Survey Report

Australian Cybersecurity Awareness and Preparedness

A survey undertaken by ESET Australia reveals that Australians are generally aware of and concerned by internet security issues but that their preparedness to create a more secure online environment for themselves still lags behind their awareness of the issues.

ENJOY SAFER TECHNOLOGY™

Introduction

Australians remain confident of their awareness of cyber security issues but data still suggests that sometimes that confidence might be misplaced.

The Australian Competition and Consumer Commission's (ACCC) Targeting Scams 2019 report[1] for example, found that **Australians lost over $634 million to scams in 2019 which was a 30% increase over the previous year.**

The true cost of cybercrime to Australians is likely to be substantially greater, with the agency noting that **around 33% of people who lost money in scams in the previous five years had not reported that loss.**

Clearly, awareness and preparedness are not the same thing.

Consumer Awareness & Preparedness

In this survey of 2000 Australian internet users[2] the results indicated a generally healthy awareness of threats and the need to prepare for them among consumers.

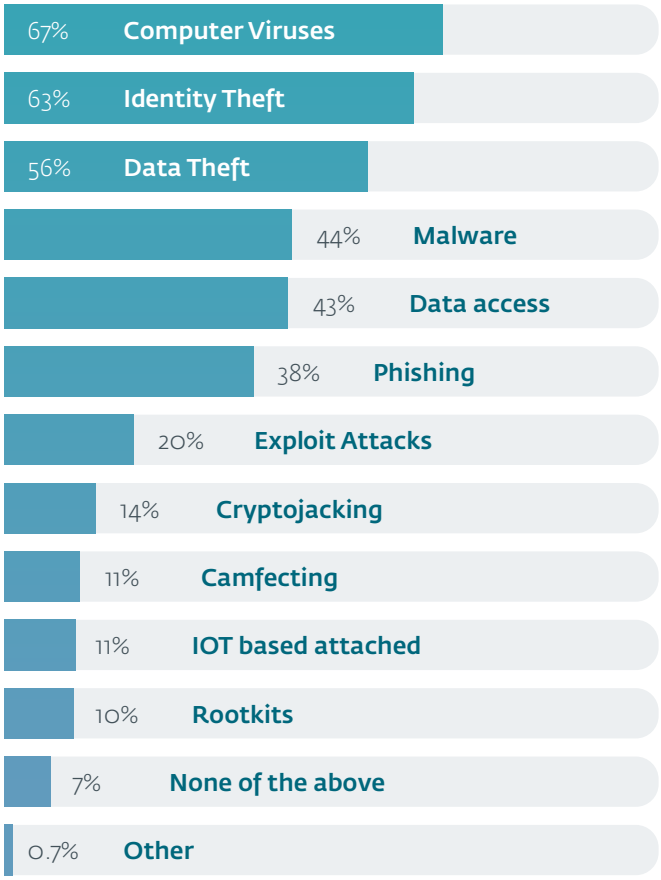
The survey found that 85.1% of respondents think that installing internet security on personal and home devices is either very or somewhat important and 81.6% were either very or somewhat concerned about internet security.

Respondents were also aware of the nature of the various threats. But while traditional threats like computer viruses (66.9%), identity theft (62.5%), data theft (55.5%) and ransomware (43.9%) were of the most concern, threats like phishing (38.1%), exploit attacks (19.6%) and IoT-based (Internet of Things) attacks (10.6%) had comparatively low concern levels.

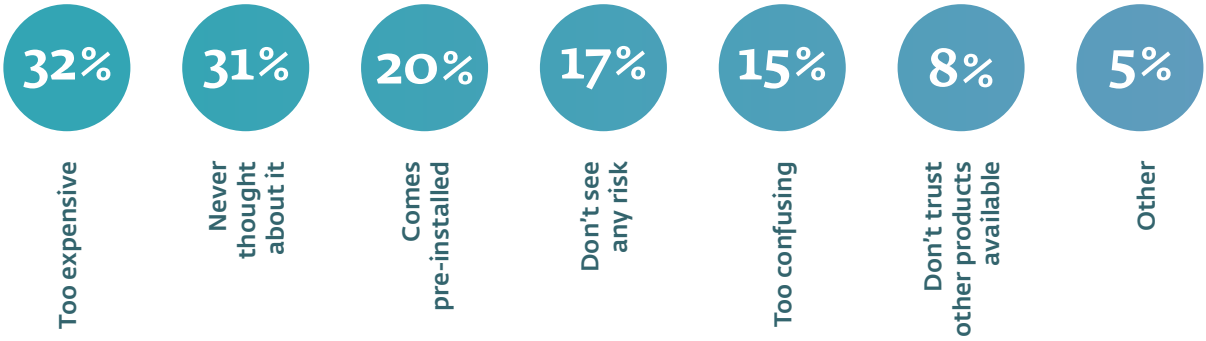
Despite this level of awareness, 23% have never installed a home antivirus or internet security product on any of their devices while 5% can't recall having done so.

The most common reasons cited for not doing so include expense (32.1%), never having thought about it (31%), protection coming pre-installed with the device (20.1%) and not seeing a risk to themselves (17%).

What internet security issues might you be concerned about?



Why have you never installed an internet security/antivirus product?

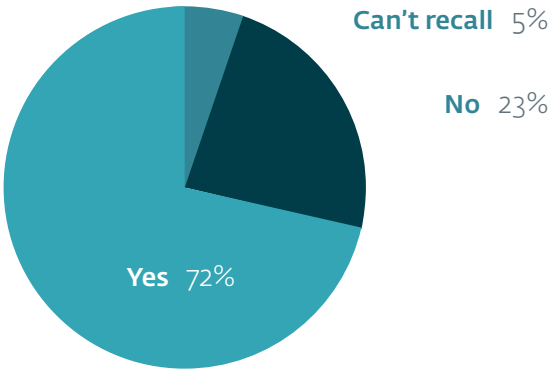


Respondents reported high levels of ownership of internet-connected devices, with 88.1% owning a smartphone, 74.3% a laptop, 47.7% a desktop, 51.2% a tablet and 55.2% a smart TV.

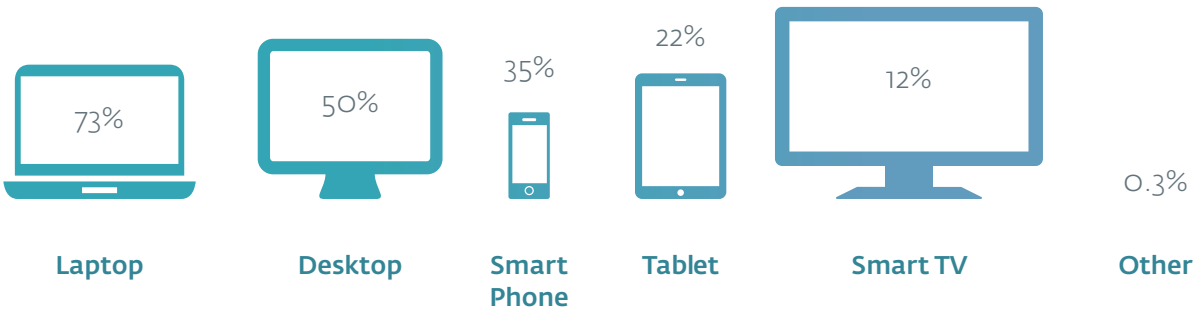
Despite this proliferation of devices that users are connecting both to the internet and their personal and work networks, the focus of internet security for many remained on their laptops and desktops.

While 73.1% had installed protection on a laptop and 49.3% on a desktop, only 35.3% had installed protection on a smartphone, 21.5% on a tablet and just 11.9% on a smart TV.

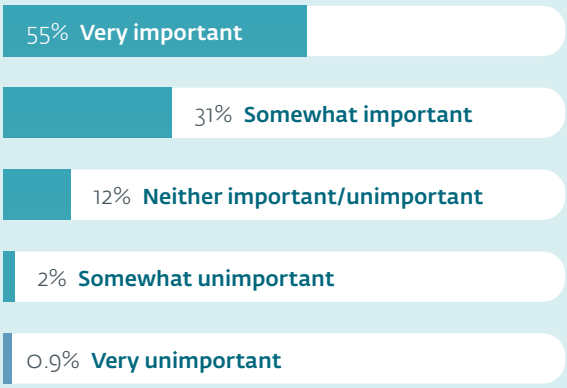
Have you ever bought or installed an internet security / home antivirus product on any of your personal or home digital devices?



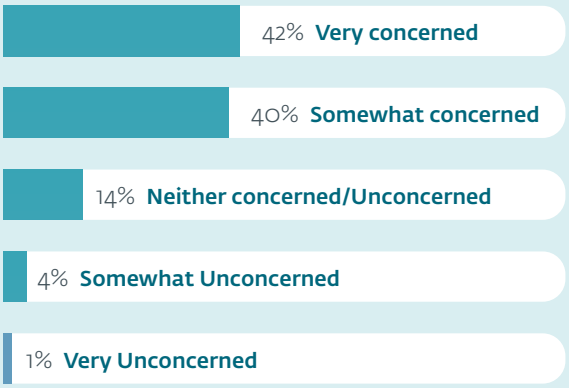
On which of your personal devices have you installed internet security /home antivirus products?



How necessary do you think internet security/home antivirus products are for personal/home based devices?



How concerned are you about internet security?



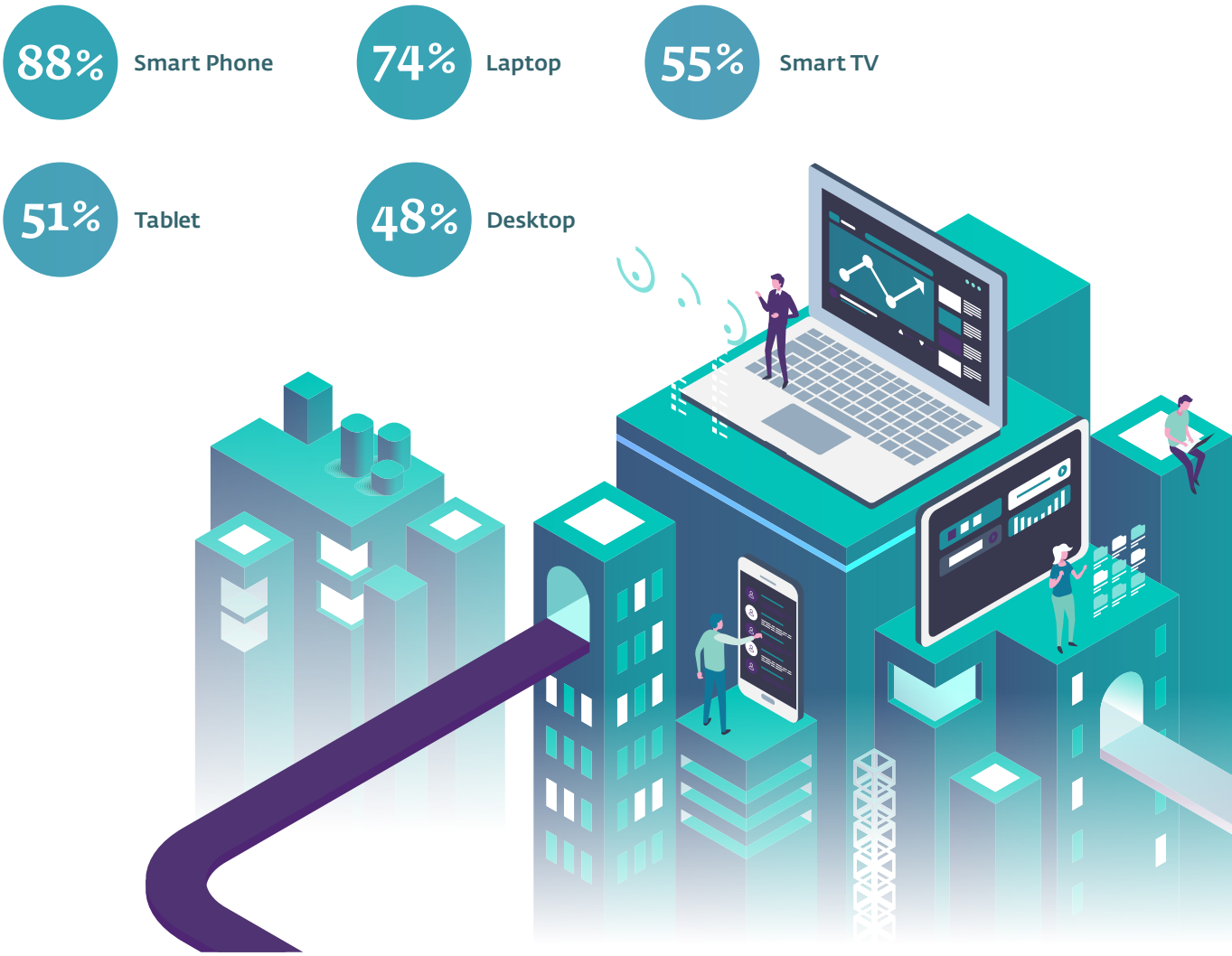
A Complex Threat Surface

The survey results indicate that while users are concerned about internet security and aware of the nature of potential threats, many are not adequately prepared to protect their online space from emerging threats.

Malicious actors are primarily motivated by money and will try to defraud people using whatever methods and technologies are available.

This is not limited to technical exploits or malware but includes social engineering where the attacker attempts to manipulate the victim onto divulging information that will allow them further access.

Which of the following digital devices do you currently personally own and use?



The Australian Cyber Security Centre (ACSC) noted in its July 2019-June 2020 Annual Cyber Threat Report that "Phishing and spearphishing remain the most common methods used by cyber adversaries to harvest personal information or user credentials to gain access to networks, or to distribute malicious content. Over the past 12 months the ACSC has observed real-world impacts of ransomware incidents, which have typically originated from a user executing a file received as part of a spearphishing campaign."[3]

Combating such attacks requires a combination of technology – spam and malware filters operating both at the email provider and individual's device level – and awareness on the part of the user.

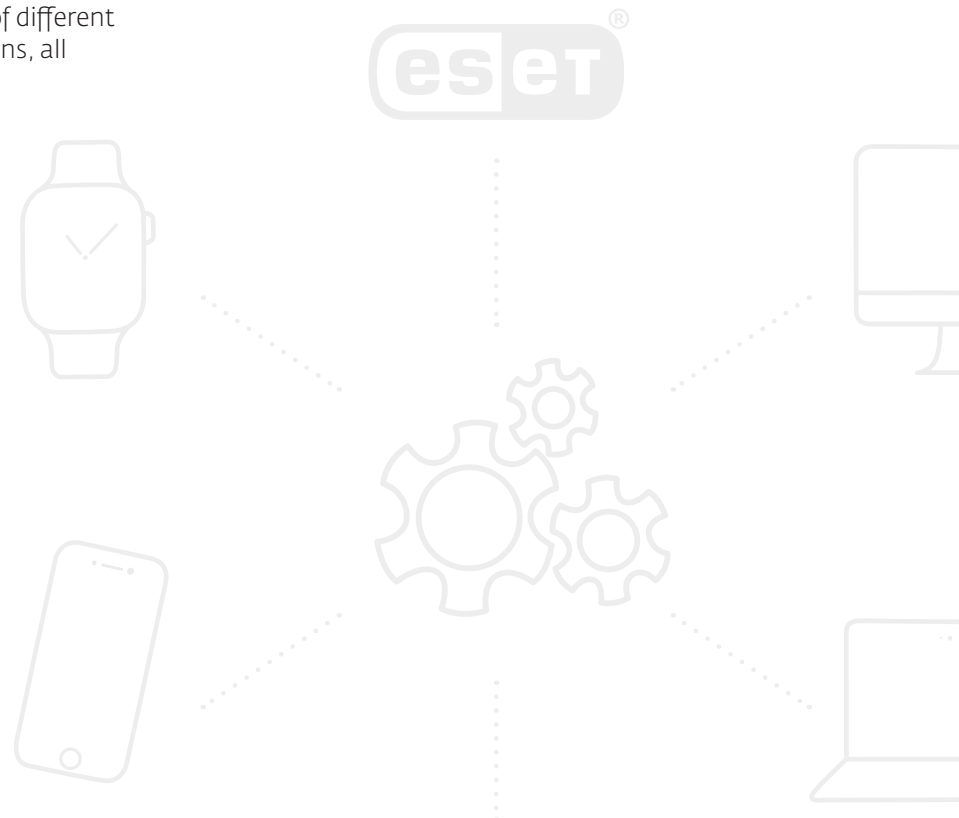
The ACSC noted that "Australians need to be mindful that cyber adversaries are constantly looking for vulnerabilities and weaknesses in systems and networks. The ACSC continues to identify many products and services being adopted and implemented by organisations that lack 'secure by design' principles."[3]

Indeed, the growing digital ecosystems present in Australian households adds complications to users' efforts to secure their online environments. Whereas in the past users needed only to be concerned with protecting a few devices, the modern household is likely to have multiple devices, running a range of different OSes and fulfilling different functions, all connected to the internet.

The growth in the use of IoT devices such as smart home hubs and smart TVs has created an expanded and complex threat surface for households. ESET Research in its Q2 2020 Threat Report[4] noted that smart devices often rely on a single security layer — password-protected access to their administrative interfaces. Despite the key role of this security measure, thousands of users do not follow basic best practice and change the default password after unboxing and plugging in their smart devices. Q2 2020 data from ESET's router vulnerability scanner module shows that several thousand of the over 100,000 devices scanned used the following weak passwords: admin, root, 1234, guest, password, 12345, support, super, Admin, pass.

ESET Research also noted that all top ten IoT vulnerabilities in Q2 2020 originated from before 2016, demonstrating the "longevity" of IoT flaws and the reluctance or inability of vendors and/or users to patch them.

With more IoT and smart devices finding their way into homes users need to be aware of the risks and take appropriate measures to ensure they are following good cyber hygiene. This includes installing any updates from manufacturers and making sure they are following robust security practices around passwords and Wi-Fi security.



Security Starts With Behaviour

The number of Australians who fall victim to cyber fraud of some type shows that technology alone cannot guarantee a safe digital environment. Many successful cyber frauds start with the attacker either exploiting their victim's behaviour via phone or email scams or targetting their use of weakly secured environments outside the home, such as using public Wi-Fi networks while doing such activities as online banking.

Using the Wi-Fi networks available in places like hotels is also a risk. The FBI's Internet Crime Complaint Center (IC3) recently issued a warning about the risks of using hotel Wi-Fi networks to access sensitive and work-related information, stating "malicious actors can exploit inconsistent or lax hotel Wi-Fi security and guests' security complacency to compromise the work and personal data of hotel guests."[5]

So users need to be aware of risks and adapt their online behaviour according to the situation. With the right internet security tools, good awareness and the correct cyber hygiene behaviour both in the home and when out and about, you should be able to enjoy your online experience without stress.

Here's our top tips for making your digital environment safer:

TAKE SOME CYBERSECURITY AWARENESS TRAINING

Many people feel confident they know how to spot a scam and avoid online threats but complacency is the cyber criminal's best friend. You might laugh at the obvious email from an alleged Nigerian prince but cyber criminals have become very sophisticated in constructing phishing and spearphishing attacks capable of fooling even tech-savvy users. Cybersecurity awareness training is a great way to upskill yourself and your family so you know how to enjoy your online experience in the safest way. We have free, user-friendly online cybersecurity training available here.

HELP YOUR KIDS STAY SAFE

Today the internet is part of the lives of children at a young age so they need to learn how to have fun online while staying safe. SaferKidsOnline is a great place for both parents and children to learn how to safely navigate the online world. Dedicated to building a safer online environment for children, by educating them, their parents and teachers about child cybersecurity, SafeKidsOnline is packed with tips and articles, plus activities for kids to help them enjoy a more secure digital world.

USE A PASSWORD MANAGER

We all know we should use secure, unique passwords for each and every website we visit but the reality is few of us can remember them all or deal with the inconvenience of writing them down. Poor password security is one of the major ways your online environment is likely to be threatened. Thankfully there is a simple solution; a password manager. Password managers store your usernames and passwords in an encrypted online service, allowing you to ensure you have a well-constructed unique password for each site without having to remember them all. Some will generate strong, random passwords for you, removing the temptation to reuse common phrases and numerical sequences. Having an online environment based on strong, unique passwords is one of the simplest and most effective ways to protect your digital experience.

BE SMART WITH YOUR SMARTPHONE

The smartphone is probably the device that most of us use the most. Since it's connected to the internet, you have to protect it. Most smartphones can now be protected with an endpoint security solution that can keep most threats at bay. Meanwhile, for added protection, you should also encrypt all the sensitive data on your phone, so you'll make it harder for cybercriminals to make use of your data even if they worm their way into your device. You can boost the security of your smartphone by applying the tips we listed out in our 20 tips for 2020 article.

SECURE YOUR WI-FI ROUTER

Securing your router should be the first step you take towards securing your internet connection; after all, it is the gateway to all your connected devices. A common mistake people make once their Wi-Fi router is installed is that they will stick to the default settings. While it is convenient it can pose a huge security risk, therefore you should immediately change both the password used to connect to the router as well as the password used to access its settings. When changing the router's password choose the WPA2 option (or WPA 3 on newer routers if all your devices can connect to it). And, as with all devices, don't forget to keep it updated to the latest firmware; while many routers do that automatically, it doesn't hurt to check every now and then to make sure that everything is up to date. For further advice, you can check out our handy article on ways to check if your router is configured securely.

UPDATE YOUR DEVICES

We cannot stress this point enough: update your devices regularly. True enough, with many connected devices it may not be exactly easy, or even possible, to put this advice into action. Still, any fixes, security patches, and updates should be applied as soon as they are released either to remedy specific vulnerabilities that, if left unattended, could be exploited. Do not disregard update prompts or hold off on installing a patch if you learn that one is available.

PROTECT YOUR SMART TV

Most modern TVs have smart features embedded and even non-smart TVs are frequently upgraded with external streaming devices like a Chromecast. However, like various other devices, smart TVs can be compromised and hijacked by cybercriminals who could exploit vulnerabilities to control the TV remotely, or it could be infested by malware. To protect your smart TV, you should start by properly configuring it and going through its settings in detail; while you're at it you should check for any firmware updates as well, and last but not least there are security solutions available that can be downloaded that will boost the security of your device.

BE SAFE, HAVE FUN

While the number and nature of internet-connected devices in the home is bringing new security challenges, safely enjoying the digital environment all these great new devices bring doesn't have to be a major chore. Making sure you're educated about the risks and how to follow good cybersecurity practices, have installed internet security tools on all applicable devices and properly set up your devices and passwords for optimal security will take the stress out of your online experience and leave you with the time to enjoy the things it has to offer.

To learn more

Overall, Australian internet users are generally aware of the risks of online activities and are at least taking some steps to protect themselves. However, most users could potentially be more secure either through better password management or a clearer understanding of the risks, which would result in more cyber aware behaviour.

To report a cyberattack, go to:

www.cyber.gov.au/report

To learn more about how to stay safe online, go to:

www.eset.com.au

www.welivesecurity.com

1 https://www.accc.gov.au/system/files/1657RPT_Targeting%20scams%202019_FA.pdf

2 Nationally representative sample based on ABS strata

3 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

4 https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf

5 https://www.ic3.gov/media/2020/201006.aspx