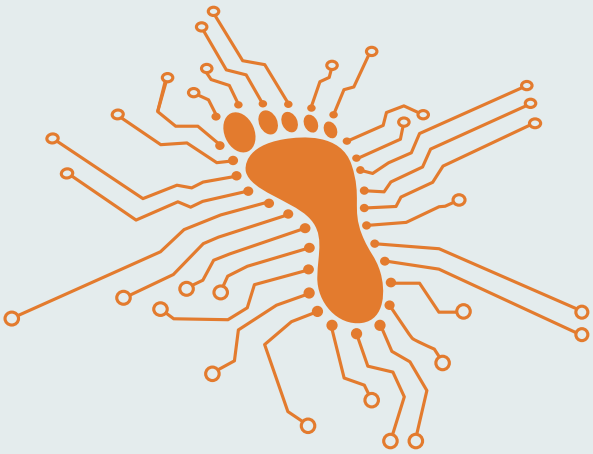

PROTECTING YOUR DIGITAL FOOTPRINT

CYBER SECURITY IS NOT JUST AN ISSUE FOR LARGE BUSINESSES. CYBER SECURITY – OR PEOPLE ATTACKING YOUR COMPUTER AND DATA – CAN ALSO BE A RISK FOR SMALL BUSINESSES SUCH AS CANE FARMS. IN THIS ARTICLE, *SRA IT MANAGER ADAM O'HALLORAN* EXPLAINS CYBER SECURITY AND SOME STEPS YOU CAN TAKE TO REDUCE RISK.

It's common for small businesses and families to believe that cyber security is something that they don't need to worry about. After all, their computer just has old files, emails and photos, right? If a hacker wants to read productivity data from five years ago, then let them!

IT'S ALL ABOUT THE MONEY

Cyber attacks are conducted by criminals with the intention to do one of three things:

1. Obtain money

The primary reason for an attack is to gain access to your machine and your files and make them both unavailable until you pay them money to regain access (which may not eventuate with payment). The most common method is ransomware. If an application of this type is installed, you will lose access to all your files and any recent backups and files that are attached in a connected device (such as an external drive).

2. Steal your identity

Identity theft is the opportunity for a criminal to obtain enough information about you, to conduct fraudulent transactions, especially credit card fraud.

3. Gain access to people that you know

If criminals obtain your email credentials (your email address; username and password), they will access your email account and send an email intended to gain access to their data or their identity, to everyone you have contacted via email.

IT'S VERY EFFECTIVE

The nature of the attack is to write a script to attempt one of the three types of attacks (or more than one) that notifies them if a copy of the script was successful – anywhere in the world. The federal government estimates cybersecurity incidents cost Australian businesses $29 billion each year.

Almost one in three Australian adults were affected by cybercrime in 2018.

WHAT SHOULD I DO?

If you are running a small business, then engage the services of a company that has experience in increasing your security. They will work with you to ensure that your business is not exposed to known risks.

Your home computer is equally at risk, but there are some simple steps that you can take:

1. If you are not running a new computer, such as Windows 10, then now is the time for an upgrade. Some computers can be upgraded, but most should be replaced.
2. Keep your computer software up to date. Ensure that your computer applies updates automatically. If you are asked to restart your machine to apply updates, do it straight away.
3. Be suspicious of emails that are asking you to perform tasks, such as follow links; entering your details or downloading software. No company will ask you to 'confirm your details'. It is unlikely that any of these emails are legitimate.
4. If you receive an email from a company that you use (such as a bank), but the email doesn't look right (it's asking you to do something), then you can always call them and ask if this is their email.
5. Google, Facebook, Instagram and many other online companies provide an option to enable 'Two-Factor Authentication'. This is a very simple process that means your account cannot be accessed without your mobile phone.
6. Save your files to a secure cloud location, such as Microsoft OneDrive, Google Drive or Dropbox.

WHAT SHOULD I DO IF I THINK SOMETHING HAS HAPPENED?

If you believe that this is an emergency, call your local Police, or dial 000. To report a cyber issue, go to the Australian Cyber Security Centre's page: ***reportapp.cyber.gov.au*** ■

Contact Adam O'Halloran
aohalloran@sugarresearch.com.au
07 3331 3316.