SECURING YOUR DIGITAL FOOTPRINT

CYBER SECURITY AWARENESS MONTH 2020

WHAT IS YOUR DIGITAL FOOTPRINT?

Your digital footprint is the trail of data you leave on the internet as you use it; this can be intentional or unintentional. In order to protect yourself from cyber attacks that include social engineering, it is important that you understand and recognise what information is on the internet about you.

WHAT ARE THE DANGERS?

Your digital footprint can prove extremely valuable to cyber criminals. When in the early stages of a cyber attack on an individual or an organisation, cyber criminals will often use multiple different websites and tools to gather publicly available information. This technique of reconnaissance is called Open Source Intelligence (OSINT). In a short amount of time, cyber criminals can build up a picture of you and your personal information. This information is then used to either target you or impersonate you to attack others or your organisation.

Information shared by others, for example comments on photographs, can be valuable to criminals trying to perform OSINT. It is easy to find partners, siblings and work colleagues from posts. An innocent "Happy 30th birthday Tyler, best nephew ever!" comment can confirm a date of birth, name and relationship to others.

It is very important to be wary of links and attachments in all communications (not just email, but also SMS text messages, social media messages and messaging applications such as WhatsApp), especially if the communication is unexpected and if it makes you feel emotional. Social engineering tends to be most successful when it elicits an emotional response in us (such as fear, shame or flattery) because this can cloud our judgement. Read out recent guidance document on phishing for some examples.

SECURING YOUR DIGITAL FOOTPRINT

CYBER SECURITY AWARENESS MONTH 2020

TOP TIPS FOR SECURING YOUR DIGITAL FOOTPRINT

Here are a few quick and easy steps you can take to put more security around your digital footprint. Remember we are only as secure as our network: pass this guidance on to friends, family and colleagues to help them be more secure online, which will in turn help raise the level of your own security.

✅ Review your social media settings. Services such as Facebook often change the configuration of security settings, and so periodically checking these settings is helpful in ensuring that profile information is as private as you would expect.

✅ Go to www.haveibeenpwned.com and check if your email address has been breached, if it has make sure you are not still using the same password for those accounts.

✅ Use a password manager to help manage strong and unique passwords for all accounts.

✅ Set up two-factor authentication (2FA) on all accounts. 2FA adds a second layer of security to your accounts, to help protect you in case your passwords get compromised. For more information on passwords and 2FA, read our recent account security guide.

HANDY TIP

Get yourself a Digital Footprint Buddy and OSINT each other! This could be a family member or work colleague. The important thing is that you're not connected on social media, as you want to find out what information is publicly available about you. Have a go at seeing how much information you can find about your OSINT buddy, as a starting point what personal and professional information can you find?

REMEMBER! OSINT should always be passive and consensual. To avoid breaking the law, you should not:

- Attempt to log into any accounts of another person without their permission, even if you have their passwords
- Perform the OSINT task on an individual without their permission