ALLADEAN CHIDUKWANI *Director / Principal Consultant, Cyber Experts Australia*
LinkedIn https://www.linkedin.com/in/alladean/

TIP 1. ONLY A FOOL SAYS "WE HAVE NOTHING WORTH HACKING"

Next time you think "our business is too small to hack" or "we have nothing of worth to be a cybercrime target", remember that one stolen identity can sell for about $60 to $80 on the digital black market (dark web). So your customer, employee and personal details ARE definitely worth something.

TIP 2. ATTACKS AREN'T PERSONAL

With the exception of 'hacktivists', most cyber criminals have nothing personal against you or your business. To them its just business and your data is the product. They simply hijack it and sell it back to you (ransomware) or steal it and sell it to the highest bidder on the dark web.

TIP 3. PRINTERS NEED SECURING TOO

"The printer is just a machine that spits our paper"! Well, think again. Your printer has firmware, RAM, a hard drive and network connections. Printers have all the elements that make up a computer; however most people don't see it that way. Unfortunately, hackers do and they will attack your vulnerable printer and pivot to access the rest of your network or systems. Printer security is just as important as computer security.

TIP 4. PASSPHRASE INSTEAD OF PASSWORD

Yes, your password can have spaces in it. Nowadays its best to make sure you put a space to make it a Pass-phrase (multiple words) instead of a password (one word). If you struggle to remember them, like me, then use a simple pass-phrase formulation techniques like…

"<name of grandparent starting with uppercase> <space> <town of birth> <space> <child/spouse/parent's date of birth>".

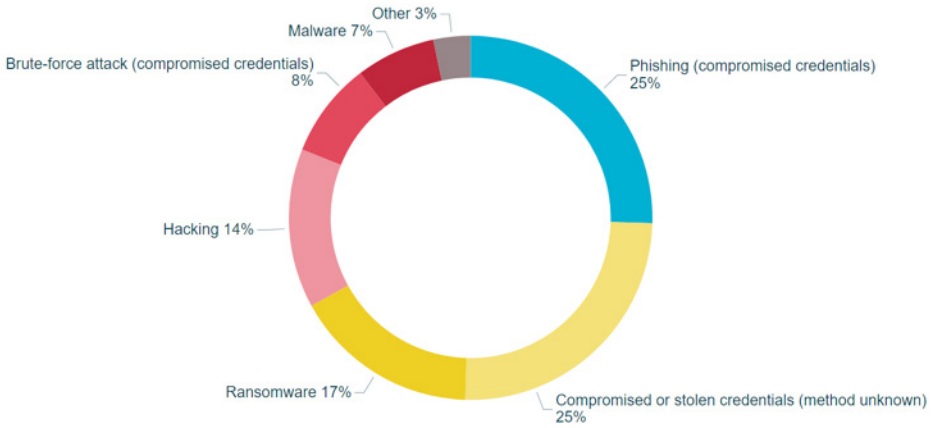
TIP 5. PHISHING EMAILS

Phishing emails are, by far, the biggest threat to individuals and businesses in Australia. The majority of ransomware attacks originate from phishing emails. The safest attitude is to treat every email as suspect until proven otherwise. Be comfortable to ignore/delete emails you are not too sure about. Remember, if it's important, they have other means to find or contact you. They can phone or SMS you (and even post a letter) if you mistakenly identify a legitimate email as a phishing email. You will not miss out on anything.

TIP 6. BEWARE OF SOCIAL ENGINEERING

Cyber criminals are now targeting and exploiting human psychology and behaviours to get unauthorised access to data and systems. They prey on human being's deeply rooted impulses, e.g.: trust, fear, compassion, ignorance, desire to help, appeal to authority etc. and trick you into doing something you shouldn't, or divulging information that you shouldn't. Treat any request via email, phone or sms as sceptical and reduce your chances of falling victim to social engineering.

CYBER INCIDENT BREAKDOWN - ALL SECTORS



Source: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/

TIP 7. BACKUP IS A MUST

Backups are your only sure way of recovering from a ransomware attack. Ensure backups are run daily. Paying the ransom is a strict no-no and, even if you do pay, there is no guarantee that the criminals will unlock your data, or leave a backdoor to lock it again when they are broke and need some more money.

TIP 8. CYBER ATTACK - NOT IF BUT WHEN

When it comes to cyber-attacks, it's not a matter of IF, but a matter of WHEN. Everyone is a target, whether individual, small business, large enterprise or government. The question is, when it comes your way, how do your defences stack up? Never let your guard down!

TIP 9. DUMPSTER DIVING IS A THING

Cyber criminals use all sorts of techniques to get to your systems and important information including searching through your trash for sticky notes with written passwords, access codes, product designs, business plans, phone lists, calendars and even discarded computer equipment that may still have data on them. Be careful what you dispose, all computers should be data wiped before disposal, and paper documents shredded to ensure they cannot be used by the dumpster divers.

TIP 10. HUMANS ARE THE WEAK LINK

Being the primary target for social engineering attacks e.g. phishing, employees should be educated about cyber threats, their impact on not only business but also on them as an individual. Most importantly, they should be educated on their important role in keeping the business and their livelihoods safe.