Social Engineering – the cost of human error

The fear of becoming a victim of cyber crime has been amplified of late due to its portrayal in the media. With recent data leaks involving major organisations such as British Airways, Equifax and Travelex, it can be incredibly hard to escape the constant coverage in the media surrounding the impact of cyber-attacks and its subsequent effect on society.

The deployment of advanced cyber security defences has not gone unnoticed by cyber criminals so they continue to attack the weakest link within an organisation; cyber criminals are bypassing the advanced defences deployed by many businesses and targeting their clients using techniques such as social engineering, as people are considered easier prey.

Social engineering can be described as the art of manipulating people so they give up confidential information or are persuaded to undertake an action for the benefit of the perpetrator. The types of information these criminals are seeking can vary, but when individuals are targeted by the criminals, they are usually attempting to trick them into revealing passwords or financial information. Cyber-criminals often use social engineering techniques to access the victim's computer, which may allow them to secretly install malicious software that will give them access to passwords and sensitive information.

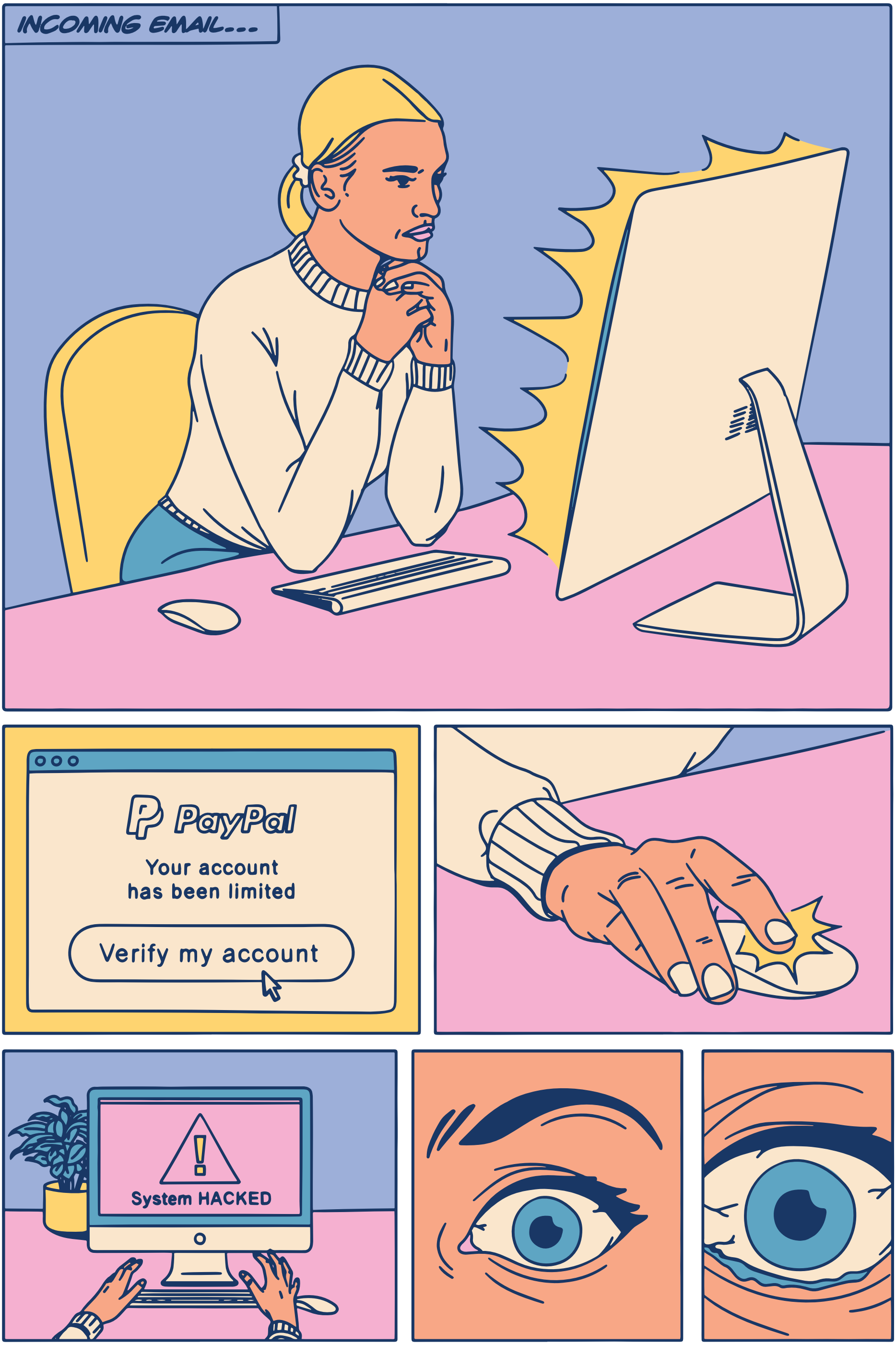
It is considered easier to exploit a person's natural inclination to trust as it is much simpler to trick someone into revealing their password than it is for them to try to hack or guess the password.

Security professionals constantly state that the weakest link in the security chain is the person who accepts an individual or scenario at face value. It is irrelevant how many locks or deadbolts are on your door, or if have an alarm, floodlights, guard dogs and security personnel, if you trust the individual at your door who claims to be the delivery person and you let them into your home without confirming they are legitimate, you are completely exposed to whatever risk they pose.

If a cyber criminal is able to socially engineer or hack your email account they will have access to your personal correspondence and your contact list. Once a cyber-criminal has your email account under their control, they are able to manipulate your messages and send emails to any of your contacts, enabling them to impersonate you for malicious purposes. Research shows that cyber criminals are regularly monitoring compromised email and social media accounts to build a profile of their target. Once they have enough information they are able to use the data collected to impersonate the victim. For example, to communicate with your financial adviser or bank to extract money.

> **“Cyber criminals are bypassing the advanced defences deployed by many businesses and targeting their clients using techniques such as social engineering, as people are considered easier prey.”**

Even if you do not use online banking, email or social media, you could still be a target of social engineering fraud. Cyber criminals are able to manipulate the telephony system to impersonate any telephone number. It is relatively easy to impersonate


INCOMING EMAIL...
PayPal
Your account
has been limited
Verify my account
System HACKED

anyone within your contact list. You must never assume the call you receive is your bank because the number displayed matches your contact. Always verify the caller by dialling them back on a trusted number you know.

It is important to remember that cyber criminals may use a variety of techniques when targeting a victim. Their main objective is to force a target into making a decision or taking an action that they would not otherwise take. They can be masters of deception, using social engineering techniques to manipulate their victim. Cyber criminals will attempt to use urgency in various guises to force their victim into making a snap decision. Do not allow any individual to rush you into a forced action and always verify independently. For example, if you are contacted by your bank or financial institution, try to seek a known trusted individual within the business to confirm the request. Contact them on a published number through Google or use your contacts through your telephone. Never be directed to click on a link within an email to access an organisation's website contact details as this can be used to trick you.

There are practical things you can do to protect yourself from becoming a victim of cyber crime. The best defence is awareness and understanding the techniques used to perpetrate these crimes and the realisation that we are most likely the weakest link.