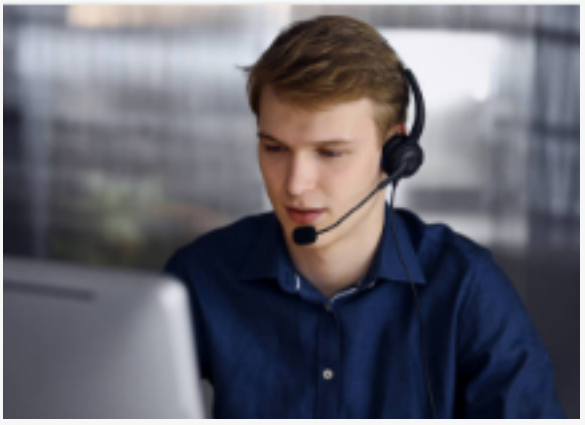
Scammers exploit human emotions in social engineering scams - Cyber-Forensic.net explains the tricks

Scammers are using all sorts of techniques in social engineering scams to lure their victims into giving them personal information.

Cyber-Forensics.net



best crypto recovery service

SOFIA, BULGARIA, July 18, 2022 /EINPresswire.com/ -- Social engineering scams are woven around users' behavior. Once the fraudster knows how a particular user behaves and reacts in certain situations, they devise an apt method to dupe the victim.

These scammers thrive on the behavior patterns of people. For instance, according to a Microsoft blog, around scams, 48% of people will give out their password just for a piece of chocolate. This behavior makes users very prone to phishing scams.

Fear and greed are the two prevalent emotions used by scammers frequently. Scammers know that getting a pop-up notification telling their security is compromised will create fear and a sense of urgency. Scammers use this fear to get the money out of the victim's pocket. In almost all lottery scams, human greed to earn quickly is exploited. The promise of quick money makes people share passwords and credit card details.

Let's take a look at the top social engineering scam techniques:

1. Phishing is the fraudulent practice inducing individuals to give their personal information by posing as an authority.

Phishing attacks are usually displayed as warning calls/pop-us, which creates fear in the user. They take actions such as clicking on the bogus website or sharing other personal information to fix the problem.

2. Pretexting: Pretexting is impersonation but very subtle and sophisticated. It intends to convince the victim to do something they wouldn't normally do. The attacker sends a text, makes a phone call, or composes an email and pretends that he's from the bank, another

> If we look at the patterns of social engineering scams, we can see how victims' heightened emotions and trust are used to create a sense of urgency in the scam."
>
> *Timothy Benson*

organization, or even one of the victim's friends. Recently scammers stole data from the revenue department and called by impersonating an IRS officer. They asked residents to file taxes and threatened police action if they did not send them money. Of course, the funds are directed to a fake IRS bank account, not a real one.
In this case, a fear of authority is evoked in the individual to take instant action.

3. Baiting: In baiting, scammers use victims' greed and curiosity by promising or offering freebies such as a free book, course, or film, so that the user receives a freebie, the victim is prompted to type in sensitive info to a website that looks legitimate but is bogus.

4. Romance Scam: A romance scam is when the scammer pretends to have a romantic relationship with the victim before trying to get money in various means. They either ask for the money directly, or introduce a third party, or often claim to know an insider that can help. In essence, scammers use love as a tool to get into the victim's trust and pockets.

"When we observe social engineering patterns, we note that that heightened emotions of the victim are used against them, in order to create urgency, a key ingredient to getting people to behave irrationally in a fraud. Practice, awareness and mindfullness seem to be the only only way to prevent this," says Timothy Benson, a cyber analyst at Cyber-Forensics.net.

What to do if scammed through any social engineering scam technique?

It is common for people to fall into scams, even if they have all the information about how fraud happens. Scammers clear their way through red flags and head out to do cons after creating a trustworthy setting. So, if someone falls prey to scams, they should:

 Secure their online payment options: Be it cards, net banking, or any mobile pay, once scammed, one should always secure their online payment options. This is done either by blocking the payment method or discarding it altogether.
 Modifying online credentials: As everything is digital, credentials are the only way to access someone else's account. Victims of scams should modify their online credentials to a more robust version.
 Report the scam: Nothing can be initiated without reporting the scam. One must report the scam to concerned authorities like banks or police,
 Contact fund recovery services: Legal battle to get back money is exhausting, and one might not even know the complete procedure for digitally recovering lost crypto and other forms of money. Fund recovery services can help victims along the process and present a strong case on

their behalf to ensure victory.

How do fund recovery services help?

A fund recovery service, like Cyber-Forensics.net, has a team of professionals. Cyber Forensic's goal is to recover the victim's money lost due to fraud with the help of the latest technology and to provide the most up-to-date and effective fraud detection and prevention.

They provide tracing software and other blockchain technologies to recover money. If needed, Cyber-forensic.net, with the help of lawyers and authorities, may run a honeypot scam to catch the fraudsters.

Additionally, they have the experience to depict how the scam happened and present it as a strong case. A victim must only find a reliable and proven fund recovery service, or they may fall victim to recover money scam.

About Cyber-Forensics.Net:

Cyber-Forensics.Net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.Net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. Touted as the best crypto recovery service, they can be reached for more information at https://cyber-forensics.net.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here
Visit us on social media:
Twitter
