TOGETHER WE CAN REVERSE THE THREAT OF CYBERCRIME

REVERSE THE THREAT

STAYSMARTONLINE WEEK 8–14 OCTOBER 2018

Learn more about how to spot phishing scams, public Wi-Fi protection, software updates and strong passwords.

Lock down your online security today, at **staysmartonline.gov.au/reversethethreat**

Follow us on facebook **fb.com/staysmartonline**

Sign up to our free alerts **staysmartonline.gov.au/alert-service**

Source:

1 Norton, Norton Cyber Security Insights Report Global Results (2017)
2 Australian Competition and Consumer Commission, Targeting scams: report of the ACCC on scam activity (2017)
3 Symantec, Internet Security Threat Report Volume 23 (April 2018)
4 Symantec, Norton Wi-Fi Risk Report (2017)
5 Last Pass, The Psychology of Passwords: Neglect is helping hackers win (2017)

Stay Smart Online is an Australian Cyber Security Centre program.

ACSC Australian Cyber Security Centre

REVERSE THE THREAT

STAYSMARTONLINE WEEK 8–14 OCTOBER 2018

Lock down your online security today!

Australian Government

6.09
MILLION ADULTS
in Australia experienced
cybercrime in 2017[1]

One in four Australians were hit by cybercrime last year[1]. This Stay Smart Online Week we're bringing the Australian public, business and government together in a united effort to reverse the threat of cybercrime.

It's all about adopting smarter ways to avoid the pain, money and time it costs to recover from cybercrime. We can all take simple actions to keep ourselves, our families and businesses protected when connected.

This guide explains four simple ways you can lock down your online security to help us reverse the threat of cybercrime. You can find more tips on how to protect yourself online at

staysmartonline.gov.au/reversethethreat

BLACK SADBATH
AUSTRALIAN TOUR
FEB 30-31

Look a little off or sound a bit dodgy?

Fake messages that try to trick you into giving away your personal info, your online banking logins or credit card details are called phishing.

- Some messages look super real by using well-known logos and branding. They can be emails, SMS or come through social media. Phishing is one of the most common online scams.
- If you receive a suspicious message do not click on any links or open any attachments.
- Always think before you click to reverse the threat of cybercrime.

$50 MILLION
lost to online-based **scams in 2017**[2]

Think before you connect.

Be_Aware
Dodgy
Public_WiFi
Can.Do
Unlimited
Damage

Public Wi-Fi isn't always safe. Cybercriminals may be able to see the information being sent between your phone and the Wi-Fi hotspot. Don't let it cost you. Reverse the threat and get smarter about using public Wi-Fi.

- Turn off any auto-connect settings for Wi-Fi or Bluetooth on your devices.
- Pay attention to which network you select. Cybercriminals set up rogue hotspots with names that look like a legitimate network.
- Avoid online banking or shopping, sending confidential emails or entering personal details like passwords or your credit card details.

87%
of people have taken risks **ON PUBLIC WI-FI**[3]

Fix the cracks in your online security.

Hackers use these weaknesses in your devices to let themselves in. Updating your software is one of the easiest ways to protect yourself online.

- Update your phone, computers and apps to add new features, install bug fixes and most importantly fix security holes that could let cybercriminals in.
- Take the time to install software updates as soon as they pop up. Better still, set your system to auto-update.

80% OF ANDROID USERS & **23%** OF IOS USERS
haven't installed the latest **software updates**[4]

CoolHipster KangaClock Easy to remember, hard to hack.

Passwords are the key to your online life. Create strong passwords by stringing together a series of words that are easy for you to remember but hard for someone else to guess.

- Lock hackers out with different passwords on all of your accounts.
- Make them weird, wacky and memorable, but unique to you.
- Don't forget to use two-factor authentication to make yourself extra safe.

59% OF PEOPLE
use the same password **across all accounts**[5]