



CYBER READY

Small – Medium Enterprise



You've made a substantial personal investment in both time and money to set up and maintain a successful business. A typical day consists of juggling endless priorities, leading your staff and continuing to building a positive brand image.

As your business continues to grow, so does your dependence on complex technologies and those you entrust to keep those systems safe & working efficiently. Unfortunately this growth

also means you become a more attractive target and your cyber risk increases from those who would hope to exploit your success.

Whether it's through direct system vulnerabilities, inadequate business processes or untrained staff, small -medium sized businesses are continually at risk of financial and reputational loss. A little of your time could save you now could save you everything.

Cyber crime is becoming big business. In 2018 it was reported that:

- 10%** of all URLs were malicious
- 20%** increase in identity theft attacks against business owners through their social media interactions
- 4,800** website payment card attacks occur each month
- 5,200** attacks per month against business routers and security cameras

Did you know that:

- Australian Mandatory Breach Laws require that you advise your customers of any data breach that involves their data
- There may be fines imposed for non-compliance, but the biggest cost may be for your brand
- It only takes one person in your staff to click a phishing email link to start an attack on your business



Cyber
Basics



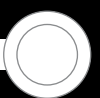
Cyber
Essentials




Cyber
Ready









Cyber
Robust



Cyber
Resilient



Follow these rules to help reduce your cyber risks:

-  All the **Cyber Essentials** rules are in place and your devices are being updated, up-to-date anti-virus is installed, unnecessary options in your browsers are turned off, multi-factor authentication is in use, and critical data can be restored from a backup.
 -  Block Office macros from the Internet and only allow trusted digitally signed macros to be used.
 -  Disable unneeded features in operating systems and applications. Remove any unwanted, or unused, applications from all devices. Restrict administrative access to all devices.
 -  Consider adding extensions to browsers to further enhance security and privacy.
 -  Train staff to recognise phishing attacks and how to respond. Remember these are attacks against PEOPLE not against devices!
-  Plan to protect your critical business data. Consider the data's sensitivity, it's value in monetary terms and the loss to the business if it were breached (both in monetary and reputational terms). Does it include your customers personally identifiable information? How is it protected? Where is it stored? Is it encrypted? Is it backed up? Who has access to it? Remember it may be mandatory for your business to report a breach or loss of data.

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

