Learn to spot the signs of fraud and earn all 10 badges

Be prepared, not scared

Like every good camper, you know that being prepared is all about having the skills to spot the signs of danger, and the knowledge to avoid becoming the next victim — especially when it comes to protecting yourself from online social engineering attacks.

Social engineering describes a range of manipulative online behaviour to trick you into revealing confidential information. Social engineers use human behaviour, rather than hacking expertise, to gain access to your computer system and network.

Careful curiosity

You know that curiosity is good, but you need to use it carefully when receiving emails or being contacted by people you don't know on social media. You're prepared, so you never select links in emails for free gifts or surveys because as your grandpa told you, (and his grandpa before him) "just because it doesn't have a price tag, doesn't mean it doesn't have a cost."

Look before you leap

You know that emails or calls with urgent requests are signs of a social engineering attack. You're prepared, so you don't let panic cloud your judgement. Instead, you take a breath, look for signs like spelling and grammatical errors, and question the source.

Be mindful

You try to always be present and mindful in your life. You enjoy the things you're doing. Because of this, you're prepared and are less susceptible to social engineering scams that prey on a fear of missing out (FOMO) or the social anxiety that comes with it.

Social butterfly

You know that feeling alone and socially isolated can make you a target for fraud by scammers looking for personal information. You're prepared, and spot this social engineering sign. Like a social butterfly, you connect with family, friends, and the community — both online and off.

Safety first

You would never be careless and stroll through a dangerous neighbourhood, and you don't take risks online either. You see a shocking headline or image, but you know the signs of clickbait and are prepared. You know that one wrong click of the mouse could infect your computer system with malware.

Fear fighter

You're brave, so you don't let fear make you susceptible to manipulation by social engineers who send menacing emails to frighten you into making an impulsive and dangerous decision. You're prepared, and instead of a knee-jerk reaction, you slow down and think about who is sending it, and why.

Inspector skeptical

You're skeptical when getting an unusual or out-of-character request from someone in a position of authority. You're prepared, because you know that scammers use respect for authority to solicit personal information, donations, or gift cards. You know that respect is good, but acting on unusual requests without questioning it could lead to financial losses.

Recycle for good only

You like to reduce, reuse, and recycle, but never for your passwords. You know that cybercriminals count on people reusing their passwords across multiple programs and platforms. You're prepared, and never recycle your passwords to prevent an easy entry to your accounts. You like to use phrases, sayings, or song lyrics that are easy for you to remember, and hard for others to guess.

Privacy pledge

You enable your privacy settings when on social media, include only close family and friends, and always consider the consequences of posting personal information. You know that hackers and thieves love private details like where you live or when you're on vacation. You're prepared, so you don't overshare information that could put your personal or financial safety at risk, and never use public Wi-Fi for private uses like online banking.

Congratulations campers!

You are now armed with knowledge and can spot the signs of social engineering.
You're ready to prepare, protect, and prevail over fraud attacks.

SCU