Small Business Connect

Department of Employment, Small Business and Training

Australian Cyber Week – 14-18 November 2022

Welcome to a special Australian Cyber Week 2022 edition of Small Business Connect.

Business owners know how important cyber security is, but do you know what to do to check your business' cyber security health and importantly, what to do to improve it?

Australian Cyber Week is all about helping you prevent or minimise the impact of cyber incidents in your business or home.

In this issue:

- Small Business Cyber Security Guide
- What to do now to protect your information security
- Webinars to help protect your business from cyberattacks
- Cyber Security Assessment tool
- Test your password security
- Are you looking for someone to help with your cyber security?
- Have you been compromised by a data breach?
- So you think you have been hacked?
- Stay in the know – Scamwatch

Small Business Cyber Security Guides

The Australian Cyber Security Centre has information online to help small businesses protect themselves from the most common cyber security incidents.

For an overview of cyber security measures the ACSC's Small Business Cyber Security Guide is a great place to start.

Step-by-step guides are also available which detail cyber security instructions for specific software, applications and devices.

1. **How to update your operating systems**
    - Update Android – keep software on your phone or tablet up to date
    - Update Microsoft Windows – turn on automatic updates on your PC
    - Back-up and restore – how to back up and restore content on your PC
    - Update Apple iOS – turn on automatic updates on all your Apple devices
    - Back-up and restore files on Apple iOS and Mac
    - Manage user accounts for Microsoft Windows 10 and Apple macOS.

2. **Password security**
    - How to change your passphrase for Microsoft Windows 10, macOS and Apple ID
    - How to check your desktop email account security for Outlook and Google
    - Turn on Two- and Multi-Factor Authentication
        - Apple ID
        - Twitter
        - LinkedIn
        - Yahoo!
        - Instagram
        - Facebook and Facebook Messenger
        - Google Accounts
        - Microsoft Accounts
        - Signal
        - WhatsApp.

3. **How to protect your computer from malware**
    - Turn on real-time protection in Windows 10 to stop malware from being installed on your device
    - Turn on Ransomware Protection for Microsoft Windows 10 to protect your business from an attack on your files
    - Perform a malware scan for malicious software.

Visit www.cyber.gov.au to learn more about the Small Business Cyber Security Guide and any of the step-by-step guides.

What to do now to protect your information security

While there is no magic wand to protect against all cyber threats, below are the top six information security priorities for a small to medium business.

You can learn more about how you can protect your business' information security in the downloadable Small Business Cyber Security Guide.

1. Automatically update your operating systems, software and apps
2. Regularly backup your important data

3. Enable multi-factor authentication (MFA) on important accounts wherever possible
4. Manage who can access what within your business
5. Where MFA is not possible, use passphrases to protect accounts and devices
6. Train your staff in cyber security basics

Webinars to help protect your business against cyberattacks

The Queensland Government, in partnership with Qudos Management has developed three free webinars about how to protect business against cyberattacks. These webinars are in no-nonsense plain English and go through the cyber security steps that small business owners need to take to protect their business.

To view a recording of the first two webinars check out:

1. Introduction to Information Security Management.
2. Information Security Management and the new edition of ISO27001

The third webinar, Information Security Management: Developing your System is on 29 November 2022.

Register here for your free one-hour webinar.

Cyber Security Assessment Tool

A Cyber Security Assessment Tool is available to help you identify what your business is doing well, and where your business can improve when it comes to cyber security.

This tool will ask a series of questions about how you manage your cyber security risks and provides a downloadable PDF list of recommendations to action.

All you need is your ABN to get started Cyber Security Assessment Tool (business.gov.au)

Test your password security

Often, the cause of data breaches are compromised passwords. Why is password security important? Not having a secure password could have dire consequences, including identity theft and sharing of sensitive data.

Some of the best practices for creating secure passwords are:

- Use 16 characters or more, these are more secure than the usual 6-8 character long passwords.
- Use a combination of letters, numbers and special characters.
- Try not to include personal information like your address, phone number. It is also best not to include any information that can be found on social media like pets' or kids' names.

- A password should not be shared with any other account.
- Try not to use consecutive letters or numbers.
- Your password should not be the word ‘password’.

Secure your information and put your password security to the test with the Password Strength Tool.

Are you looking for someone to help with your cyber security?

AUCyberscape is Australia’s first consolidated online destination for understanding Australia’s cyber security capabilities.

You can use this site to find Australian cyber security companies and their products, services, business solutions and sector experience. The platform is free to users and providers.

A number of Queensland based companies are now registered on the site, where you can look them up here.

Have you been comprised by a data breach?

have i been pwned is a free online resource for anyone wanting to quickly assess whether their phone or email has been at risk due to an online account of their being compromised, or ‘pwned’ in a data breach.

Using the website is easy – enter your home email address, business email, or phone details to see if you have been caught up in a data breach. The best feature about this website is you also get notified if a data breach happens in the future!

To find out if you have been compromised or ‘pwned’, visit have i been pwned.

So you think you’ve been hacked?

If you can’t access your account, have received a strange phone call from someone that wants to access your device, accidentally used a fake website or opened a suspicious email or message, it is possible that you have been hacked and you need to act now.
Follow the steps on Australian Cyber Security Centre’s Have you been hacked? webpage to find out if you have been hacked, or call the Cyber Security Hotline on 1300 292 371.

Stay in the know – Scamwatch

Scamwatch is run by the Australian Competition and Consumer Commission (ACCC) and provides information to consumers and small businesses about how to recognise, avoid and report scams.
Your best defence against scams is to stay up to date with the latest Scamwatch advice and subscribe to Scamwatch for email alerts on the latest scams.

If you think you’ve been scammed, report it now!

Stay connected

In addition to this newsletter, you can receive the latest information from the Queensland and Australian Governments by visiting the Business Queensland website.

Follow us on social media on the Business Queensland Facebook page.

For more information, visit
business.qld.gov.au or call 1300 654 687

Queensland
Government