Cybersecurity Digest

Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

MEGHALAYA RURAL BANK

Volume 3 Issue 4

Date:16-05-2026

SOCIAL ENGINEERING

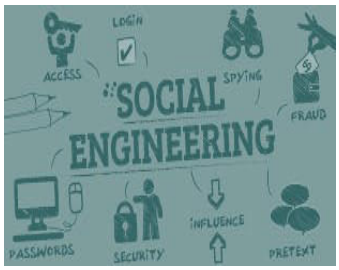
Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.

In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren't aware of certain threats like drive-by downloads.

Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

Generally, social engineering attackers have one of two goals:



Sabotage: Disrupting or corrupting data to cause harm or inconvenience.

Theft: Obtaining valuables like information, access, or money.

HOW DOES SOCIAL ENGINEERING WORK?

Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data. The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows:

Prepare by gathering background information on you or a larger group you are a part of.

Infiltrate by establishing a relationship or initiating an interaction, started by building trust.

Exploit the victim once trust and a weakness are established to advance the attack.

Disengage once the user has taken the desired action.

This process can take place in a single email or over months in a series of social media chats. It could even be a face-to-face interaction. But it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware.

It's important to beware of social engineering as a means of confusion. Many employees and consumers don't realize that just a few pieces of information can give hackers access to multiple networks and accounts. By masquerading as legitimate users to IT support personnel, they grab your private details like name, date of birth or address. From there, it's a simple matter to reset passwords and gain almost unlimited access. They can steal money, disperse social engineering malware, and more.

TRAITS OF SOCIAL ENGINEERING ATTACKS

Social engineering attacks center around the attacker's use of persuasion and confidence. When exposed to these tactics, you are more likely to take actions you otherwise wouldn't.

Among most attacks, you'll find yourself being misled into the following behaviors:

Heightened emotions : Emotional manipulation gives attackers the upper hand in an any interaction. You are far more likely to take irrational or risky actions when in an enhanced emotional state. The following emotions are all used in equal measure to convince you.

- Fear
- Excitement
- Curiosity
- Anger
- Guilt
- Sadness

Urgency: Time-sensitive opportunities or requests are another reliable tool in an attacker's arsenal. You may be motivated to compromise yourself under the guise of a serious problem that needs immediate attention. Alternatively, you may be exposed to a prize or reward that may disappear if you do not act quickly. Either approach overrides your critical thinking ability.

Trust: Believability is invaluable and essential to a social engineering attack. Since the attacker is ultimately lying to you, confidence plays an important role here. They've done enough research on you to craft a narrative that's easy to believe and unlikely to rouse suspicion.

How to Spot Social Engineering Attacks

Defending against social engineering requires you to practice self-awareness. Always slow down and think before doing anything or responding.

Attackers expect you to take action before considering the risks, which means you should do the opposite. To help you, here are some questions to ask yourself if you suspect an attack:

Are my emotions heightened? When you're especially curious, fearful, or excited, you're less likely to evaluate the consequences of your actions. In fact, you probably will not consider the legitimacy of the situation presented to you. Consider this a red flag if your emotional state is elevated.

Did this message come from a legitimate sender? Inspect email addresses and social media profiles carefully when getting a suspect message. There may be characters that mimic others, such as "torn@example.com" instead of "tom@example.com." Fake social media profiles that duplicate your friend's picture and other details are also common.

Did my friend actually send this message to me? It's always good to ask the sender if they were the true sender of the message in question. Whether it was a coworker or another person in your life, ask them in-person or via a phone call if possible. They may be hacked and not know, or someone may be impersonating their accounts.

Does the website I'm on have odd details? Irregularities in the URL, poor image quality, old or incorrect company logos, and webpage typos can all be red flags of a fraudulent website. If you enter a spoofed website, be sure to leave immediately.

Does this offer sound too good to be true? In the case of giveaways or other targeting methods, offers are a strong motivation to drive a social engineering attack forward. You should consider why someone is offering you something of value for little gain on their end. Be wary at all times because even basic data like your email address can be harvested and sold to unsavory advertisers.

Attachments or links suspicious? If a link or file name appears vague or odd in a message, reconsider the authenticity of the whole communication. Also, consider if the message itself was sent in an odd context, time, or raises any other red flags.

Can this person prove their identity? If you cannot get this person to verify their identity with the organization, they claim to be a part of, do not allow them the access they are asking for. This applies both in-person and online, as physical breaches require that you overlook the attacker's identity.

How to Prevent Social Engineering Attacks

Beyond spotting an attack, you can also be proactive about your privacy and security. Knowing how to prevent social engineering attacks is incredibly important for all mobile and computer users.

Here are some important ways to protect against all types of cyberattacks:

Safe Communication and Account Management Habits

Online communication is where you're especially vulnerable. Social media, email, text messages are common targets, but you'll also want to account for in-person interactions as well.

Never click on links in any emails or messages . You'll want to always manually type a URL into your address bar, regardless of the sender. However, take the extra step of investigating to find an official version of the URL in question. Never engage with any URL you have not verified as official or legitimate.

Use multi-factor authentication. Online accounts are much safer when using more than just a password to protect them. Multi-factor authentication adds extra layers to verify your identity upon account login. These "factors" can include biometrics like fingerprint or facial recognition, or temporary passcodes sent via text message.

Use strong passwords (and a password manager). Each of your passwords should be unique and complex. Aim to use diverse character types, including uppercase, numbers, and symbols. Also, you will probably want to opt for longer passwords when possible. To help you manage all your custom passwords, you might want to use a password manager to safely store and remember them.

Avoid sharing names of your schools, pets, place of birth, or other personal details. You could be unknowingly exposing answers to your security questions or parts of your password. If you set up your security questions to be memorable but inaccurate, you'll make it harder for a criminal to crack your account. If your first car was a "Toyota," writing a lie like "clown car" instead could completely throw off any prying hackers.