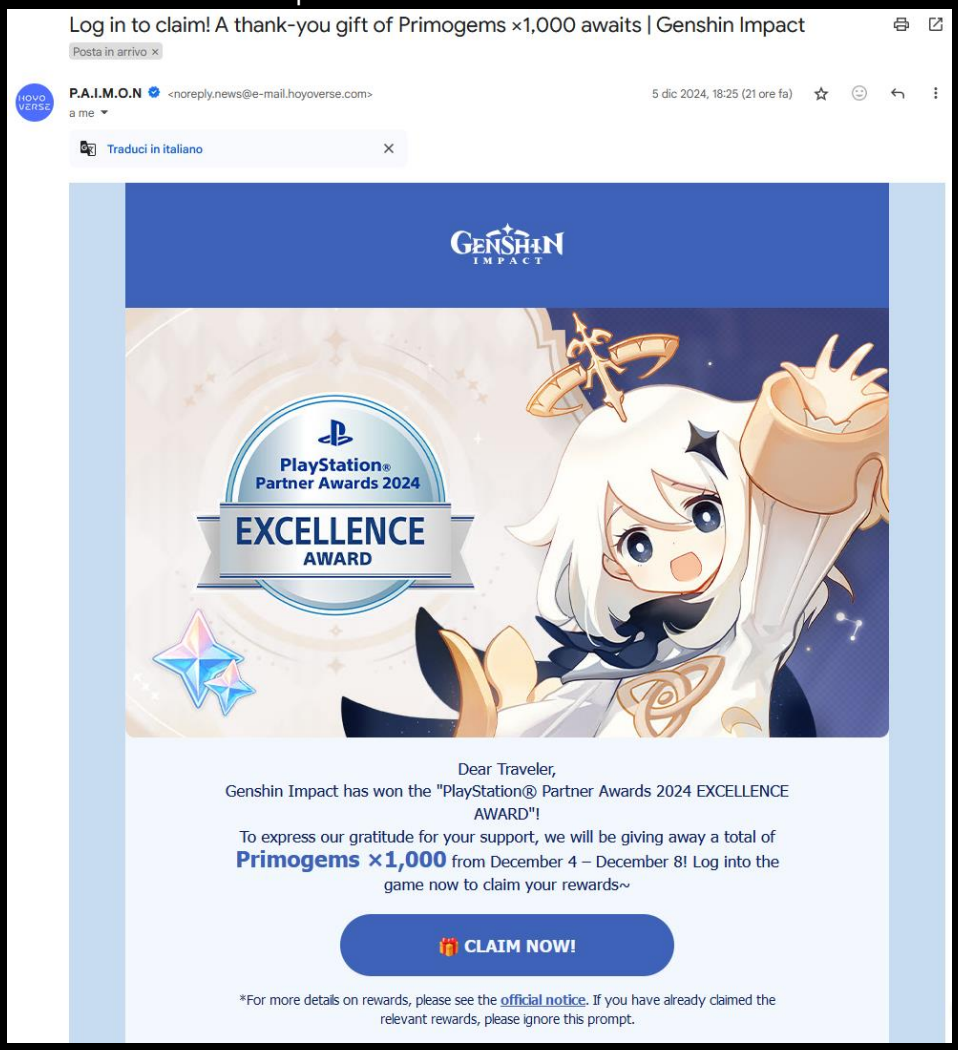
Relazione Test Email di Phishing

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:



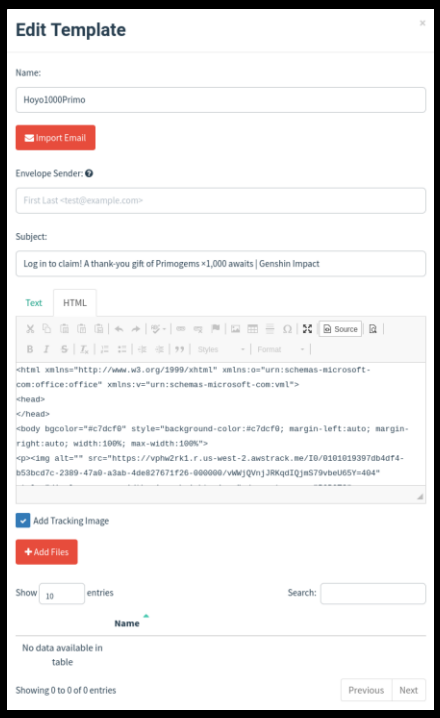
Ho preso il contenuto di questa mail e l'ho clonato, prendendo il file sorgente e sostituendo ogni link con un URL temporaneo(che sostituiró in seguito con un URL funzionante)

GoPhish

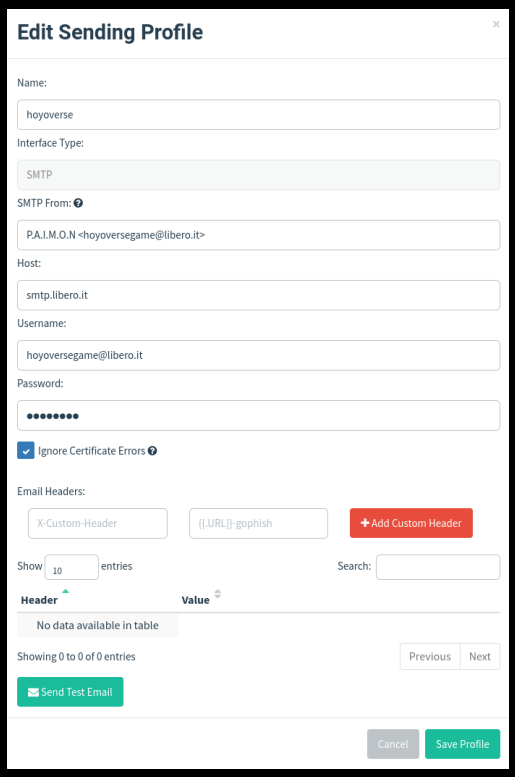
Dopo aver fatto questo, ho installato GoPhish sulla mia macchina, settando i vari parametri per permettere al servizio di inviare delle mail funzionanti, con un email creata appositamente per risultare "simile" a quella originale, ma abbastanza diversa da renderla riconoscibile ad un occhio attento.

Di seguito le varie impostazioni:

Contenuto della mail

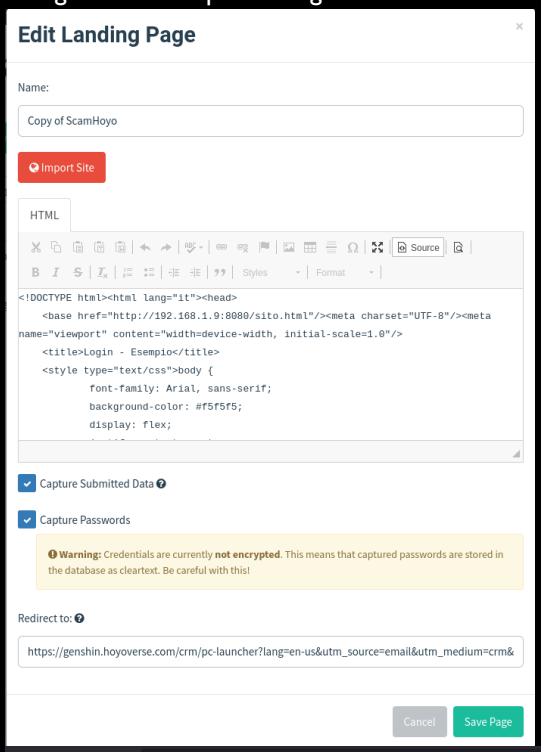


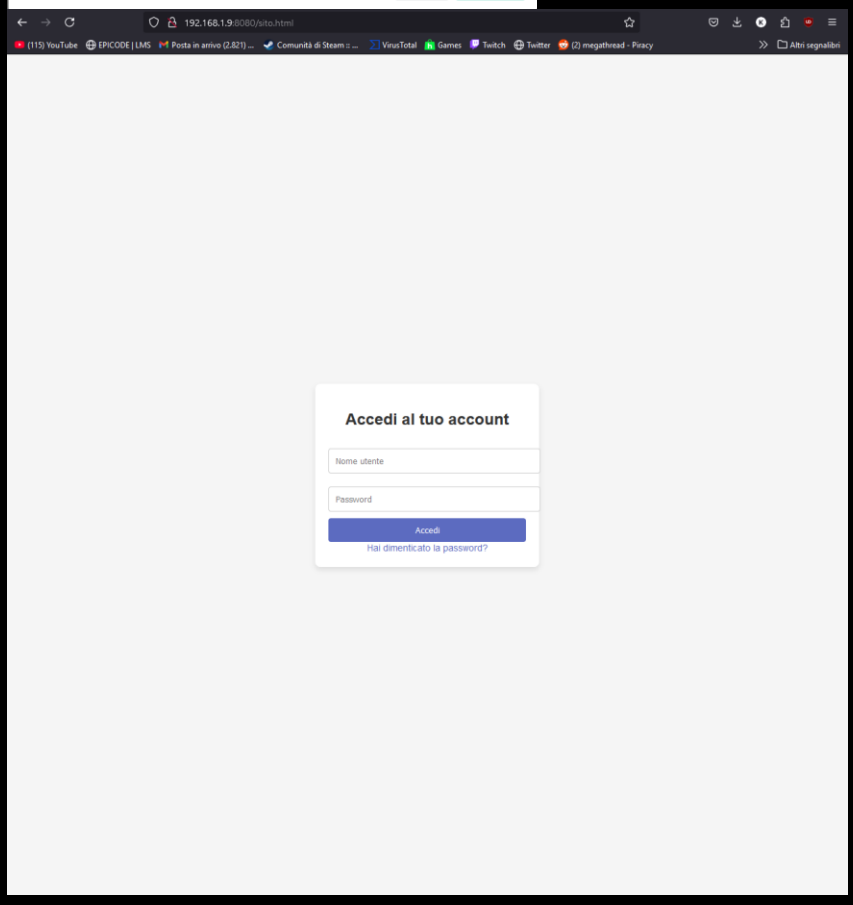
Mittente



Creazione pagina login

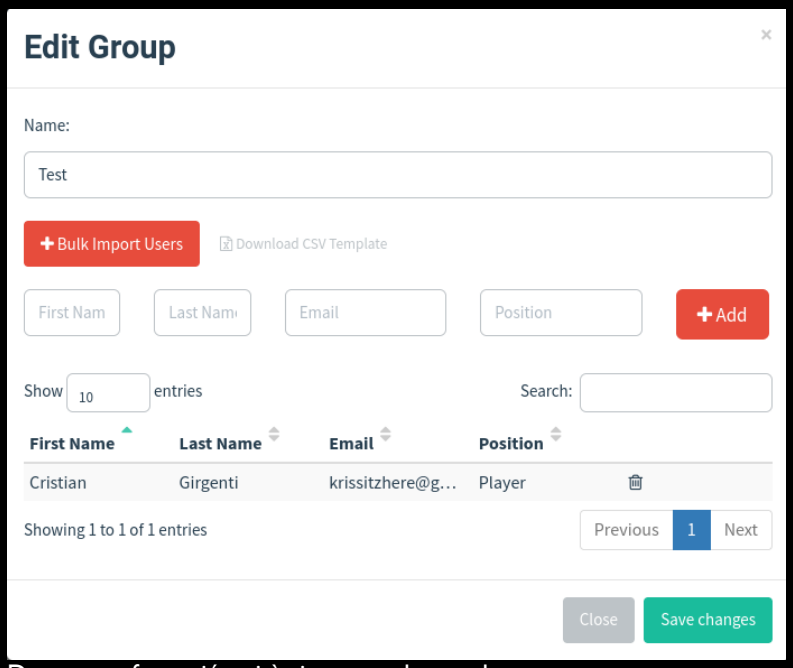
In seguito, ho creato una finta pagina di login dove l'utente ignaro veniva reindirizzato, invece del sito ufficiale, che ho in seguito hostato per testing su un indirizzo locale della macchina.



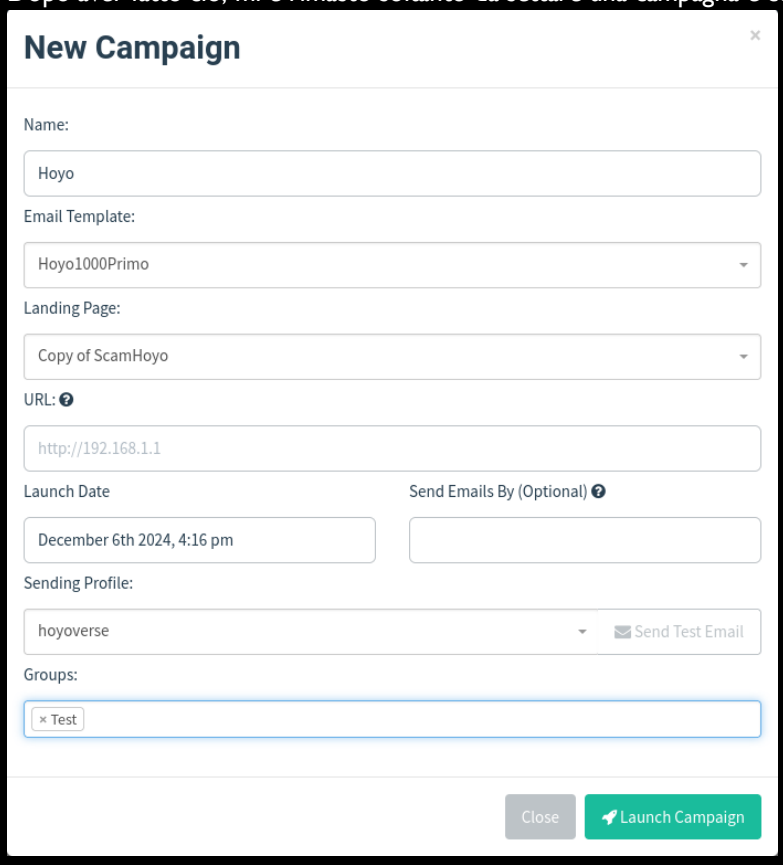


Selezione target

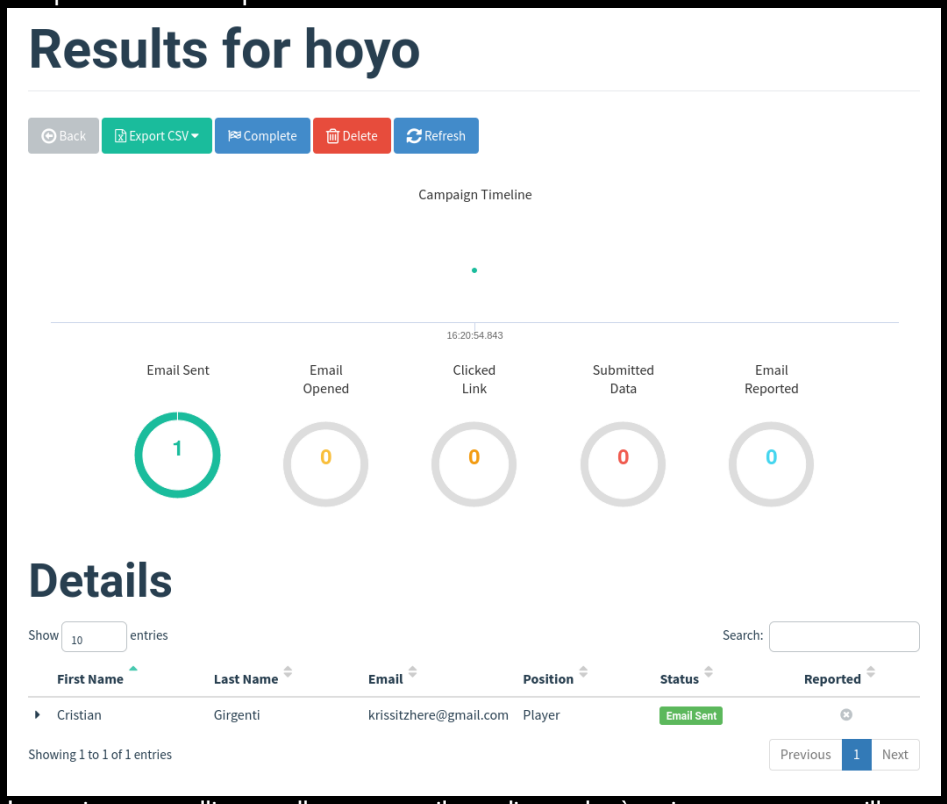
Ho in seguito selezionato un target verosimile, in questo caso ho utilizzato me stesso, ed inserito quel target nella lista degli utenti a cui inviare mail



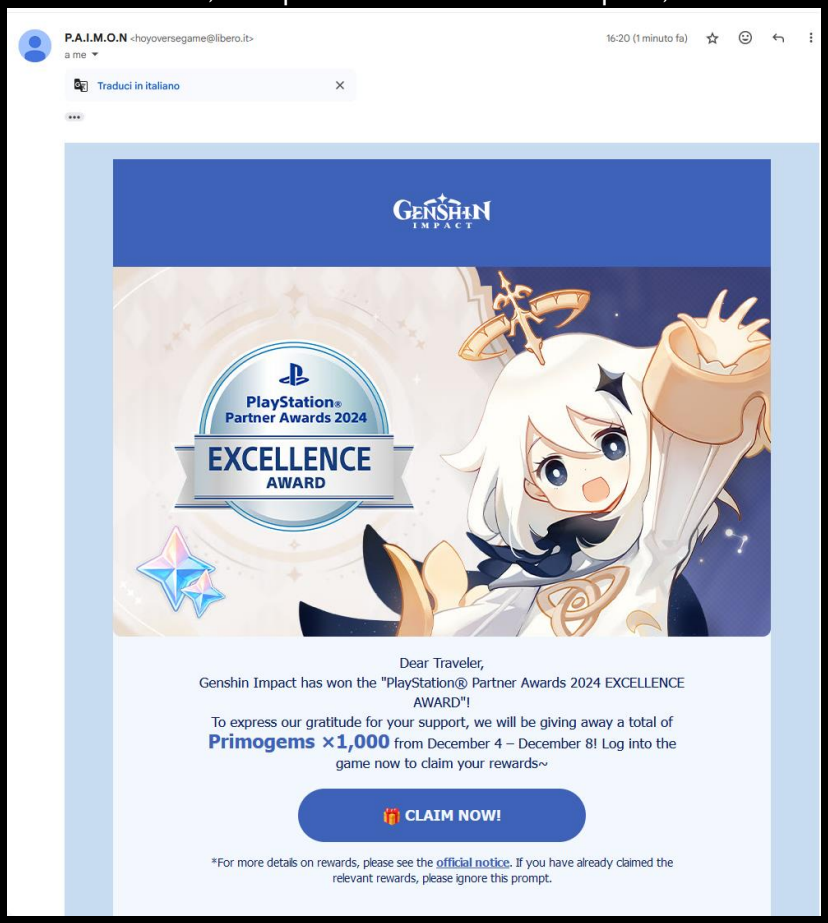
Dopo aver fatto ció, mi è rimasto soltanto da settare una campagna e cominciare ad inviare le mail



Da questa schermata possiamo vedere che la mail è stata ricevuta

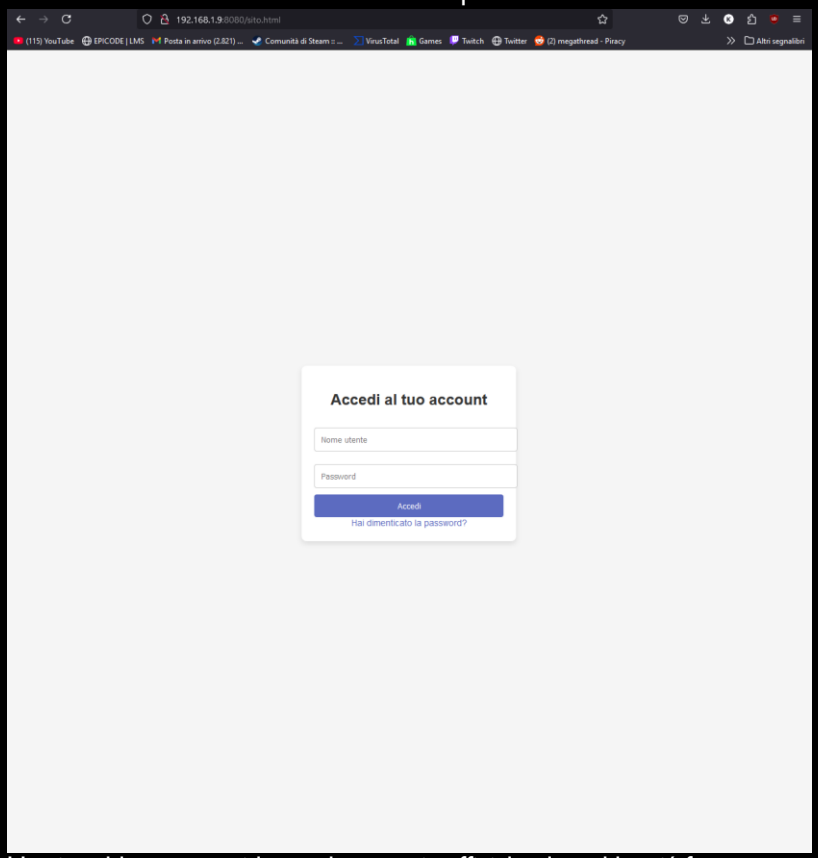


In seguito, controlliamo nella nostra mail e vediamo che è arrivato tutto tranquillamente, potremo anche notare che la mail risulta diversa, ed è quella che abbiamo scelto noi prima, nonostante il contenuto sia identico alla mail originale



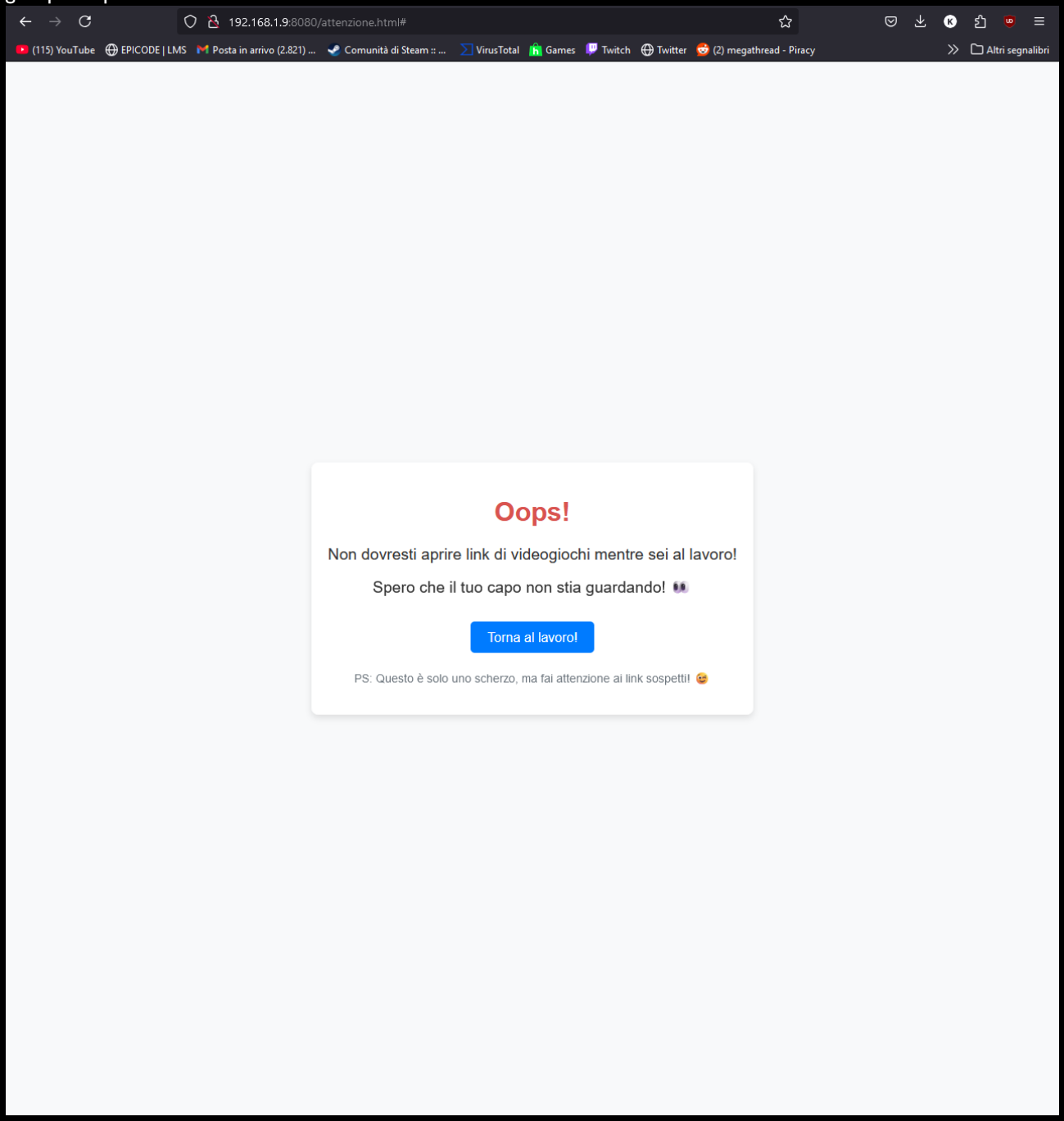
Se l’utente clicca ingenuamente la mail, senza notare che la mail che lo invia non è credibile ed è diversa da quella originale, il risultato sará questo:

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



Un sito abbastanza evidente che non sia ufficiale, dovrebbe giá 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 piú tempo per essere impostato bene, ed essendo solo un test va bene cosí

Infine, se l'utente decide di mettere password ed email, verrá 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!