SECURITY IN AN INSECURE WORLD

As a security professional advising large corporates, OR Angus Darroch-Warren's (Capel 1986) article makes us all think about our own personal safety and offers tips and advice...

My main role is to analyse the threats and risk to client organisations, their people and other assets, be they tangible, intangible or a bit of both. It is my role to understand the threats to operations, the vulnerabilities and the likelihood of an adverse incident taking place and the mitigation strategy that will, hopefully, prevent loss.

I hasten to point out that I am supported ably by a team of specialists, whether physical security practitioners, information professionals and those that have their credentials in the cyber world. Indeed, I would be almost certain that several of our ORs fit into one of these categories.

From the simple to the serious

These experts work collaboratively to reduce risk to organisations – big, small, government or private – but yet, increasingly, we hear of incidents directed against individuals and property, from the rudimentary (bladed weapon attacks) to the more sophisticated (coordinated terror attacks) to organised criminal activity (kidnapping to extort money). Sadly we, the public, have become used to the sight of armed police offers patrolling our streets, barriers and blockers to mitigate vehicle attacks and a host of other measures.

So, what do we do about these threats? In reality, the chance of being involved in an incident is extremely low, but it is our perception of risk that skews the reality and perhaps makes us consider options, such a cycling to work to avoid public transport, even though the likelihood of being injured on a bike is far greater than being affected by a terror incident. From a personal perspective, it's important to try and be 'security aware' and pay attention to your surroundings. If something looks suspicious, it probably is. Be prepared to act on your feelings and report to the nearest police officer or person of authority but take yourself away from the threat – a false alarm is always preferable to seeing the aftermath of an attack.

Cyber security

However, those that are looking to harm us are increasingly diverse in their approach. Terror groups (some state sponsored) use the internet for sophisticated publicity surrounding their cause and activist groups attack websites and deface homepages. It is known that nations spy on each other and some have publicly stated that they are looking to gain whatever competitive edge they can through espionage and covert operations. Similarly, criminals have realised that it is a lot safer, and far more effective, to use the internet as a way to steal, defraud and extort, particularly the unsuspecting and the vulnerable.

How do they do this? A combination of their skills and our ignorance of their tactics. Just recently, I received a text message purporting to be from my own bank, telling me to expect another text that would allow me to update my preferences with regards to paperless banking. Intriguingly, the first text came from a number that I know is used by the bank in question. The second email arrived with a link to change my preferences, however, the email address in the message was from an account

> From a personal perspective, it's important to try and be 'security aware' and pay attention to your surroundings.

SECURITY IN AN INSECURE WORLD

I had closed in 2014. The unwary, less tech-savvy person may have followed the link, putting themselves at risk of losing their savings.

The examples of how we put ourselves at risk are numerous and varied, with threats that include:

- **Advance fee fraud** – upfront fees are requested for goods or services that never materialise.
- **Lotteries** – you receive a letter from an overseas lottery company saying that you have won a prize (even though you never entered) but they require a fee or further personal details to release the prize.
- **Online account scams** – you receive an email or message from a bank or financial institution asking you to provide details, perhaps to unlock the account, which you do. It may be that they ask for the '1st and 3rd' digits from your online PIN, which you provide. Unfortunately, there is a 'system error' and the caller asks for the '2nd and 4th' digits. They now have all of your PIN number.
- **LinkedIn** and other business networking sites are riddled with fake profiles that can be traced back to hostile nation states and organised crime gangs looking to compromise users into divulging sensitive data regarding their organisation. Manage the information you put online and be prepared to check the profile of the person trying to make contact and block them if suspicious.
- **Delivery scams** – as the lockdown has required us to be more reliant on delivery services, this has given scammers a golden opportunity to send out messages that require you to follow a link, purportedly to collect a parcel, thereby giving out personal and/or financial details.
- **WhatsApp** continues to suffer from account hijacking, as does Facebook. Criminals send out contact requests from a compromised account, asking for you to connect with them, and then they have access to your personal details.

These types of scam rely on social engineering; criminals knowing how people might think and react to a given scenario, thus making them susceptible and easily targeted.

Stealing personal data

But the threats to our personal data extend beyond what most people imagine. The 'Internet of Things' refers to the connectivity between physical objects, through various technologies (Wi-Fi, Bluetooth), in order to exchange data across the internet. Connectivity is increasing, making our lives 'simpler' but, potentially, this comes at a price as criminals look to exploit this connectivity to further their own ends.

We are vulnerable in so many ways, from not changing default passwords and codes on mobile phones or Wi-Fi routers, to inadvertently sharing personal data online.

For instance, on social media, you receive a post forwarded by a friend. It asks you to name your first car or best friend at school or first pet. A harmless piece of fun? In reality you have given away a potential security question for your bank account/credit card and the criminal can use these credentials to access your accounts, telling the bank they have forgotten their/your details.

Alternatively, there is a post for a house/car/speedboat/holiday lottery as the company has had a sale fall through. They ask you to register your details and now you have just provided a scammer with your email address, phone, sexual orientation etc.

You buy a new car and find the satellite navigation system so useful, and easy to use: press the button and up comes the route to your house. However, if the car is stolen, the thief knows where you live, and the locations of family and friends. Alternatively, the in-car system may be easy prey to a hacker who can download all of the data. A simple solution is to input your 'home' address as a local supermarket, petrol station or other public location.

With lockdown restrictions easing, it may be that you decide to fly off to the sun, finding a great spot overlooking the beach, luckily the beach bar has free Wi-Fi so you logon and upload your pictures to Instagram. However, the Wi-Fi hotspot is compromised and all your data, including your Apple Pay transaction, has been passing through a criminal's network. ■

Similarly, criminals have realised that it is a lot safer, and far more effective, to use the internet as a way to steal, defraud and extort, particularly the unsuspecting and the vulnerable.

Protect yourself

So, what can you do to protect yourself? Without sounding too paranoid, think before you do anything!

- Don't go onto sites that you are unsure of – if in doubt, get out!
- Don't click on links in emails or texts that you have received – check the source, check the sender details, check spelling and grammar as these are give-aways that a scammer is involved.
- Think carefully – why am I being contacted? Why am I being asked to provide personal details?
- Ask for the caller's name and contact details and say you will call them back – check with the purported organisation.
- If the caller/email/text is demanding that you act quickly, pressurising you to make a decision on the 'fantastic' deal on offer, stop and think. If an offer appears too good to be true, then it probably is.
- Regularly change passwords to accounts – don't use a single password for all your accounts.
- Where possible, set up your accounts to have '2 Factor Authentication'. This requires a unique, one-time passcode to be sent to your device which you enter on your account.
- Consider using an Authenticator App, this generates passcodes for specific sites that you need access to.
- On all your devices, change the default password/PIN number.
- Consider the use of a Virtual Private Network (VPN) on your devices. A VPN protects your internet connection and enhances privacy through encryption and hiding your IP address (allowing you to use the beach bar Wi-Fi hotspot).

It sounds complicated, but in reality a couple of simple steps will enhance your personal security, both in the online world and on the streets of our cities. Be 'security aware' and pay attention to your surroundings (physically and virtually): remove yourself from the threat; think before you act and consider your options; report suspicious activities and trust your instincts.