Be cyber safe: what is social engineering?

Description

When scammers try to manipulate you into performing an action or sharing confidential information, it is known as social engineering. Cybercriminals use this technique to access computer systems, gather information or make money.

Most successful social engineering attacks are caused by human error. Familiarising yourself with common social engineering methods can help you recognise and avoid these attacks.

Social engineering tricks

Cybercriminals use several different methods to trick you with a social engineering attack, including:

- **Malicious links:** Cybercriminals may use malicious links to trick you into downloading dangerous software or opening an unsafe webpage. They may send you a phishing email, which tries to convince you to share sensitive information, click an unsafe link or download a malicious attachment. For example, you could receive an email that contains a link to access shipping information for an order. Because the email seems legitimate, you may be tempted to click the link – but then the link could download malicious software that allows the cybercriminal to control your computer.
- **Fake webpages:** Cybercriminals may create fake webpages to trick you into logging into the page or entering sensitive information. For example, you could receive a phishing email that contains a link to log in to LinkedIn. Because the email seems legitimate, you may be tempted to

click the link and enter your login credentials. Once you've entered your login credentials, the cybercriminal can log into your LinkedIn account, view your personal information and change your password so that you can't access your account.

- **Impersonation:** Cybercriminals may impersonate a celebrity or someone you know to trick you into revealing sensitive information, clicking an unsafe link or downloading a malicious attachment. For example, you could receive a phone call from a cybercriminal posing as your internet provider. The cybercriminal could tell you that your monthly payment is overdue and mention your account number and date of birth. Because the call seems legitimate, you may be tempted to provide your payment information. Keep in mind that impersonation attacks can also occur over email, text message or social media.

How to avoid social engineering

Follow these tips to protect yourself from social engineering attacks:

- Before clicking a link, hover your mouse over the link to make sure that the link is secure and matches the website you're looking for.
- Instead of clicking a link or a button in an email to navigate to a website, navigate directly to the website by entering the URL into your address bar.
- Before sharing sensitive information such as your birthdate or your payment information, verify that the source you're sharing the information with is legitimate.
- If someone you know messages you to ask about your organisation or sends you a link, call or text the person directly to make sure the request is legitimate. If a message seems suspicious, it likely is suspicious.

Category

1. Our Knowledge Corner