Staying safe online

Financial cybercrime is on the rise in Australia, as the increasing use of technology such as online banking and social media makes it an attractive target for criminals.

Despite increasingly sophisticated methods being used, there are a number of things you can do to help you and your family stay safe online.

As our financial lives move increasingly online, cybercrime is becoming more prevalent. As simple as a phishing email or as far-reaching as the WannaCry ransomware attack that hit more than 150 countries in May 2017, cybercrime can have devastating impacts for individuals and businesses alike.

What is cybercrime?

Cybercrime refers to criminal activity that is directed towards a computer or mobile device. It involves gaining personal details from a victim, such as banking account or credit card details, in an attempt to steal money, data or other personal information.

The impacts of cybercrime can be significant and extremely upsetting for the victim, with the costs being not only financial, but emotional, as the victim has their privacy and sense of security violated.

Types of cybercrime

There are a number of different methods that cyber criminals use to access your information for financial gain. Understanding these risks can help you better detect suspicious activity and make smarter decisions around how to respond.

- Online scams. Schemes that seek to take advantage of individuals by presenting a solicitous offer (such as a free or cheap holiday) that turns out to be dishonest or non-existent.
- Identity fraud. Illegally accessing an individual's information and using that information to steal money or other benefits.
- Malware and ransomware. Malicious software designed to gain unauthorised access to an individual's computer system. Typically used to steal data, destroy data, or to prevent the user from being able to access their files, holding them to 'ransom'.
- Phishing. An email pretending to be from a legitimate, trusted company (such as a bank or other service provider) that attempts to trick an individual into providing their personal or financial information.
- Bullying and harassment. Using technology to conduct behaviour that is intended to make a person feel fearful, uncomfortable or offended.

Spotlight on phishing

In June 2017, the Australian Competition & Consumer Commission (ACCC) warned people to be vigilant of 'phishing scammers' pretending to be from well-known businesses and government departments.

"Scammers use phishing to trick their victims into giving out valuable personal information such as their bank account numbers, passwords, credit card numbers or even their online passwords for their PayPal, Apple or social media accounts. Any personal information you have is potentially valuable to a scammer and they will try to get it off you in a variety of ways," said ACCC Acting Chair Delia Rickard.

"The scammer may say that the bank or organisation is verifying customer records due to a technical error that wiped out customer data. Or, they may ask you to fill out a customer survey and offer a prize for participating. These are all part of a scammer's bag of tricks which they use to get you to give up your valuable personal data," said Ms Rickard.

Once they have enough personal information, scammers can conduct criminal activity such as making purchases with the victim's credit cards, stealing their identity, or scamming the victim's friends or family.

Tips for staying safe online

While there are no guarantees that you can protect all your information from being unlawfully accessed, there are a number of things you can do to reduce your risk of becoming a victim of cybercrime.

- Regularly update software. Installing updates for your operating system and applications is essential.
- Don't divulge personal information when requested via email. Verify any such request using a different channel (such as a phone call).
- Beware of emails asking for financial information. Banks, super funds and other financial providers will never ask their customers to email personal financial information or login details for secure websites.
- Choose a strong password. A good password is easy for you to remember but difficult for anyone else to guess. The strength of your password is determined in part by its length and complexity (try to avoid words you'd find in a dictionary). Avoid using the same password across multiple services – if you use a lot of digital services, consider use of a password manager that stores data on your local device. It's also best practice to change passwords for critical services every few months.
- Invest in basic antivirus protection. Anti-virus software can go some way toward protecting your device against known threats.
- Restrict use of public Wi-Fi to web browsing. An open Wi-Fi network can be used to intercept communications between your devices and the internet, such as user names, passwords and financial information.
- Log out after browsing. Always log out from your internet banking session and other secure websites, and close your internet browser when you have finished.

Source: Colonial First State