What is Social Engineering And How do You Protect Yourself?

AVAST CYBERHOOD WATCH **TOOLKIT**

Social structures can be ‘hacked’ just like physical and digital structures can. Hacking a database, for example, would require significant technical ability, whereas tricking the owner of the database into revealing the password to access it is comparatively easy. Fundamentally, social engineering is about tricking people into doing what you want them to do. More often than not, a trickster will use various psychological manipulation techniques to obtain sensitive information from the victim, such as passwords or financial data. The attacks often come from apparently trustworthy sources, and victims do not even realise they’re being conned until it’s too late and their sensitive data has been accessed.

Types of Social Engineering

Though social engineering can happen in person, over the phone or online, attacks often appear as an email, text, or voice message from a seemingly innocuous source. Here are some examples:

Phishing

Phishing is an attack in which emails are disguised as being from a trusted source and are designed to trick victims into giving away personal or financial information.

Baiting

Baiting is when an attacker leaves a malware-infected device, such as a USB drive, where someone is likely to find it and use it.

Vishing

Also known as “voice phishing,” attackers call and disguise themselves as technicians, fellow employees or IT personnel to gather personal or financial information.

Smishing

Smishing comes in the form of text messages or SMS. Attacks usually threaten and solicit immediate action from a victim, such as a click on a link.

Pretexting

Pretexting involves pretending to be someone else to obtain private information. Attackers often do a lot of research to pass themselves off as authentic.

AVAST CYBERHOOD WATCH TOOLKIT

How to Prevent a Social Engineering Attack

The best way to prevent social engineering attacks is to know how to spot them. You don’t need to be a tech expert to practice good social engineering prevention, just use your intuition and consider the following tips:

1 Double-check the content

In the case of email or text message, if the sender’s domain looks suspicious, it could mean the message is malicious. If the content includes grammatical and punctuation errors and an over-dramatic sense of urgency, this may indicate the same.

2 Research the source and links

If you receive an email, SMS, or phone call from an unfamiliar source, search for that address or phone number and see what comes up. Even if the sender looks and claims to be legitimate, check anyway because the email address or phone number may turn out to be just slightly different from the real source.

3 **Question the context**

One simple rule applies: if something sounds too good to be true, it probably is. Ask yourself, “Would they really ask me for this information in this way? Would they really share this link with me?”

4 **Install a strong antivirus**

Ensure your devices and applications are always up-to-date, and install strong antivirus software with an anti-phishing feature to ensure your personal information is secured.