access
freedom to do more

Employee Checklist

Keeping your data safe while working from home

If you've joined the "working from home" workforce, the reality is that you need to ensure you're not a security threat to your organisation by following a few simple steps:

Phishing	Phishing emails or calls are designed to make you provide information by posing as people from organisation, 3rd party providers, customers or suppliers. **Tips to identify:** 1. If you don't recognise the sender, don't engage or click, download or open the email. Hover over the sender address or clickable links to reveal the source. 2. Look for mistakes/bad grammar. 3. Be aware of the tactics used – use of authority and urgency to scare you into taking action or curiosity and desirability to lure you into seeking more information, or similarity and branding to make the email appear trustworthy.	✓
Your home network	If you're accessing a wifi network connection, it's likely visible to your neighbours, ensure: 1. Your administration password is different to the password your internet service provider gave you when you set up your internet and make sure this new password is different to your other passwords you use. 2. Your password is strong and best practice. That means using a passphrase which is a combination of 3 or more words e.g. donut armchair candle – with a few added numbers and special characters	✓
Password manager	For optimal password protection: 1. Use a password manager, such as LastPass, which removes the need to remember a multitude of passwords. Passwords and other account information are encrypted and stored, accessible with a master password. 2. If possible, enable two-factor or multi-factor authentication on your devices and accounts. This method uses two or three of the following to confirm your identity – something you are (a fingerprint), something you have (a code sent to a mobile) and something you know (password). IT can recommend a service.	✓
BYOD	If you're using your personal device at home: 1. Ensure the latest versions of operating system, software and applications are up to date. 2. Check your virus and malware protection is active and up to date. 3. Check other devices connected to the same wifi network to ensure hackers can't find backdoors to your network through another device. 4. Ensure you download software from the correct and verified site and don't go for unknown alternatives.	✓
Keeping your data safe	Once you've sorted your devices and passwords, some considerations for best practice for sharing and keeping your information safe: 1. Don't store business critical data directly on your desktop. 2. File sharing should be via a solution that's approved by your organisation to ensure security of information. 3. Don't let your kids (or anyone else) use your work devices.	✓

The Access Group is a leading provider of HR, Digital Learning, Payroll and Accounting software delivered through an integrated, single sign-on, cloud platform that transforms the way business software is used, giving every employee the freedom to do more - **www.theaccessgroup.com.au**