STAYING SAFE ONLINE

Tips to keep you and your family safe from cybercrime

The internet has changed the way we live – from shopping and banking to connecting with friends and catching up with the news. But now that so many of the activities we do every day are online, it's become easier for hackers to get access to your personal information.

Colonial First State

Cybercrime in Australia

How widespread is cybercrime? Probably more than you think.

In a 2016 survey by the Australian Institute of Criminology, 8.5% of respondents had experienced identity theft or misuse of their personal information in the previous 12 months.[1]

Identity theft occurs when someone uses your personal information to pretend to be you in order to carry out fraudulent activities, such as trying to access your bank accounts or opening a credit card in your name.

Cybercrime campaigns often start with an email that attempts to convince someone to install unauthorised software on their computer, or asks them to provide personal information. This can result in financial loss or other negative consequences.

The good news is there are easy steps you can take to keep yourself and your family safe online.

By understanding more about cybercrime and how cybercriminals target their victims, you can learn to recognise potential scams and adopt safe online behaviour. This guide is a great place to start.

Types of cybercrime

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 this information to steal money or other benefits.

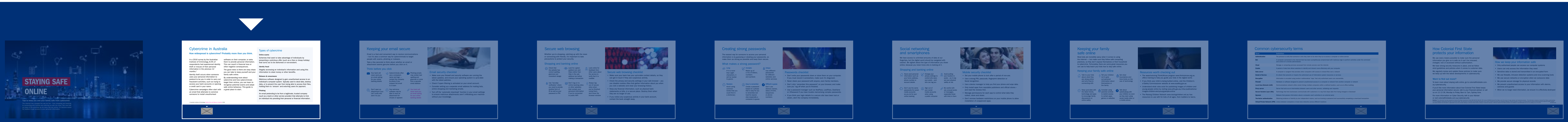
Malware & ransomware

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’ and extorting users for payment.

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.

[1] Australian Institute of Criminology, *Identity Crime and Misuse in Australia*, 2016



Keeping your email secure

Email is a fast and convenient way to receive communications – but it’s also a common way for cybercriminals to target people with scams, phishing or malware.

Take a few seconds to think about whether an email or attachment seems genuine before you click on it.

Think before you click

Your bank will never send you an email asking for your online banking details

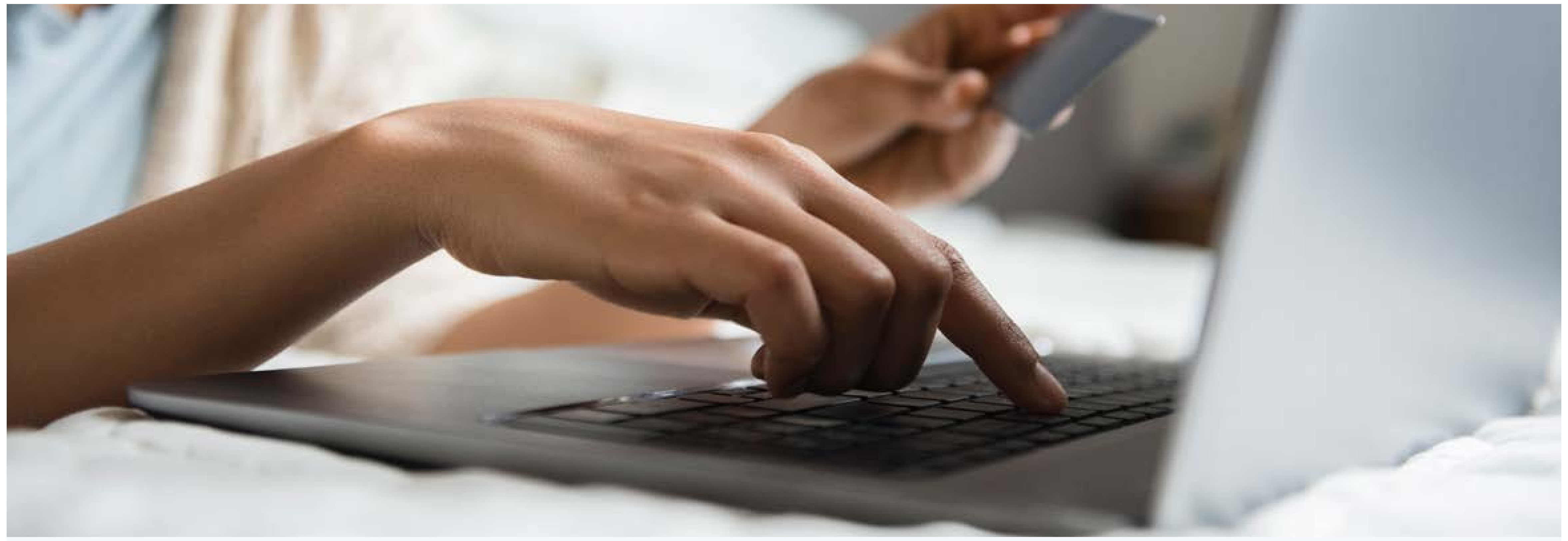
Cybercriminals often use a company’s name and logo — contact the company by phone if you suspect the email is a scam

Phishing emails may contain bad spelling and grammar or come from a peculiar email address

Don’t open an attachment if you can’t verify who sent it to you

Your anti-virus software may be able to scan an attachment for viruses or spyware

Only click on links if you recognise and trust the web address it will take you to



Email security checklist

- Make sure your firewall and security software are running the latest updates, and ensure your operating system is up-to-date with the latest patches.
- Check if spam filtering is activated on your email account.
- Consider setting up a separate email address for mailing lists, online shopping and marketing emails.
- Turn off the ‘automatic download’ function in your email settings to ensure malicious attachments aren’t infiltrating your machine without your knowledge.

Secure web browsing

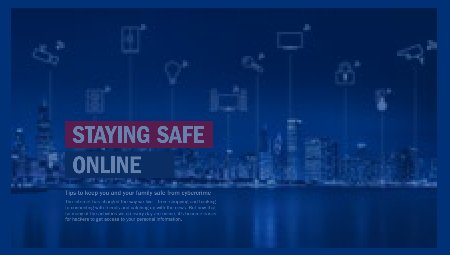
Whether you're shopping, catching up with the news or connecting with friends, it's important to take precautions to protect your security.

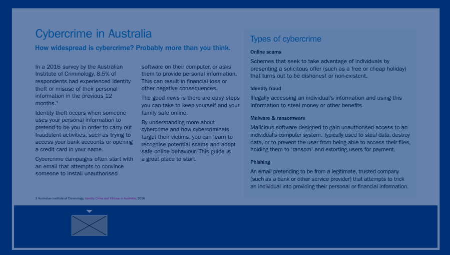
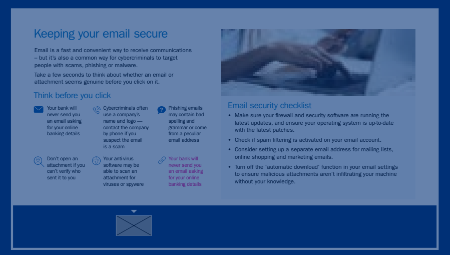
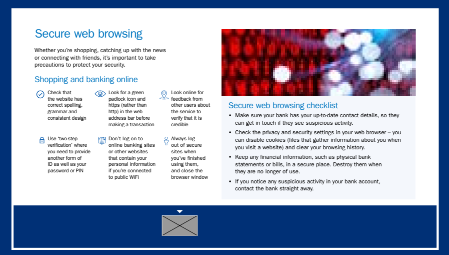
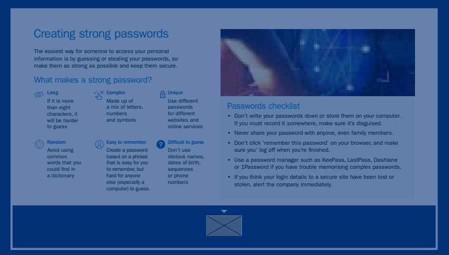
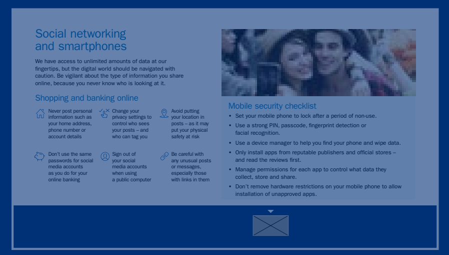
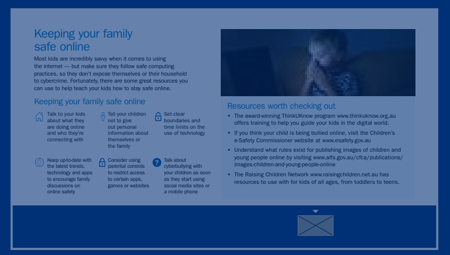
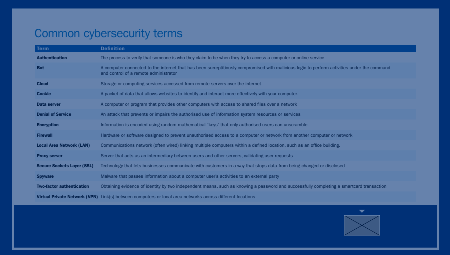
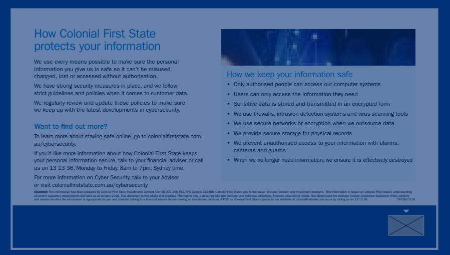
Shopping and banking online

- ✓ Check that the website has correct spelling, grammar and consistent design
- Look for a green padlock icon and https (rather than http) in the web address bar before making a transaction
- Look online for feedback from other users about the service to verify that it is credible
- Use 'two-step verification' where you need to provide another form of ID as well as your password or PIN
- Don't log on to online banking sites or other websites that contain your personal information if you're connected to public WiFi
- Always log out of secure sites when you've finished using them, and close the browser window

Secure web browsing checklist

- Make sure your bank has your up-to-date contact details, so they can get in touch if they see suspicious activity.
- Check the privacy and security settings in your web browser – you can disable cookies (files that gather information about you when you visit a website) and clear your browsing history.
- Keep any financial information, such as physical bank statements or bills, in a secure place. Destroy them when they are no longer of use.
- If you notice any suspicious activity in your bank account, contact the bank straight away.



Creating strong passwords

The easiest way for someone to access your personal information is by guessing or stealing your passwords, so make them as strong as possible and keep them secure.

What makes a strong password?

Long

If it is more than eight characters, it will be harder to guess

Complex

Made up of a mix of letters, numbers and symbols

Unique

Use different passwords for different websites and online services

Random

Avoid using common words that you could find in a dictionary

Easy to remember

Create a password based on a phrase that is easy for you to remember, but hard for anyone else (especially a computer) to guess

Difficult to guess

Don’t use obvious names, dates of birth, sequences or phone numbers

Passwords checklist

- Don’t write your passwords down or store them on your computer. If you must record it somewhere, make sure it’s disguised.
- Never share your password with anyone, even family members.
- Don’t click ‘remember this password’ on your browser, and make sure you’ log off when you’re finished.
- Use a password manager such as ‘KeePass’, ‘LastPass’, ‘Dashlane’ or ‘1Password’ if you have trouble memorising complex passwords.
- If you think your login details to a secure site have been lost or stolen, alert the company immediately.

Social networking and smartphones

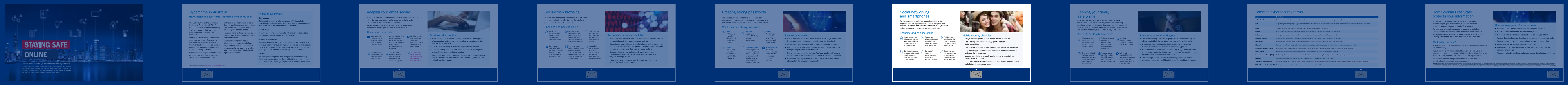
We have access to unlimited amounts of data at our fingertips, but the digital world should be navigated with caution. Be vigilant about the type of information you share online, because you never know who is looking at it.

Shopping and banking online

- Never post personal information such as your home address, phone number or account details
- Change your privacy settings to control who sees your posts – and who can tag you
- Avoid putting your location in posts – as it may put your physical safety at risk
- Don’t use the same passwords for social media accounts as you do for your online banking
- Sign out of your social media accounts when using a public computer
- Be careful with any unusual posts or messages, especially those with links in them

Mobile security checklist

- Set your mobile phone to lock after a period of non-use.
- Use a strong PIN, passcode, fingerprint detection or facial recognition.
- Use a device manager to help you find your phone and wipe data.
- Only install apps from reputable publishers and official stores – and read the reviews first.
- Manage permissions for each app to control what data they collect, store and share.
- Don’t remove hardware restrictions on your mobile phone to allow installation of unapproved apps.



Keeping your family safe online

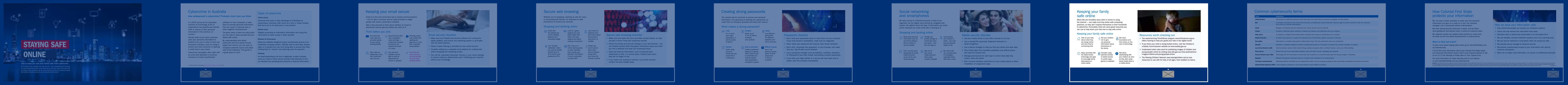
Most kids are incredibly savvy when it comes to using the internet – but make sure they follow safe computing practices, so they don't expose themselves or their household to cybercrime. Fortunately, there are some great resources you can use to help teach your kids how to stay safe online.

Keeping your family safe online

- Talk to your kids about what they are doing online and who they're connecting with
- Tell your children not to give out personal information about themselves or the family
- Set clear boundaries and time limits on the use of technology
- Keep up-to-date with the latest trends, technology and apps to encourage family discussions on online safety
- Consider using parental controls to restrict access to certain apps, games or websites
- Talk about cyberbullying with your children as soon as they start using social media sites or a mobile phone

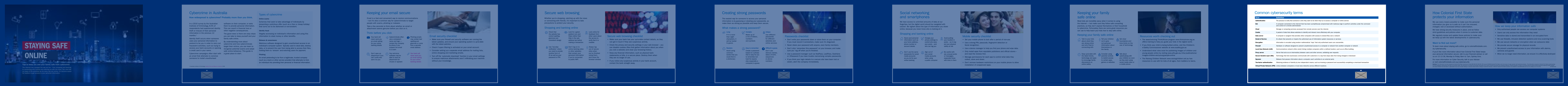
Resources worth checking out

- The award-winning ThinkUKnow program www.thinkuknow.org.au offers training to help you guide your kids in the digital world.
- If you think your child is being bullied online, visit the Children's e-Safety Commissioner website at www.esafety.gov.au
- The Raising Children Network www.raisingchildren.net.au has resources to use with for kids of all ages, from toddlers to teens.



Common cybersecurity terms

Term	Definition
Authentication	The process to verify that someone is who they claim to be when they try to access a computer or online service
Bot	A computer connected to the internet that has been surreptitiously compromised with malicious logic to perform activities under the command and control of a remote administrator
Cloud	Storage or computing services accessed from remote servers over the internet.
Cookie	A packet of data that allows websites to identify and interact more effectively with your computer.
Data server	A computer or program that provides other computers with access to shared files over a network
Denial of Service	An attack that prevents or impairs the authorised use of information system resources or services
Encryption	Information is encoded using random mathematical `keys’ that only authorised users can unscramble.
Firewall	Hardware or software designed to prevent unauthorised access to a computer or network from another computer or network
Local Area Network (LAN)	Communications network (often wired) linking multiple computers within a defined location, such as an office building.
Proxy server	Server that acts as an intermediary between users and other servers, validating user requests
Secure Sockets Layer (SSL)	Technology that lets businesses communicate with customers in a way that stops data from being changed or disclosed
Spyware	Malware that passes information about a computer user’s activities to an external party
Two-factor authentication	Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction
Virtual Private Network (VPN)	Link(s) between computers or local area networks across different locations



How Colonial First State protects your information

We use every means possible to make sure the personal information you give us is safe so it can't be misused, changed, lost or accessed without authorisation.

We have strong security measures in place, and we follow strict guidelines and policies when it comes to customer data.

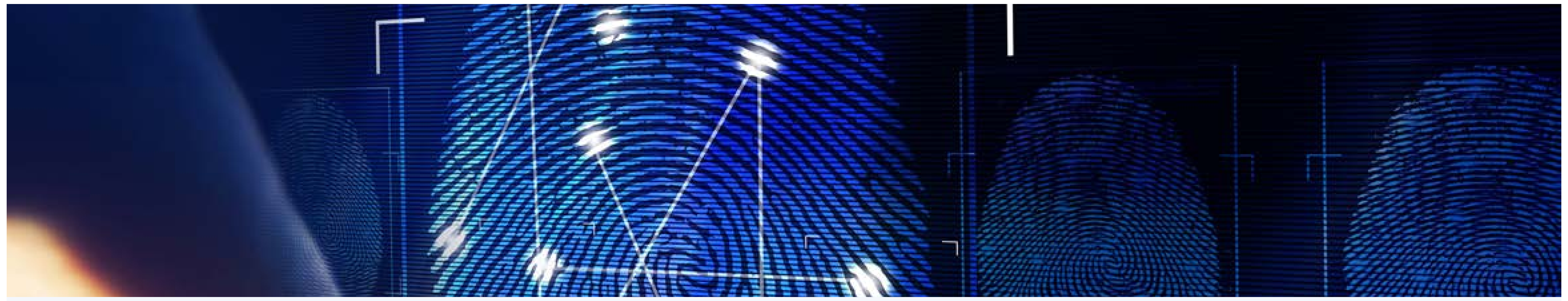
We regularly review and update these policies to make sure we keep up with the latest developments in cybersecurity.

Want to find out more?

To learn more about staying safe online,
go to colonialfirststate.com.au/cybersecurity

If you'd like more information about how Colonial First State keeps your personal information secure, talk to your financial adviser or call us on 13 13 36, Monday to Friday, 8am to 7pm, Sydney time.

For more information on Cyber Security, talk to your Adviser.



How we keep your information safe

- Only authorised people can access our computer systems
- Users can only access the information they need
- Sensitive data is stored and transmitted in an encrypted form
- We use firewalls, intrusion detection systems and virus scanning tools
- We use secure networks or encryption when we outsource data
- We provide secure storage for physical records
- We prevent unauthorised access to your information with alarms, cameras and guards
- When we no longer need information, we ensure it is effectively destroyed

Disclimer: This information has been prepared by Colonial First State Investments Limited ABN 98 002 348 352, AFS Licence 232468 (Colonial First State), and is the issuer of super, pension and investment products. This information is based on Colonial First State's understanding of current regulatory requirements and laws as at January 2018. This document is not advice and provides information only. It does not take into account your individual objectives, financial situation or needs. You should read the relevant Product Disclosure Statement (PDS) carefully and assess whether the information is appropriate for you and consider talking to a financial adviser before making an investment decision. A PDS for Colonial First State's products are available at colonialfirststate.com.au or by calling us on 13 13 36. 24726/0118