Tip 3 : Slow down and take extra care when connected to the internet

An increasingly connected world makes our business and personal lives much easier. Sadly it also exposes us to greater risks of attack by cyber criminals and increases the likelihood of theft of our personal and confidential data.

Many social engineering attacks prey on the internet user by creating a sense of urgency or panic in order to trick the user into opening a link or downloading an infected file or disclosing personal details.

Some common scams preying on users and creating a sense of urgency include an email from a bank saying your ATM access is being denied, a message or email from Australia Post asking you to confirm delivery details, communication from your internet provider threatening to cut off access if a bill is not paid or a notice from the Taxation department stating that you will be fined if outstanding tax amounts are not paid.

All these communications will contain a link or an attachment that needs to be opened to respond. It is these links or attachments that are infected and either provide access to your personal accounts and details or alternatively impregnate your systems with malware.

There are some simple things to remember when faced with these communications to help you avoid being tricked into taking harmful action.

1. **Slow Down:** The implied urgency in emails and messages is one of the biggest factors in users making the wrong decision and mistakenly or inadvertently responding to a phishing attempt. Read the communication carefully and think about the sender, and the content. Does it seem legitimate? Are there any red flags? When in doubt, do not open any attachments or click on any links until the communication has been checked

2. **Always Verify the communication:** This is important before any action is taken by the user in response – particularly if it asks for personal or confidential information. If you receive a message asking for critical confidential or personal data, even if it is from someone you know, call the sender on a independently – verified telephone number and confirm the legitimacy of the request.

3. **Ask Questions:** Don't be reluctant or embarrassed to ask questions and demand proper explanations regardless of who is claiming to need the information from you. Some people are embarrassed demanding a seemingly foolish explanation, but verifying the validity of information requests is never stupid when there are personal details involved.

4. **Double check the language and format of emails:** Poor grammar and spelling should be a red flag. If your email comes from one of your known contacts, take a little time to check that the wording, format and sign off look usual. If anything looks different, be wary.

5. **Double Authenticate any money transfers**: Whenever a sum of money, large or small is to be paid (particularly when receiving email confirmation of payment details), ALWAYS require a separate voice or in person confirmation prior to making the payment. If telephoning to confirm the payment and you do not know the voice of the person

authenticating the payment,, use an independently sourced telephone number – not the one on the invoice.

6. **Foster a culture of openness around email and data security:** All employees need to feel comfortable asking questions about unusual or suspicious communications. They should be encouraged to question anything suspicious.

7. **Think:** Remember that no bank or online payment system will ever ask you for private information via email: Most financial institutions send reminders to their clients that they will never ask for personal information via email. Despite this, many internet users are fooled into providing personally identifiable information on email or to the caller in an unsolicited telephone call. Always verify the request for information by an independent means, particularly when the request for information contains some urgency..

8. **Antivirus Software:** Use a reputable antivirus software on all your devices.

9. **Back Up Regularly:** back up your devices to an external hard drive or the Cloud.

10. **Educate:** Continue to educate all employees and staff on healthy email security and practices and reinforce your organisation's cyber security guidelines on a regular basis.