Cybersecurity Digest

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Volume 1, Issue 5

Newsletter Date: 15-11-2024

PIG-BUTCHERING SCAM

A pig-butchering scam is a type of investment fraud that lures individuals into investing their money in seemingly legitimate and profitable ventures. Typically, the scammers promise high investment returns within a short period. Pig-butchering scammers often use fake images and impressive-yet-fraudulent investment portfolios to convince victims of the legitimacy of their schemes. Once victims are hooked and have invested a significant amount of money, the scammers suddenly disappear, leaving victims with no way to recover their funds. The term ["pig butchering"]() is derived from the idea that the scammers fatten up their victims with the promise of lucrative returns before "slaughtering" them for their money.

Pig Butchering Scam

The scam often begins with a seemingly innocent chat initiated by a random person. The scammer might claim to have received the victim's number from a mutual friend, while also appearing unsure if they have the correct number. However, this is just an act to engage the victim in conversation. Scammers have also been known to use images of attractive people to lure victims, preying on their desire for companionship or romance to build trust and establish a connection.

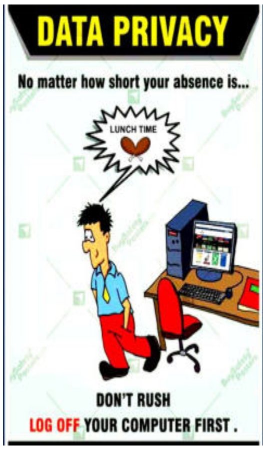
As the conversation progresses, the scammer gradually introduces the victim to the fake investment scheme and promises significant profits within a short period if the victim invests a certain amount. Unfortunately, many victims fall for this fraudulent scheme due to the scammers' persuasive tactics and convincing appearance of legitimacy.

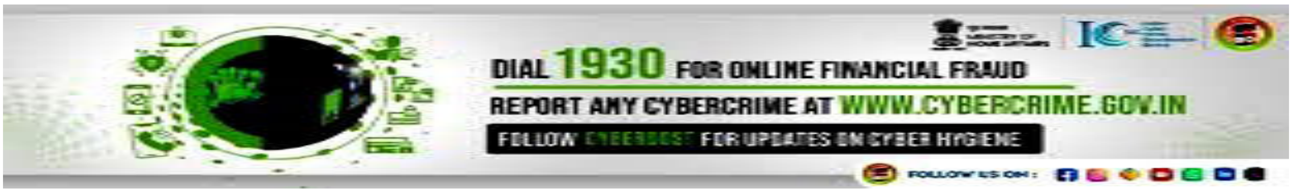
Inside this issue:

The Group Chat Strategy

By adding multiple people to chat groups that are centered around investment discussions, scammers can quickly gauge the interest of their targets. Those who remain in the group are more likely to be interested in investing, making them prime candidates for the scam. On the other hand, individuals who leave the group are either aware of the scam or are uninterested in investing. Hence, they are less likely to be persuaded by the scammer's tactics.

The scammers consist of a group of individuals with different roles and objectives. Some of the chat group members are fake profiles created by the scammers themselves to make the group seem more authentic. This approach makes the process for scammers easier, enabling them to focus their effort on individuals who are more susceptible to their fraudulent schemes. It also creates an environment that promotes a sense of community and social validation, as potential victims would see that other people are engaging in discussions about investment and are not calling out the scam.

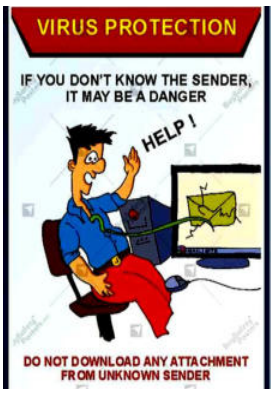


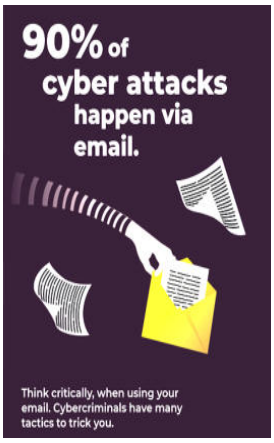


Saving victims from falling prey to pig-butchering

Given the alarming trends and the growing sophistication of pig-butchering scams, it is crucial for individuals to take proactive steps in safeguarding their investments and personal information. The following recommendations are designed to help individuals recognize the warning signs of these scams and take appropriate action:

1. **Be cautious of unsolicited messages and group chats.** As previously discussed, scammers often initiate contact through seemingly innocent chat messages or by adding individuals to investment-themed group chats. Be wary of engaging with strangers and carefully consider the source of any unsolicited messages or group chat invitations.
2. **Verify the legitimacy of brokerages.** Before investing your money, make sure that you conduct a thorough investigation of the brokerage you're considering. Check for recently created domains via registration data or news articles. If something seems suspicious, trust your instincts and avoid engaging with the platform.
3. **Monitor identity theft resources for leaked personal information.** Be vigilant about the security of your personal information. Regularly check or sign up for reputable identity theft monitoring services to track any leaks or breaches involving your data and take appropriate steps to secure your information if needed.
4. **Be skeptical of high investment returns with low risks.** If an investment opportunity promises high returns with minimal risk, it is likely too good to be true. Always research and verify investment opportunities before committing your money.
5. **Educate yourself about emerging tactics.** Stay informed about the latest strategies employed by scammers, such as the use of group chats and fake brokerages. By understanding how these scams work, you can better recognize the warning signs and avoid becoming a victim.
6. **Report suspicious activity.** If you encounter a potential pig-butchering scam, report the incident to law enforcement. Your report could help prevent others from falling victim to the same scam. If you have already transferred funds to fake brokerage websites, it is best to report this as soon as possible to potentially recover them.





Cyber Crime News

- Cyber crimes: 4.5 lakhs 'mule' accounts frozen, many in public sector banks - ***The Indian Express***.
- Incidents of cyberattacks in India may reach 17 trillion by 2047: Study - ***The Hindu***.
- Indians lose ₹ 1.5 lakh to cyber criminals every minute: Official – ***The Hindu***.
- Cyber Fraudsters impersonate TRAI officials, MHADA employee scammed of ₹ 3 lakh in digital arrest scheme –***The 420.in***
- Class XI "influencer" student scams 200 Instagram followers with a fake investment scheme - ***The Indian Express***.