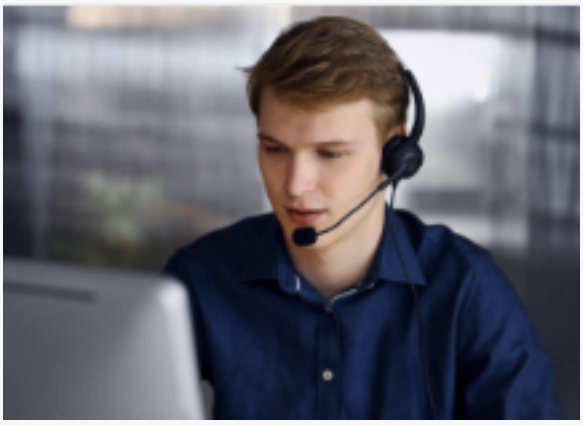
Scammers creating fake scenarios to steal data: Cyber-Forensics.net urges to pause, think, and act

Pretexting is where fraudsters create a believable scenario around their scam with an ultimate aim to extract information and money.



Cyber Forensic Specialist

Cyber-Forensics.net

SOFIA, BULGARIA, February 28, 2022 /EINPresswire.com/ -- In cybercrime, social engineering is one of the most common techniques used by cyber crooks to target individuals. Many forms of social engineering attacks like phishing, smishing, vishing, and spear-phishing are used to manipulate people into supplying sensitive data, bank credentials, or access to secure networks.

According to the latest reports, a newly refined version of this social engineering attack called Pretexting is becoming a personal favorite of fraudsters.

Cyber-Forensics.net, a leading cyber forensics service for online victims, reveals that a pretexting attack involves scammers impersonating someone with an authoritative voice to gain the trust of the potential targets. They create a fake scenario to make the case sound genuine and deceive people into giving information.

Chief fraud recovery specialist Timothy Benson at Cyber-Forensics.net recently analyzed a case where a father and his daughter mentioned receiving an SMS presumably from their bank. The SMS inquired whether the account holder had authorized a $5,000 payment. The message asked the account holder to reply "Yes" or "No" or press 1 to decline future fraud alerts.

When the account holder typed No, scammers immediately called pretending to be from the fraud department. The fraudster then asked the potential victim to secure his account by providing bank information first. The father sensed something was amiss and disconnected the call.

Luckily, the father-daughter duo escaped the fraud by a close call.

> Consumers need to become aware of potential cybersecurity threats and take measures to protect critical assets and increase security."
>
> *Timothy Benson*

But contrary to this, millions of account holders either fail to identify what could be a suspicious call or a suspicious email? As a result, they fall victim to pretexting attacks.

Pretexting is not the only way scammers attack potential victims. Today, crooks are turning to hybrid forms of cyber-attacks. They combine multiple forms of cheating to blast out information from people.

They use a mix of phishing and smishing methods to send suspicious emails and immediately call anyone who responds.

Cyber expert Timothy Benson, who has spent years studying pretexting attacks, mentions: "consumers need to become aware of potential cybersecurity threats and take measures to protect the critical assets and increase security."

What can be done to avoid becoming victims of Pretexting attacks?
A few measures can help consumers stay away from such fraudsters such as:

Pause, Think, and Act: People often become victims of an attack when they give in to the urgency created by scammers and respond immediately. On the contrary, practice patience to pause for a moment, think about the outcomes, and act after investigating.

Gather information about prevalent forms of online attacks: As per the accounts given by pretexting attack victims, scammers may employ a combination of methods to create a believable scenario to deceive targets. Timothy Benson adds, "Pretexting attacks are successful when individuals are unaware of the techniques used by attackers."

Here are some common techniques used by attackers:

Phishing: Involves sending fraudulent or compromised email links from reputable and trustworthy sources.

Smishing: This technique employs SMS text messages to trick victims into sharing personal information.

Vishing: Scammers try to dupe potential victims into handing over confidential information over Phone calls.

Gather Information on How Pretexting Attacks Are Made:

Online platforms are becoming common mediums to launch such attacks as it is often easier to

hide identities. But, cannot implement any pretexting attack without creating-

A plausible situation: Scammers build a series of believable events designed to extract information. Keep a check when a story begins to sound heightened or a message too detailed or less detailed. The initial information usually provides an answer to the chosen pretext by scammers.

A character: The fraud involves the social engineers assuming a role much like an actor and impersonating any fictitious character. But it is important to consider aspects of that character, like how they made initial contact with the target.

Question the suspicious callers:

A scammer usually acts abnormally when the listener begins questioning their intent. Thus, listen to pretext created carefully before responding to sent messages or clicking email links.

Report the matter and Spread the word:

Chris Tapin from the Verizon Threat Research Advisory Center believes that security professionals often face "decision paralysis" when individuals do not report data breaches. Tappin further adds to the statement- "organizations need to educate individuals about malicious activities and respond to them when they see something suspicious."

For example, users receiving unexpected emails or SMS should immediately report the case to superiors.

What to do when a pretexting attacker steals money?
In most cases, the primary purpose of pretexting attacks is to steal personal information with an ultimate goal to steal money. And if one has lost money, the aim would be to get it back, which is called fund recovery in legal terminology.

However, the main problem in fund recovery comes when the online victims do not know the source of the attack. Failing to collect enough evidence leads to building a weak case. To avoid this, pretexting attack victims can take help from cyber experts.

A dedicated team of professional investigators can track the attack's origin, the medium, device IP addresses, and other details. This helps in allowing victims to claim that the fraud took place without their knowledge and makes them eligible for fund recovery.

Thus, choosing a credible and experienced fund recovery specialist team is essential. Thousands of pretexting attack victims recommend Cyber-Forensics.net as a credible agency.

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. Cyber-Forensics.net commonly deals with bitcoin scams and forex withdrawal problems. For more information, please visit https://cyber-forensics.net/.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here
