Common Types of SOCIAL ENGINEERING SCAMS

The National Cyber Security Centre (NCSC) defines social engineering as 'manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker'. In other words, social engineering consists of cyber-criminals convincing victims to make a mistake and compromise themselves.

With many employees working remotely during the coronavirus pandemic, cyber-criminals have increased the frequency of their attacks. As such, organisations and employees should be aware of these common types of social engineering scams:

PHISHING

Phishing attacks can be conducted via email or text and generally attempt to coerce victims into opening harmful attachments or links that result in a device being infected with malware.

BAITING

These attacks stem from a criminal tempting a victim, such as by offering them a fake online prize. Baiting can also be physical. A criminal might give away free USB sticks that compromise a device upon being inserted.

VISHING

This type of attack is conducted over the telephone and often includes a fake, urgent voicemail that attempts to scare the victim into calling back and providing sensitive information.

PRETEXTING

Pretexting attacks consist of cyber-criminals attempting to use a pretext or story to gain the victim's attention and interest, such as by offering a fake inheritance from an unknown distant relative or pretending to be a person of authority. Once trust is gained, the perpetrators then attempt to procure sensitive information or money from the victim.

WATER-HOLING

In this type of scam, cyber-criminals gather information about legitimate websites that an organisation's employees may visit often. The criminals then infect these websites with malware, resulting in employees who visit the site to also have their devices become infected.

RISK SOLUTIONS