Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

COVID-19: Cyber Security Tips When Working From Home

APRIL 2020

Introduction

This guidance outlines key cyber security practices for people who are working from home.

The COVID-19 pandemic has resulted in many people working from home for the first time. Working from home has specific cyber security risks, including targeted cybercrime. When compromised, unauthorised access to your stored information can have a devastating effect on your emotional, financial and working life.

Cyber security tips

Here are nine things you can do to in your new working environment to protect your work and your household's cyber security.

Beware of scams

Cybercriminals see a crisis as an opportunity. Major change brings disruption, and businesses transitioning to working from home arrangements can be an attractive target.

Be aware that the COVID-19 pandemic will be used by cybercriminals to try to scam people out of their money, data and to gain access to systems. While working from home you should:

- Exercise critical thinking and vigilance when you receive phone calls, messages and emails.
- Exercise caution in opening messages, attachments, or clicking on links from unknown senders.
- Be wary of any requests for personal details, passwords or bank details, particularly if the message conveys a sense of urgency.
- If in any doubt of the communicator's identity, delay any immediate action. Re-establish communication later using contact methods that you have sourced yourself.

For more ACSC information on how to identify and protect yourself from scams see:

- Threat Update: COVID-19 Malicious Cyber Activity
- Detecting Socially Engineered Messages.

Use strong and unique passphrases

Passwords are passé! Strong *passphrases* are your first line of defence. Enable a strong and unique passphrase on portable devices such as laptops, mobile phones and tablets.

Use a different passphrase for each website and app, particularly those that store your credit card details or personal information. To use the same username (such as an email address) and passphrase for multiple accounts means that if one is compromised, they are all at risk.

For more ACSC information, see 'Passphrases' in the:

- Small Business Cyber Security Guide.

Implement multi-factor authentication

Multi-factor authentication is one of the most effective controls you can implement to prevent unauthorised access to computers, applications and online services. Using multiple layers of authentication makes it much harder to access your systems. Criminals might manage to steal one type of proof of identity (for example, your PIN) but it is very difficult to steal the correct combination of several proofs for any given account.

Multi-factor authentication can use a combination of:

- 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).

If your device supports biometric identification (such as a fingerprint scan) it provides an additional level of security, as well as a convenient way to unlock the device after you have logged in with your passphrase.

For more ACSC information on how to implement multi-factor authentication for specific services, see:

- Step-by-Step Guides – Turning on Two-Factor Authentication
- Stay Smart Online – Two-Factor Authentication.

Update your software and operating systems

It is important to allow automatic updates on your devices and systems like your computers, laptops, tablets and mobile phones. Often, software updates (for operating systems and applications, for example) are developed to address security issues. Updates also often include new security features that protect your data and device.

For more ACSC information on updating operating systems and software, see:

- Step-by-Step Guide – Turning on Automatic Updates (For Windows 10)
- Step-by-Step Guide – Turning on Automatic Updates (For iMac & Macbook, and iPhone & iPad).

Use a Virtual Private Network (VPN)

Virtual Private Network (VPN) connections are a popular method to connect portable devices to a work network. VPNs secure your web browsing and remote network access.

Sometimes organisations specify that you use a VPN on work devices. If this is the case, you should familiarise yourself with your organisation's VPN requirements, policies and procedures.

For more information on VPNs see advice from the Canadian Centre for Cyber Security:

- Using Virtual Private Networks.

Use trusted Wi-Fi

Using free wireless internet may be tempting; it can also put your information at risk. Free Wi-Fi by its very nature is insecure and can expose your browsing activity to cybercriminals. Cybercriminals have also been known to set up rogue Wi-Fi hotspots with names that look legitimate and can intercept communications, steal your banking credentials, account passwords, and other valuable information.

Use trusted connections when working from home, such as your home internet or mobile internet service from your telecommunications provider.

For more ACSC information on the steps you can take to secure your Wi-Fi, see:

- Stay Smart Online - Wi-Fi and Internet Connections.

Secure your devices when not in use

It's much easier to access your information if other people have access to your devices. Do not leave your device unattended and lock your computer when not in use, even if it's only for a short period of time.

You should also carefully consider who has access to your devices. Don't lend laptops to children or other members of the household using your work profile or account. They could unintentionally share or delete important information, or introduce malicious software to your device.

If you do share your computers or devices with family or your household, have separate profiles so that each person logs in with a unique username and passphrase.

For more ACSC information on good cyber security behaviours, see:

- Stay Smart Online - Protecting Your Computer From Online Threats.

Avoid using portable storage devices

When transporting work from the office or shop to home, portable storage devices like USB drives and cards are easily misplaced and, if access isn't properly controlled, can harm your computer systems with malware.

If possible, transfer files in more secure ways, such as your organisation's cloud storage or collaboration solutions. When using USBs and external drives, make sure they are protected with encryption and passphrases.

For more ACSC information on portable storage cyber security, see:

- Quick Wins for your Portable Devices.

Use trusted sources for information

Cybercriminals and other malicious actors use popular and trending topics such as COVID-19 to spread disinformation or scam people. Impersonating, cloning or creating websites to look genuine is one way to do this (see 'Beware of scams' above). Producing and sharing false information on social media is another.

Be sure to only use trusted and verified information from government and research institution's websites. Think critically about the sources of information that you use, and balance all evidence before believing what people share.

For the latest COVID-19 information, see:

- Australian Government COVID-19 website.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).