Category:

MISC

Name:

SNS investigation

Message:

Welcome to SNS investigation, an OSINT challenge that will test your detective skills on social media. One X account, @Mark54666780228, has recently come under suspicion for its involvement in cryptocurrency fraud on SNS (https://x.com/Mark54666780228). Your task is to dive deep into this account's activities to discover subtle hints leading to the personal information that could link to the actual account holder. Find the following information to form the flag:

1) Identify the mail address associated with this account.
2) Determine the Skype username associated with the mal address.
3) Find out the domain of the website which this person promotes online.

Flag Format : CSG_FLAG{mail_address:Skype_username:domain}

Note that the letters in curly brackets are all in small case;

e.g. CSG_FLAG{foo@example.com:john123: xxx-yyy.com}

Hints:

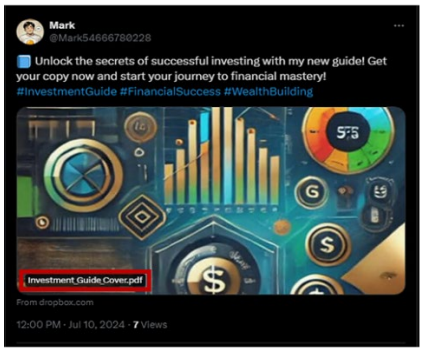
- Found that PDF on Dropbox yet? Don't let those blacked-out blocks fool you. Try converting it to something more flexible... You might just be able to slide those secrets right out!
- Got an email address? Look closer at that quirky alias. With a little OSINT magic, pivoting on that alias could lead you to other social media accounts. Who knows what else you might uncover?

Objective:

Your task is to reveal information around one suspicious SNS account that could link to the actual account holder. This requires fundamental investigative skill on social media.

Instructions:

1. If you don't have X account, create an account prior to the investigation. As you sift through the tweets, you will come across a tweet containing a Dropbox link. Download the PDF file from this link. The downloaded PDF will feature blacked-out sections intended to obscure sensitive information.



2. To potentially reveal the hidden details, convert the PDF to a PowerPoint file using any tools like Adobe's online conversion tools. If done correctly, this might allow you to remove the black masks and discover a hidden email address behind it (hiropi1991tanapon@gmail.com).
3. Utilize the uncovered email address to search for associated Skype details. This could involve using any OSINT tools such as EPIEOS.
4. Employ the unique string from the email address, "**hiropi1991tanapon**", to search for additional social media footprints. According to one of the tweets, the account holder shows interests in opening a YouTube channel. It leads us to a YouTube channel, which uses the same alias as the mail address (https://www.youtube.com/**@hiropi1991tanapon**). Examine the channel's description carefully to find the domain of a website promoted by this account.

In an OSINT investigation, pivoting on a characteristic alias can be an effective strategy for discovering other social media accounts operated by the same individual, thereby expanding the scope of the search.

Flag is:

CSG_FLAG{hiropi1991tanapon@gmail.com:enj0y555crypt0:h00r@y-g00d-j0b.com}

References:

- EPIEOS (https://epieos.com/)
- PREDICTA SEARCH (https://www.predictasearch.com/)
- VEDBEX (https://www.vedbex.com/tools/email2skype)