Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Practical cyber security tips for business leaders

Content Complexity
SIMPLE

January 2024

Introduction

Business leaders can be appealing targets for malicious actors due to the sensitive information they can access, the important people they interact with and the influence they hold. This publication includes a checklist of practical tips business leaders can implement to improve their cyber security. The checklist is followed by a brief explanation of each tip and why it is recommended.

Summary checklist

	Top tips	Read more
☐	Enable multi-factor authentication (MFA)	3
☐	Update and patch your software and applications	3
☐	Update and patch your operating systems	3
☐	Back up your important files	3
	Devices	
☐	Use separate work and personal devices and accounts	4
☐	Do not share work devices with others	4
☐	Use screen locks on all devices	4
☐	Give only minimum permissions to software and apps	4
☐	Factory reset your devices after suspected compromises	5
☐	Turn mobile devices off once a day	5
☐	Only install software and apps from trusted sources	5
☐	Charge devices with trusted cables and power outlets	5
☐	Only plug trusted devices into your laptop, phone or computer	5
☐	Turn off communications capabilities when not required	6
	Accounts	
☐	Screen suspicious calls, emails and messages	6
☐	Use strong, unique passwords or passphrases	7
☐	Never share passwords and passphrases	7
☐	Don't use publicly available information for password reset questions	7
	Social Media	
☐	Restrict social media privacy and security settings	8
☐	Don't share private information on social media	8
☐	Use separate work and personal social media accounts	8
☐	Never share login details for social media accounts	8
☐	Watch for and report fake social media accounts	9
	Communications	
☐	Enable security features on messaging apps	10
☐	Use group messages with caution	10
☐	Only do work communication from your work devices	10
☐	Only share meeting invitations through private channels	10
☐	Only allow invited participants to join meetings	10
☐	Join meetings from a private location	10
☐	Be cautious when screen sharing	10
	Travel	
☐	Do not use public Wi-Fi	11
☐	Take precautions to reduce the impact of lost or stolen devices	11
☐	Consider using dedicated travel devices and accounts	11

Practical cyber security tips for business leaders

Enable multi-factor authentication (MFA)

Enable multi-factor authentication (MFA) to prevent unauthorised access to your devices and accounts. MFA requires you to prove your identity in two or more ways before you can access your devices or accounts. Enable MFA wherever it's supported, especially for your email accounts. MFA is one of the most effective cyber security measures you can take. Some secure MFA options you can use include an authenticator app, an authenticator token or a physical security key. You can also use email and SMS authentication, but be aware that these options are more vulnerable to attacks by malicious actors.

Never share your MFA codes and never approve an unexpected MFA prompt. Malicious actors may try to trick you into sharing MFA codes or approving MFA prompts so they can access your devices or accounts.

You can access guidance to turn on MFA for key services on cyber.gov.au.

Update and patch your software and applications

Update and patch your software and applications to fix vulnerabilities and add security features. You should turn on automatic updates, wherever possible.

Updating your software and applications is just as important as updating and patching your operating system. Your software and apps can often access sensitive information such as your messages, credit card details and photos. Updates can protect this information by fixing vulnerabilities and adding security features.

Update and patch your operating systems

Update and patch your operating systems to protect your devices. Updates and patches to your operating systems (for example, Windows, macOS, iOS and Android) add new features, fix critical vulnerabilities and introduce stronger security features. You should receive a notification from your device when an update or patch for your operating system is available. Install the update or patch as soon as you can to keep your devices more secure. Turn on automatic updates for your operating system if they're available.

Consider replacing your devices if they are no longer receiving patches and updates.

Consider how quickly security updates are delivered when you are buying a new device. Timely updates for your operating system keep your device protected against emerging threats.

Back up your important files

Protect your important information by regularly backing it up. Backing up your files lets you recover your information if it is ever lost, stolen, compromised by malicious software or damaged in a fire, flood or other disaster. It is best practice to regularly back up your important files to a reputable cloud backup service or through an offline backup by using an external storage device, such as a USB stick or external hard drive.

Secure your devices

Use separate work and personal devices and accounts	Why
Your role may require you to use multiple devices. There are steps you can take to manage these devices securely. **Use different accounts for your work and personal devices** to protect sensitive information. Companies such as Apple, Google and Microsoft are making it easier to synchronise information between devices. It is not just your files that can synchronise between your devices. Your messages, call logs, passwords and photos can synchronise too. While this can be convenient for your personal information, it presents a security risk for sensitive information. If sensitive information is synchronised with personal devices, it is easier for it to be inappropriately accessed or stolen. To prevent this from happening, use separate accounts for your official and personal devices, this includes your Apple, Google and Microsoft accounts. **Share your apps and paid services securely** by using services such as Apple Family Sharing, Google Play Family Library and Microsoft Family Group. These services let you securely share your purchases including your apps, games, books and movies with other accounts. Avoid directly signing into your accounts on your family members' devices. If you do, there is a risk that sensitive information will be synchronised to their devices where it can be inappropriately accessed.	Protects sensitive information from unauthorised access and inadvertent leaks. Takes advantage of the security measures that are typically applied to work devices.
Do not share work devices with others	
Avoid sharing your work devices with others. Sharing your work devices puts sensitive information at risk of being inappropriately accessed. It is best practice to not share your devices, even though it might be convenient.	Protects sensitive information from unauthorised access and inadvertent leaks.
Use screen locks on all devices	
Keep your devices secure by using a screen lock with a strong passphrase, fingerprint unlock or face unlock. Avoid swipe or gesture-based unlocks as they often leave a mark on the screen that makes them easier to guess.	Protects against unauthorised access to your device and any sensitive information or accounts it holds.
Give only minimum permissions to software and apps	
Protect sensitive organisational information by restricting what your software and apps can access. Software and apps can ask for permission to access things such as your location, contacts, camera, files and microphone. Consider restricting these permissions, even for well-known software and apps, such as social media platforms. You can restrict permissions in your devices' privacy settings. Be suspicious of any software or app that asks for extensive permissions or permissions they have no reason to access. For example, a calculator app that asks for permission to access Bluetooth functionality and your calendar.	Protects sensitive information from software or apps that collect excessive data or are lax with data security.

Factory reset your devices

Factory reset your devices after suspected compromises. There may be situations where your devices are not used securely. For example, a family member may have installed potentially malicious software or apps on your devices while travelling, or your devices may have temporarily left your possession. You can mitigate this risk by backing up your important data then factory resetting your devices. A factory reset can remove many (but not all) strains of malware.

Turn your mobile devices off daily

Turn your mobile devices off and on at least once a day. Turning off a device can remove many strains of persistent malware. For this measure to be effective, devices need to be turned off completely, not just locked or placed in sleep mode.

Only install software and apps from trusted sources

Protect your devices by using trusted software and apps. It is best practice to download your software and apps from official app stores and websites, for example, the Apple App Store, Google Play Store and Microsoft Store. If you use pirated software or untrusted app stores, your devices are more likely to become compromised and less likely to be supported with patches and updates by vendors and developers.

Charge your devices securely

Charge your devices only with trusted cables and power outlets. Malicious actors can use charging cables to infect devices with malware. Only use charging cables from your device's manufacturer or a reputable third party vendor. USB power outlets can also be used to deliver malware to your devices. Only plug your devices into a USB power outlet you trust, for example, one at your home or office. Never plug your devices into a public USB power outlet, for example, at an airport or café; use a regular power outlet instead.

Only plug trusted devices into your laptop, phone or computer

Only plug trusted devices into your laptop, phone or computer. This includes removable media, such as USB sticks and external hard drives, as well as peripherals, such as USB headphones and microphones. You should not trust:

- Devices that were gifted to you.
- Devices that have been in the possession of untrusted people, even if briefly.
- Removable media that has been plugged in to another party's systems or devices.

Anything you plug into your devices should be made by a reputable manufacturer and purchased at a reputable store. Ask your IT team to thoroughly scan any device you intend to connect to a work system.

Why

Protects against many strains of persistent malware.

Protects against malware.

Maintains support from vendors and developers.

Protects against malware.

Turn off communications capabilities when not required

Turn off your device's communications capabilities when not required, including cellular data, wireless, Bluetooth and Near Field Communication. Communications capabilities have improved over time, however none are immune to compromise. You can reduce the number of ways a malicious actor can exploit your device by disabling communications capabilities when not required.

Why

Minimise device vulnerabilities.

Secure your accounts

Screen suspicious calls, emails and messages

Look out for suspicious calls, emails and messages. They could be the first steps in a cyber attack. Be suspicious of any correspondence that:

- Comes from an unfamiliar phone number or email address.
- Asks you to click on a link, open an attachment or visit a website.
- Is suspiciously written, or has an unusual tone, spelling mistakes or incorrect capitalisation.
- Pressures you to take urgent action.
- Claims that your device has a technical problem.
- Requests information that the sender has a questionable need to know.

It can be hard to recognise what is legitimate and what is not. Malicious actors can spoof their phone number or email address to make their communication appear to come from a legitimate source. They may also use publically available information about you to add personal touches to their communication. For example, information from your social media pages. These personal touches can make their messages very convincing.

If you receive suspicious correspondence, do not interact with it. Be particularly careful to avoid opening any links or attachments. Contact your IT support staff to report the suspicious message and ask for support.

Protects against a wide range of threats including:

- Ransomware & other types of malware
- Account compromise
- Remote access scams
- Identity theft
- Financial theft

Use strong, unique passwords or passphrases

Use a password manager or passphrases to create strong, unique passwords. Password managers can create strong, unique passwords for each of your accounts. With a password manager, you only need to remember one master password, the password manager takes care of the rest. Your master password is the key to all your accounts so make sure it is strong.

For accounts that you sign into regularly, or that you otherwise do not want to store in a password manager, consider using a passphrase as your password. Passphrases are a combination of random words, for example 'crystal onion clay pretzel'. They are useful when you want a secure password that is easy to remember. ASD's ACSC recommends using passphrases that: are at least 14 characters long, use a random mix of four or more words, do not use popular phrases, and are not re-used across multiple accounts.

Do not store your passwords or passphrases next to the devices they are linked to. For example, do not store the passphrase for your laptop in your laptop bag.

Never share passwords and passphrases

Do not share your passwords or passphrases, even with family members and staff. Be aware that any actions performed by staff using your accounts will likely be attributed to you.

Don't use publicly available information for password reset questions

Set strong password reset questions when required to prevent malicious actors from accessing your accounts. Be careful to avoid publicly available information when setting password reset questions. Business leaders often have biographical information published about them online. This information can render common password reset questions like 'mother's maiden name' and 'childhood address' insecure.

Why

Protects accounts, devices and the sensitive information they hold from unauthorised access.

Secure your social media

Restrict social media privacy and security settings

Update your privacy settings on social media platforms to make sure you know who can see your information. Privacy settings often change after functionality is added to social media platforms so it is important to check them regularly. Be aware that your data may be stored in other countries where Australian legislation may not apply. Further information is available on ASD's ACSC's Security Tips for Social Media and Messaging Apps page.

Don't share private information on social media

Don't share private information on social media, and ask your friends and family to do the same. While some information might not seem important, many small pieces of information can be put together to form a picture about you. If you reveal too much private information online, malicious actors may collect enough information to steal your identity, guess weak account reset questions, guess weak login details, or add personal touches to scams or phishing attempts targeting you.

Never assume that anything you do or post online will remain secret from anyone, including malicious actors. Even trusted online platforms and services may be compromised by a cyberattack and suffer a data breach.

Use separate work and personal social media accounts

Separate your public and private life. Consider creating separate work and personal social media accounts to segregate the information you share with different audiences.

Never share login details for social media accounts

Do not share login details for social media accounts. Instead, use business or corporate social media accounts that allow multiple users to manage a profile without sharing login details. Several social media platforms, including Facebook and X, offer this functionality.

Why

Protects sensitive information from inadvertent sharing.

Makes it harder for malicious actors to learn enough about you to steal your identity, target you with personalised phishing messages or guess your password reset questions.

Protects against unauthorised account access.

Reduces the risk of unauthorised account activity by limiting permissions.

Watch for and report fake social media accounts

People may attempt to impersonate you online. You can stop misinformation by reporting fake accounts to your IT support staff and the social media platform.

Malicious actors may also try to impersonate someone you trust in order to trick you. Be suspicious of social media accounts with an unusually low number of posts, pictures or connections; unrecognised email addresses or unknown phone numbers. Be aware that malicious actors often use personal details to create very convincing digital identities to mislead people.

Be cautious when approving requests to verify social media accounts. These requests can be sent by malicious actors to trick you into verifying fake accounts. Only verify accounts if you know the request came from you.

Why

Protects against scams that target you or scams that use your identity to target others.

Secure your communications

Enable security features on messaging apps

Use encrypted messaging applications and familiarise yourself with their security features.

If you use iMessage, be aware that blue text bubbles indicate that a conversation is encrypted between the participants. Green text bubbles indicate that a conversation is not encrypted, this typically occurs when messaging an Android device.

If you use Google Messages, be aware that a lock over the send button indicates that a conversation is encrypted. If there is no lock over the send button, your conversation is not encrypted, this typically occurs when you are messaging an iPhone. Google Messages lets users verify they are communicating only with whom they intend with a unique verification code.

If you need to communicate sensitive information between both Android and iPhone users, consider a cross-platform encrypted messaging product, such as WhatsApp or Signal. These products provide similar end-to-end message encryption capabilities, but are not limited to a single operating system or device type.

If you use other encrypted messaging applications, ensure that you have multi-factor authentication enabled. Check if your app has a mechanism to verify that you are communicating only with whom you intend, this usually involves all parties in a conversation comparing a security code.

Protects messages from being intercepted and read.

Helps you detect if malicious actors are impersonating your contacts.

Use group messages with caution	Why
Be cautious when using group messages. The larger the group, the more opportunities there are for information to be compromised. Be aware that some messaging software and apps allow new members of a group to see messages sent before they joined the group. When sharing content, check whether your messaging apps offer end-to-end encryption for group messages; not all do.	Protects sensitive information from being leaked.
Only do work communication from your work devices	
Only use your work devices to store or share work-related information. Your work devices should have security measures in place to protect your sensitive work information. Your personal devices are unlikely to have the same level of protection so should not be trusted to share or store work-related information.	Protects sensitive information from being leaked or inappropriately accessed.
Only share meeting invitations through private channels	
Only share meeting invitations through private channels such as email or encrypted messaging applications. If you share meeting invitations on publicly accessible websites or social media platforms, there is a risk that unwelcome guests will attend. Regularly update meeting login details and access links for recurring meetings to make sure previous guests cannot access meetings they have not been invited to.	Protects sensitive information from being accidentally shared.
Only allow invited participants to join meetings	
Only allow invited participants to join a meeting. Consider requiring a password to join online meetings to reduce the risk of unwanted participants. Once all participants are present, consider locking the meeting so guests cannot join without approval. If there are unknown participants in the meeting, ask them to identify themselves and disconnect them if they refuse.	
Join meetings from a private location	
Join meetings from a private location whenever possible. If there are other people nearby, it is best practice to use headphones so that only meeting participants will hear the full conversation. Point your webcam away from any sensitive information in your background and use background-blurring features, if they are available.	
Be cautious when screen sharing	
Be careful when sharing your screen. Only share specific software or apps you need to, instead of your entire screen. It is also good practice to set expectations regarding recording a meeting or publishing the details of proceedings in advance.	

Secure your travel

Don’t use public Wi-Fi

Public Wi-Fi is insecure by nature and can expose your internet activity to malicious actors. When you are travelling, it is more secure to set up a personal mobile hotspot rather than to use public Wi-Fi.

Why

Protects your internet traffic from being intercepted and read by malicious actors.

Take precautions to reduce the impact of lost or stolen devices

One of the biggest risks to your information is from lost or stolen devices. Never leave mobile devices or removable media unattended for any period of time, including by placing them in checked-in luggage or leaving them in hotel safes. If your devices support encryption, this should be enabled to secure your information in the event you lose them or they are stolen. If your devices have a ‘find my device’ function, or the ability to remotely erase your information, these measures can provide additional security in the event of loss or theft.

Protects sensitive information and accounts on your devices from being inappropriately accessed.

Consider using dedicated travel devices and accounts

Your devices may be more susceptible to targeting by malicious actors when you travel overseas so only travel with the devices you need. Talk to your IT support team about setting up dedicated travel devices and accounts before you go overseas and resetting them when you return. Travel devices should use a VPN to help secure your internet traffic. Travelling with dedicated devices and accounts is best practise because it limits the amount of information that can be accessed if your devices are compromised, lost or stolen. Consider following ASD’s ACSC’s advice on travelling overseas with electronic devices, or Smarttraveller advice on securing mobile devices for overseas travel.

What to do if you think you have been compromised

If you think you have been the victim of a cyber incident you should speak to your IT support team immediately. The sooner they know, the sooner they are able to help you. Cyber incidents can also be reported to the Australian Cyber Security Centre on 1300 CYBER1 (1300 292 371). This service operates 24 hours a day, 7 days a week. For more detailed advice on how to immediately respond to a suspected cyber incident, visit ASD's ACSC 'Have you been hacked?' tool at cyber.gov.au.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre