Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

COVID-19: Protecting your small business

MARCH 2020

Introduction

This guide has been developed to help small and micro businesses adapt to working during the COVID-19 pandemic. This document will help businesses with simple and actionable advice in order to both identify common and emerging cyber threats and develop resilient business practices to protect themselves.

The cyber security basics

The COVID-19 pandemic has heightened concerns throughout society, including around cyber security. No matter the type of cyber threat, there are simple steps that businesses can take to protect themselves.

Watch out for scam emails (phishing)

Scam emails or phishing (pronounced 'fishing') are emails that are often made to appear as if they were sent from individuals or organisations you *think* you know, or you *think* you should trust. They are designed to trick individuals out of their money and information.

Phishing communications often mimic professional phrasing, branding and logos of authentic businesses in order to appear genuine. They are designed to defraud individuals and businesses by: requesting or pretending to confirm personal information, passphrases or credit card numbers; demand payment for a fake account; or by tricking them into clicking a harmful link or attachment. Attachments may contain malware, which is software designed to harm your computer or to gain access to your computer without your knowledge.

Phishing is not just limited to email. These scams are delivered via SMS, instant messaging and social media. Phishing is becoming increasingly difficult to identify, as criminals adapt their methods and find new ways to steal money and data.

Small and micro businesses should:

- Read the Australian Cyber Security Centre (ACSC) Threat Update: COVID-19 Malicious Cyber Activity which details recent COVID-19 phishing attempts.
- Do not open messages or their attachments, or click on links from unfamiliar individuals or organisations.
- Remember that reputable organisations including banks, government departments, online shopping and social media companies will not call or email to verify or update your personal information. This includes companies such as Amazon, PayPal, Google, Apple and Facebook.
- Use spam and message scanning services offered by your email, SMS or social media providers to filter potentially harmful content.

- Do not provide personal information to unverified sources and never provide someone with remote access to your computer.
- Use multi-factor authentication (see advice below) on all important services such as email, bank and social media accounts.

See the ACSC's guidance on Detecting Socially Engineered Messages.

Update your software

An update is a new, improved or safer version of installed software (an operating system or application) on computers and mobile devices.

Small and micro businesses should:

- Turn on automatic updates for operating systems (such as Microsoft Windows or Apple iOS/macOS) and applications (such as antivirus and web browsers).
- Set a convenient schedule for automatic updates to avoid disruptions to your business as usual activities.
- If automatic updates are unavailable, regularly check for updates from vendors and install them as soon as possible.

See the ACSC's Step-by-Step guidance on how to turn on Automatic Updates for Windows 10 and Automatic Updates for iMac & MacBook and iPhone & iPad.

Use strong unique passphrases

Passwords are passé! Pass*phrases* are the first line of defence for your accounts. Passphrases grant access to a computer, application or online service and are most effective when they are unique to a single account.

Small and micro businesses should:

- Ensure staff use strong unique passphrases for every account.
- Never share passphrases with others.
- Keep your passphrases secure. Never write a passphrase down or leave them where people might find them.
- Never choose to let your web browser remember passphrases.

See the ACSC Small Business Cyber Security Guide for guidance on creating strong passphrases.

Enable multi-factor authentication

Multi-factor authentication is one of the most effective security controls you can implement to prevent unauthorised access to computers, applications and online services. Multi-factor authentication typically requires a combination of proofs, such as:

- Something the user knows (a passphrase, PIN or an answer to a secret question).
- Something the user physically possesses (such as a card, token or security key).
- Something the user inherently possesses (such as a fingerprint, or retina pattern).

Using multi-factor authentication makes it much harder for cybercriminals to attack your business. Cybercriminals might manage to steal one type of proof of identity (for example, your passphrase) but it is very difficult to steal the correct combination of several proofs for any given account.

Small and micro businesses should:

- Use multi-factor authentication whenever possible, especially for important accounts such as email, banking and social media.

See the ACSC's Step-by-Step guidance on how to turn on multi-factor authentication for Apple ID, Facebook, Gmail and Twitter.

Backup your data

A backup is a digital copy of your business' most important data (for example, customer details or sales figures). This data can be saved to an external USB hard dive (which is disconnected from computers when not in use), or to somewhere on the internet, such as a cloud storage service. You can set your computer to automatically backup your data and it will save your data periodically without human intervention. So long as you maintain regular backups, in the event that you lose access to your onsite data, you will then be able to restore what was lost.

Small and micro businesses should:

- Backup important data, such as customer details and financial information, using an external USB hard drive or cloud storage service, preferably both.
- Ensure your backups are disconnected and stored separately from your computer, and preferably keep one copy of backup data onsite and another copy offsite (or in a cloud storage service).
- Regularly test your backups to make sure you are able to restore your data if the need arises.

Additional COVID-19 measures

The COVID-19 pandemic has meant businesses need to be flexible to a different way of operating, such as having more people work from home. Remote working introduces new cyber security risks. The following are additional measures you can implement while operating your business in the COVID-19 environment.

Portable devices

You and your staff may be using portable devices – such as laptops, tablets or mobile phones – to conduct business activities. Some staff may need training on the cyber security basics when using unfamiliar portable devices and connecting them to your business network.

Small and micro businesses should:

- Ensure that portable devices are updated before they connect to your business' network. This includes staff personal devices (see above: *The cyber security basics*).

See the ACSC's guidance on Quick Wins for your Portable Devices.

Physical security

The physical security of assets is important when considering an increase in the number of staff who are working remotely. As more staff are mobile, there is a greater risk that portable devices can become lost, stolen or broken, and for strangers to obtain access to your business operations.

Small and micro businesses should:

- Ensure all portable devices use either a strong unique passphrase, fingerprint or facial identification.
- Remind staff to lock, or lock away, their portable devices when not in use, even if it is for a short period of time.
- Be aware of who can overhear phone conversations.
- Don't access sensitive information if it can be observed by others.

Avoid public Wi-Fi

Public Wi-Fi hotspots, such as those available in places like cafes, libraries, hotels and airports, can be convenient. They can also be a cyber security risk. Cybercriminals have been known to set up rogue Wi-Fi hotspots with names that look legitimate but can intercept communications in order to steal your banking credentials, account passphrases or other valuable information.

Small businesses should:

- Direct staff to avoid using public Wi-Fi hotspots. It is safer for them to use their home Wi-Fi or mobile data instead.
- If available, direct staff to use your work Virtual Private Network (VPN). See the ACSC's guidance on Using Virtual Private Networks.

Staff training

Working from home can be daunting for staff who haven't done it before, especially if it's a sudden decision. Informing and training staff in their cyber security responsibilities is important and will ensure your staff can help protect your businesses.

Small and micro businesses should:

- Train staff in practicing good cyber security habits. The ACSCs Small Business Guide and the ACSC's COVID-19 Malicious Cyber Activity Threat Assessment are good places to start.
- Train your staff in any new portable devices or software they may need to use when working from home, such as how to log in securely to your business network. You may consider developing your own how-to guides.
- Make sure staff know how to report any cyber security incidents, including how to report cybercrime to the ACSC using ReportCyber.

Further information

The ACSC's ***Threat Assessment on COVID-19 Malicious Activity*** provides an overview of observed COVID-19 malicious activity impacting Australians. It can be found at: https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity.

The ***ACSC Small Business Cyber Security Guide*** contains cyber security guidance tailored for small businesses to help them protect themselves against cyber threats. It can be found at: https://www.cyber.gov.au/publications/small-business-cyber-security-guide.

The ACSC's ***Step-by-Step Guides*** are practical handbooks with steps and visual-aides for small businesses to turn on automatic updates for operating systems, such as for Microsoft Windows 10 and for Apple iOS and macOS. They can be found at: https://cyber.gov.au/small-business.

The ACSC's ***Step-by-Step Guides for turning on multi-factor authentication*** are a practical handbooks with steps and visual-aides for small businesses to turn on multi-factor authentication for Apple ID, Facebook, Gmail and Twitter. They can be found at: https://cyber.gov.au/small-business.

The ACSC's ***Quick Wins for your Portable Devices*** provides information on actions small businesses can take to improve the security of their portable devices. It can be found at: https://www.cyber.gov.au/publications/quick-wins-for-your-portable-devices.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).