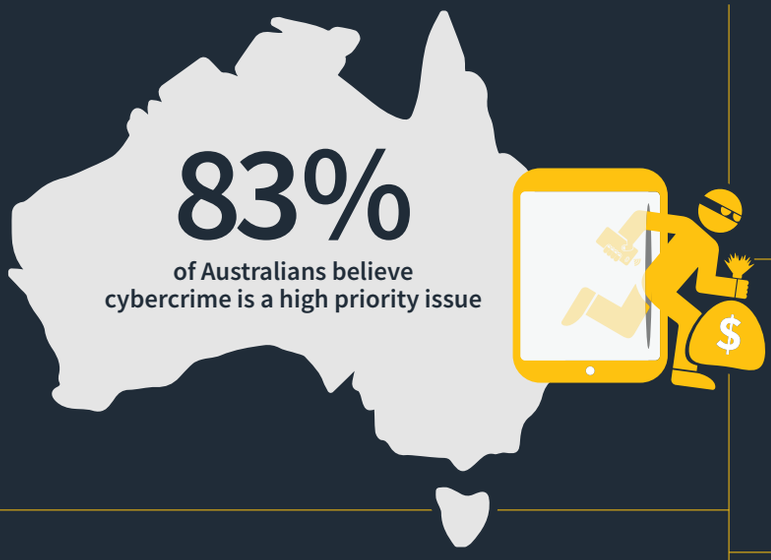
Cybercrime at tax time

Norton LifeLock 2019 Tax Time Survey – Australia



83%

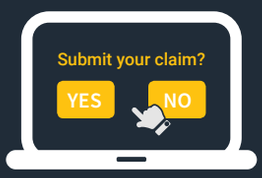
of Australians believe cybercrime is a high priority issue

58%

of working Australian respondents[1] agree they are more wary of cybercrime at tax time than at any other time of year

Over half of Generation Z Australian workers surveyed think cybercrime affects other people but not them, **yet they engage in risky online behaviours like sharing their tax returns using public Wi-Fi**
(12% of respondents)

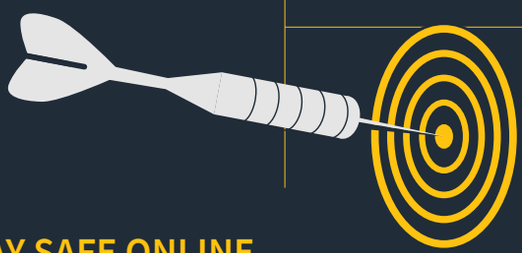
1 in 5



working Australian respondents do not think it is safe to complete their tax return online

61%

of working Australian respondents say they would worry about any amount of financial loss as a result of cybercrime



42%

of working Australian respondents claim to have been targeted by ATO impersonation scams in the past

6 TOP TIPS TO STAY SAFE ONLINE

Mark Gorrie, Senior Director and Security Expert ANZ, Norton LifeLock

→ Be cautious of Australian Taxation Office (ATO) impersonation scams

The ATO may use letters, email, phone calls, or SMS to contact you, but will never ask for: your Tax File Number or bank details via email or SMS; and will never contact you using social media sites like Facebook or Twitter to ask for your personal information; nor email you from an unofficial email address.

→ If you're not sure about the validity of any communication from the ATO, call them directly

Take down their information, hang up, and call the ATO's office using a number from the official website or a previous letter you have received from the ATO to validate its identity and its request. You can also report suspected scam emails by forwarding them to ReportEmailFraud@ato.gov.au

→ Use comprehensive security software on your computer and backup regularly

Norton LifeLock research found that 47% of Australian workers claim to not use a comprehensive security solution on their personal mobile, laptop, tablet or desktop computer. Using robust security software, such as Norton Security Premium, to protect your home network and personal devices is the first line of defense against cybercriminals.

→ Look for misleading signals in an email and never open attachments if you are unsure

Key tell-tale signs that an email may be illegitimate include: incorrect logos within the email; the communication does not address you as the recipient by name; it is not sent from a legitimate vendor email address; is unexpected; the message contains poor grammar; and/or, the email asks you to click a link that appears to lead to a government website but when hovering over the link it does not lead to an official web address.

→ Know the status of your tax affairs and your accounts

Get to know your finances to ensure you can identify any unexpected changes in your account as a result of cybercrime quickly. If you know you don't have debt with the tax office, then an email or phone call that states otherwise cannot be real.

→ If you're filing your taxes online, use a secure Wi-Fi connection or a VPN

66% of Australian workers claim they do not use a VPN for their personal mobile, laptop, tablet or desktop computer, yet eight per cent of Australian workers have sent personal financial info/documents via public Wi-Fi. If that's you, one of the best ways you can protect yourself is to make sure your internet connection is secure and not a publicly available network. If you are not sure about the security of your internet connection use a VPN. Products such as Norton Secure VPN can help protect your personal information by encrypting all the data you send and receive online.

Norton™ LifeLock™