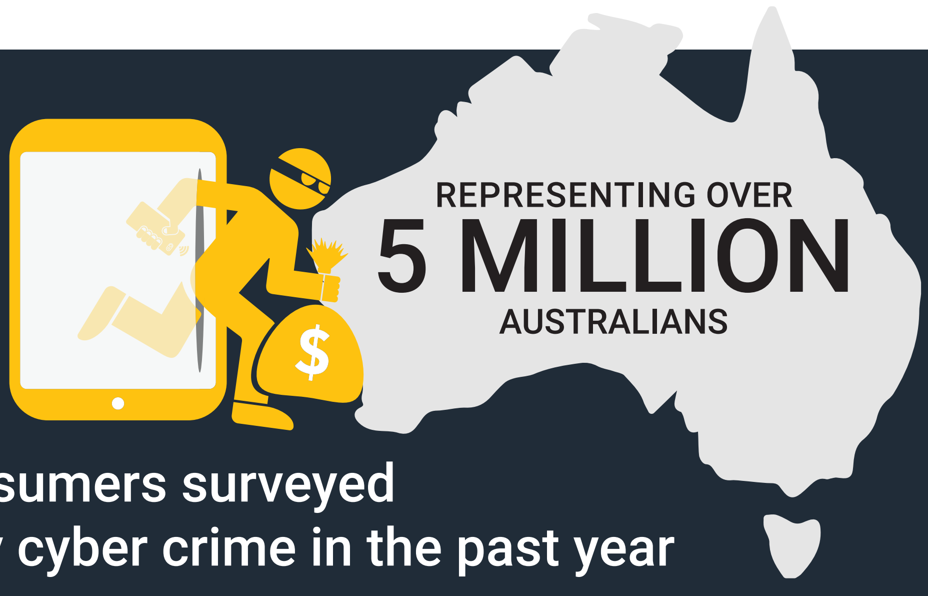
THE FACTS:
AUSTRALIAN CYBER CRIME VICTIMS

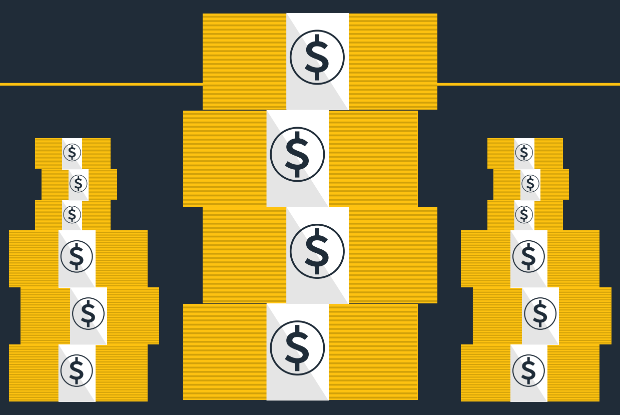
2018 Norton LifeLock Cyber Safety Insights Report - Australia



REPRESENTING OVER
5 MILLION
AUSTRALIANS

30%

of Australian consumers surveyed were impacted by cyber crime in the past year



38% of those impacted have lost some money to cyber crime:

AN ESTIMATED
$1.3 BILLION AUD

31% of Australians needed a week or more to resolve it

89% of Australians surveyed want to do more to protect their privacy, yet 50% say they don't know how

86%
SAY THEY ARE CONCERNED ABOUT THEIR PRIVACY

✓

86% have taken at least one step

Steps taken to protect personal information/online activities:	
55%	limited information shared on social media
48%	cleared or disabled cookies
39%	changed default privacy settings on devices
38%	read the T&Cs in full before installing or downloading a device or service
35%	stopped using public Wi-Fi
24%	use something other than your full name for social media profiles
19%	deleted a social media account
18%	used anonymous payment methods
14%	used a virtual private network (VPN) to encrypt information sent to and from my device
10%	used an encrypted email service
4%	other

!

but **14%** have not done anything

Consumers have low trust in providers to manage and protect their personal information

yet

68%
accept certain risks to their online privacy to make their life more convenient

Stay safer online with these best practices

- **Never open suspicious-looking emails:** Cyber criminals send fake emails or texts that may look legitimate. The links in these emails or texts contain malicious software that can download malware and spyware. The software may be able to mine your computer for personal information, which is then sent to a remote computer where the attacker could sell the information on the dark web.
- **Make use of a VPN on public Wi-Fi:** Many public Wi-Fi connections are unencrypted. This could give cyber criminals a chance to snoop on data being sent and received by your device. If there are software vulnerabilities on your device, attackers can inject malware to help them gain access to your data. In some cases, attackers create fake Wi-Fi hotspots purporting to be legitimate networks.
- **Own your online presence:** Carefully read the terms and conditions before opening an account or downloading an application, including social media accounts. Be sure to set the privacy and security settings on web services and devices to your comfort level for information sharing.
- **Get two steps ahead and manage your passwords:** Switch on two-step verification or multi-factor authentication wherever offered to help prevent unauthorised access to your online accounts. Always change the default passwords to something strong and unique on your devices, services, and Wi-Fi networks.

Norton™ LifeLock™

Source: Norton LifeLock Cyber Security Insights Report 2018 – Australia.
Facts and figures listed based on Australian respondents surveyed.