Ransomware is a type of malicious software or malware that locks or encrypts your digital files making them or even your whole device unusable. Criminals aim to trick people into downloading ransomware, disrupting and halting work before demanding money in return for unlocking the files. So how could ransomware get on your device? It could come from malicious websites or links, email attachments, links in emails, on social media or messaging apps, downloadable applications or though software vulnerabilities on your devices which could allow malware to be installed. Thankfully, there are ways to reduce the risk of ransomware. Install software updates and turn on automatic updates. This is particularly important for antivirus software. Never click on a link or open an attachment in a suspicious email. Back up your data regularly and test restoring it. And finally create an incident management plan in case you are affected by ransomware. If you experience a ransomware event, try the following. Disconnecting your device form the internet. If possible, stopping the ransomware from running. On Windows devices, using task manager to identify and stop it. On Mac, holding the power button to shut it down. On Windows devices, running a malware scan. Then getting help by seeking assistance from an IT professional. Finally, be sure to report the incident to the Australian Cyber Security Centre. Remember paying the ransom does not guarantee that your files will be unlocked and may even make you a target for further attacks. Prevention is better than cure. Learn how to protect your business from online threats at nab.com.au/security. NAB more than money.