



CYBER ESSENTIALS

Small Office/Home Office



As a small business operator, you work long hours focused on what you do best to deliver value and service to your customers.

For most technology is an important tool, helping to keep small business going by increasing efficiency, improving quality and providing direct access to markets in distant regions, but are you risking it all?

Each year 60% of small businesses across Australia will experienced a preventable Cyber Security incident. Some will never recover.

Protecting against the majority of these risks doesn't require expensive software or expert knowledge, but it does require a little of your attention.

Cyber crime is on the rise. In 2018 small business saw an increase of:

56% in attacks against business websites

12% in ransomware attacks against business

33% in mobile ransomware infections

48% of malicious email attachments are files disguised as an invoices or receipts

Did you know that:

- Cybercrime costs Australia business an estimated \$1 Billion annually
- 41% of attacks can cost up to \$5000 to fix
- 60% of cybercrime is targeting small business yet only 10% of businesses think it's a priority
- Dependant on your business, there may be regulatory requirements on how to deal with cyber attacks which you should know about



Cyber Basics



Cyber Essentials




Cyber Ready










Cyber Robust



Cyber Resilient



It's estimated that more than 95% of all cyber attacks can be prevented by following these basic rules:

-  You have all the **Cyber Basics** covered and your devices are being updated, up-to-date anti-virus is installed, all passwords are different, your Wi-Fi router is secure and any critical business data is routinely backed-up (see Cyber Safe - Cyber Basics).
-  Use multi-factor authentication for your critical apps, such as internet banking, business email, etc. This makes it much harder for an attacker to access your accounts.
-  Start using a password manager to increase password complexity and security (and help your memory!).
-  Restore data from your backups as a test. You don't know for sure if your backups work until you know you can restore them. This could be your saviour in a ransomware attack.
-  Use a supported, up-to-date web browser and block or uninstall Adobe Flash and Java unless they are necessary for business. Consider installing an anti-malware browser extension in your browser.
-  Ensure you know who has access to your work computer.
-  Practice safe handling of credit card data. Avoid storing credit card details in your system, never write down details (e.g. post-it notes) and discourage customers from email you their credit card information.

For further information go to cyber.gov.au/small-business



NCC Group assisted in the development of this framework. NCC Group is a global cyber security company with offices in Sydney and Melbourne nccgroup.trust/au

