Simulazione email di phishing

Introduzione

I tentativi di phishing oggigiorno sono diventati sempre più sofisticati e comuni, gli hacker sfruttano tecniche psicologiche come l'urgenza e la fiducia in figure note per ingannare le vittime e ottenere informazioni sensibili, come credenziali di accesso o dati finanziari.
Ho deciso di scrivere l'email in inglese per aumentarne la credibilità, poiché molte piattaforme internazionali (come Steam e Twitch) utilizzano prevalentemente l'inglese nelle loro comunicazioni.

1. Creare uno scenario

Lo scenario riguarda un'email di phishing basata su un giveaway organizzato da OhnePixel, uno streamer famoso di CS:GO. L'email è indirizzata a "Yummy", un giocatore assiduo di CS:GO, con l'obiettivo di convincerlo a reclamare una Steam Gift Card da 50€.

Obiettivo del phishing :
L'obiettivo principale è ottenere le credenziali di accesso dell'account Steam di Yummy. Questo viene fatto inducendolo a cliccare su un link falso che lo porta a una pagina di phishing dove viene richiesto di inserire le proprie credenziali.

2. Email generata da AI:

Subject: 🎁 OhnePixel has gifted you a 50€ Steam Gift Card – Claim it now before they're gone!

Body of the email:

Hi Yummy,

It's **OhnePixel** , the CS:GO streamer you love watching every day!

I want to thank you for your incredible support during my latest CS:GO case opening event. To show my appreciation, I've decided to gift you a **50€ Steam Gift Card** as part of my special giveaway!

But hurry: the gift card codes are **limited** and will be assigned on a first-come, first-served basis until they run out. **Act fast** , because they might be gone sooner than expected!

To claim your prize, click the link below within the next **24 hours** . After this period, the code will be reassigned to another winner:

Claim Your Prize

Important Note *: Before receiving your code, you'll need to verify your identity by logging into your Steam account via the official giveaway page. This step is mandatory to ensure the prize is delivered to the correct user.*

Once logged in, you'll receive detailed instructions on how to download your redemption code.

Remember : Make sure to use the same Steam account you used to participate in my last event to avoid any issues during verification.

If you need assistance, feel free to contact our support team at: support@ohnepixel-steam-giveaway.com

Thank you once again for your amazing support! I hope you enjoy your new Steam balance!

Catch you soon on my channel,

OhnePixel

P.S.: Don't forget to follow me on Twitch to stay updated on future giveaways!

3. Descrizione dello scenario

Nel nostro caso, Yummy riceve un'email apparentemente legittima da OhnePixel, uno streamer popolare di CS:GO, che annuncia un giveaway di una Steam Gift Card da 50€. La mail include elementi convincenti come il nome di OhnePixel, un contesto specifico (un evento di apertura di casse), e un senso di urgenza per spingere Yummy ad agire rapidamente.

Perché l'email potrebbe sembrare credibile alla vittima :

1. **Familiarità con OhnePixel** : Yummy è un giocatore attivo di CS:GO e probabilmente segue streamer famosi come OhnePixel. Il riferimento diretto all'evento di apertura di casse rende la mail plausibile.
2. **Giveaway comune nel mondo gaming** : Gli giveaway sono frequenti tra gli streamer, quindi il giocatore potrebbe trovare naturale ricevere un'email del genere.
3. **Urgenza e scarsezza** : La combinazione di tempo limitato ("entro le prossime 24 ore" e "codici limitati") crea un senso di urgenza, inducendo Yummy a cliccare sul link senza riflettere troppo.
4. **Procedura di verifica** : Richiedere di accedere con l'account Steam per verificare l'identità sembra una procedura legittima, simile a quelle utilizzate da molte piattaforme online.
5. **Call-to-action chiaro** : Il bottone "Claim Your Prize" è facile da individuare e invita direttamente all'azione.

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

1. **Indirizzo email del mittente** : Se Yummy controlla attentamente l'indirizzo email del mittente, potrebbe notare che non proviene da un dominio ufficiale di Steam o di OhnePixel (es. **support@ohnepixel-steam-giveaway.com** vs. **@steam.com** o **@twitch.tv**).
2. **Dominio del link** : Il link fornito (**https://ohnepixel-steam-giveaway.com/redeem**) potrebbe contenere piccole variazioni rispetto ai domini ufficiali di Steam o Twitch. Un utente attento potrebbe riconoscere che il dominio è fittizio.

3. **Richiesta di credenziali** : Una piattaforma legittima come Steam non chiederebbe mai le credenziali tramite un'email. Questo è un segnale di avvertimento evidente.
4. **Mancanza di personalizzazione completa** : Sebbene il nome utente di Yummy sia incluso nell'email, altre informazioni personalizzate (come il nickname usato durante l'evento) potrebbero mancare, rendendo il messaggio meno convincente su un esame più attento.
5. **Supporto fittizio** : L'email fornisce un indirizzo di supporto (**support@ohnepixel-steam-giveaway.com**), ma questo potrebbe essere facilmente falsificato. Un utente attento potrebbe cercare il supporto ufficiale di OhnePixel o Steam e scoprire che non esiste.
6. **Assenza di marchi ufficiali** : Una mail legittima avrebbe probabilmente incluso loghi ufficiali di Steam o Twitch, firmature autentiche e collegamenti diretti ai siti ufficiali.

4. Campagna di Phishing

Dopo aver creato lo scenario e l'email di phishing, ho proceduto con la configurazione della campagna utilizzando **GoPhish** , una piattaforma open-source per simulare attacchi di phishing in ambito educativo.

Configurazione della Campagna

1. **Template Email** :
    a. Ho importato il template HTML dell'email generato in precedenza, assicurandomi che tutti gli elementi visivi (loghi, stili, ecc.) fossero coerenti con quelli di Steam e OhnePixel.
    b. Tutti i link del call-to-action puntano alla landing page phishing creata.

🎁 OhnePixel has gifted you a 50€ Steam Gift Card!

Hi Yummy,

It's **OhnePixel**, the CS:GO streamer you love watching every day!

I want to thank you for your incredible support during my latest CS:GO case opening event. To show my appreciation, I've decided to gift you a **50€ Steam Gift Card** as part of my special giveaway!

But hurry: the gift card codes are **limited** and will be assigned on a first-come, first-served basis until they run out. **Act fast**, because they might be gone sooner than expected!

To claim your prize, click the link below within the next **24 hours**. After this period, the code will be reassigned to another winner:

Claim Your Prize

Important Note: Before receiving your code, you'll need to verify your identity by logging into your Steam account via the official giveaway page. This step is mandatory to ensure the prize is delivered to the correct user.

Once logged in, you'll receive detailed instructions on how to download your redemption code.

Remember: Make sure to use the same Steam account you used to participate in my last event to avoid any issues during verification.

If you need assistance, feel free to contact our support team at:

Thank you once again for your amazing support! I hope you enjoy your new Steam balance!

Catch you soon on my channel,
OhnePixel

P.S.: Don't forget to follow me on Twitch to stay updated on future giveaways!

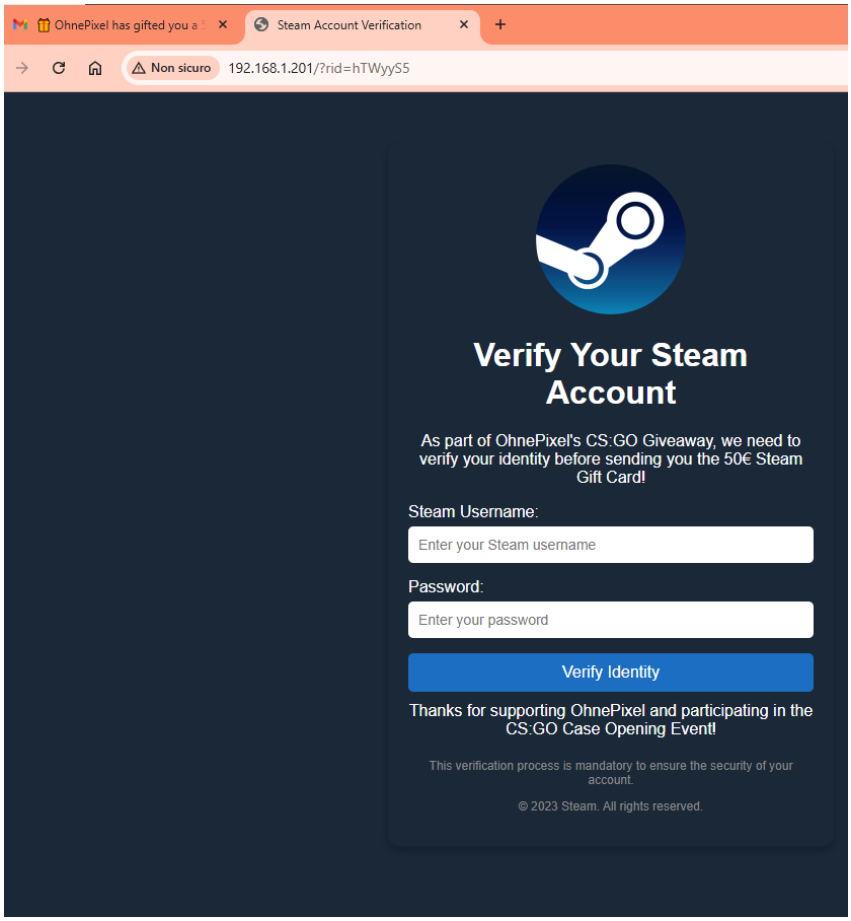
2. **Landing Page** :
    a. Con l'aiuto dell'IA ho progettato una landing page che mimica l'aspetto ufficiale di Steam, con riferimenti al giveaway di OhnePixel e all'evento di apertura di casse di CS:GO.
    b. La landing page includeva un form per la raccolta delle credenziali (username e password) senza specificare un redirect esplicito, lasciando che GoPhish gestisse automaticamente i dati inviati.
3. **Gruppo di Destinatari** :
    a. Ho creato un gruppo di destinatari contenente l'indirizzo email di Yummy, il giocatore target della simulazione(in questo caso la mia mail).
    b. L'email è stata personalizzata inserendo il nome utente "Yummy" nel corpo del messaggio per aumentarne la credibilità.
4. **Invio della Mail** :
    a. Ho configurato il server SMTP in GoPhish per inviare l'email usando un indirizzo fittizio ma plausibile (ohnepixel@giveaway.com)
    b. L'email è stata inviata a seguendo tutte le istruzioni precedentemente definite.

5. Risultati della Campagna

Comportamento della Vittima

- **Accesso alla Landing Page** : Dopo aver cliccato su un link qualsiasi, vengo reindirizzato alla landing page phishing, dove è stato invitato a verificare la sua identità inserendo le credenziali Steam.

- **Inserimento delle Credenziali :**



Dati Raccolti

- **Username** : **Yummy**
- **Password** : **Yummy123**

Tutti i dati sono stati registrati automaticamente su GoPhish.