Australian Government
Australian Security Intelligence Organisation

SECURE YOUR SUCCESS

Securing technology, research and expertise

ASIO

asio.gov.au

Espionage and foreign interference are occurring at an unprecedented scale.

Australian innovation and know-how is world-leading, making it an attractive target for adversaries. Foreign powers are gaining advantage from Australian innovation by stealing intellectual property, harvesting expertise and co-opting academic research. They may do this by directly employing you, contracting your services, or by stealth. The loss and/or compromise of your knowledge, expertise, intellectual property or information can harm your career and your business.

Foreign powers or their proxies can use cyber, human or technical means to get the information they want.

- **Cyber**—by employing cyber tactics, such as sending you phishing emails with malicious links or gifting you with a USB device that will execute malware once connected to your computer or network.
- **Human**—by approaching you directly. They may overtly identify themselves and ask you to help them, or they may covertly try to gain your trust and assistance.
- **Technical**—by using audio or visual recording devices in areas where you might discuss or conduct sensitive matters.

Security is a shared responsibility.

Individuals and organisations can take the following actions to prevent foreign powers conducting harmful activities

- *Implement ASIO's Protective Security Top 10*
- *Build a strong security culture*
- *Protect your research, collaborate with care*
- *Prying Minds. Report suspicious approaches and activities*
- *Think Before You Link. Be discreet and secure online*
- *Counter the insider threat*
- *Be security-aware when you travel*
- *Protect electronic devices*

Implement ASIO's
Protective Security Top 10

All organisations face threats to their people, places, technology and information. The nature of these threats will vary in type and scale depending on the organisation's, or individual's, unique risk. These threats can adversely impact the wellbeing of employees as well as the safety, stability, productivity, reputation and prosperity of a workplace.

Organisations can manage the risk of threats by implementing multi-layered protective security measures to deter, detect, delay, respond to and recover from compromise. ASIO's *Protective Security Top 10* identifies the essential components of a complete security framework to protect people, places, technology and information.

1

Know the threat to you and your workplaces so you can prepare accordingly

- Identify the threats to—and vulnerabilities of—staff, key functions, critical systems, data, assets and facilities. And know that you may also be targeted.
- Conduct a risk assessment to identify your unique risks and risk tolerance.
- Apply a risk-based approach to security: focus your attention and resources where it will achieve the best outcomes.
  - **Threat** = intent and capability of an adversary.
  - **Vulnerability** = a flaw or weakness which could be exploited.
  - **Risk** = likelihood and consequence of an attack.
  - **Risk tolerance** = an informed decision to accept a certain level of risk.

2 Establish a security governance model to support oversight, control and decision-making

- Develop a security plan and establish a corporate body responsible for overseeing security matters and decision-making.
- Security is a shared responsibility—assign security responsibilities to trained personnel and collaborate—no single person or area can manage security alone.
- Establish sound and tested policies and procedures that are easy to follow and access and update them regularly—make doing the right thing, the right way, as easy as possible.
- Include policies and procedures to manage any risks posed by external visitors, contractors, managed service providers, staff working remotely and staff travelling overseas.

3 Build a strong security culture to enable, encourage and educate employees towards security-savvy behaviours

- Regularly assess the culture for trends that require attention.
- **Enable:** leadership, compliance and correction.
- **Encourage:** ownership, reporting, discipline, innovation and confidence.
- **Educate:** communicate and deliver security awareness training to all staff.

4 Install and maintain physical security systems to protect people, places, technology and information

- Provide secure and reliable infrastructure for all staff, including those working remotely.
- Ensure highly secure areas have systems that are auditable and can control access to sensitive information and assets, detect breaches or attempted breaches of access and provide real-time alerts about unauthorised access.
- Keep an inventory of all physical assets assigned to personnel (passes, tokens, laptops) and update the inventory regularly.
- Ensure physical and ICT supply chain risks are considered and addressed.

Implement robust ICT systems to protect your critical systems, devices and data from cyber threats

- Implement the ACSC's *Essential Eight*.
- Secure your accounts, devices and email—patch regularly and use complex passwords, multi-factor authentication and protection software.
- Manage the connectivity of systems and devices—**anything connected to the internet is vulnerable** (this includes PROTECTED networks).
- Secure all electronic devices: maintain physical control of them at all times; switch them off daily; limit the information stored on them; and sanitise them before destruction or disposal.
- Carefully consider the potential risks of using the cloud or data centres.
- Regularly back up devices, data and systems.

Implement a personnel security framework to ensure employees are suitable to have access to your people, key functions, critical systems, data, assets and facilities

- Implement appropriate and proportionate personnel screening procedures during pre-employment, throughout employment and at the conclusion of employment.
- Include external providers, managed service providers, contractors, consultants and business partners.
- Implement a counter insider threat program.
- Remember security clearance holders have additional obligations.

Protect unique, privileged, sensitive and national-security classified information

- Hold sensitive activities and discussions in secure areas (for example, recently swept spaces, device-free areas, Security Zones and SCIFs).
- Handle, use, store and destroy sensitive material appropriately.
- Control information access to only those with an appropriate security clearance and/or need to know.
- Restrict mobile devices in secure areas or near sensitive discussions.
- Protect your research and intellectual property by collaborating with care.
- Conduct technical security countermeasures sweeps if required.

8 Be secure online

- Restrict, limit or securely manage the connectivity of systems and devices.
- Regularly check the security settings of online accounts and delete or deactivate accounts no longer in use.
- Periodically review, update or remove information available online or on social media that could compromise the safety of your employees, workplace and assets, or be of interest to adversaries.

9 Recognise and respond to suspicious behaviour and security incidents

- Establish a reporting mechanism that is confidential, accessible and timely.
- Educate employees on what to report and how.
- Educate security teams to recognise and respond to possible reconnaissance activities.
    - Reconnaissance is the purposeful observation of people, places, vehicles and locations to gather information; it may be undertaken through physical and/or technological means.
- Educate employees to Think Before You Link when connecting online and to report suspicious approaches or persistent questioning.
- Establish emergency and security incident investigation and response procedures and know when referral to external agencies is required.

10 Regularly review your settings for effectiveness

- Regularly review your security governance and controls for effectiveness and adjust if required.
- Review security incidents to assess if there were missed opportunities to intervene earlier, if additional or different measures or training could have assisted, and if it was an isolated incident or part of a trend.
- Review and test incident response and investigation procedures for effectiveness.

Build a strong security culture

Security measures are only effective if people use them. A strong security culture will create a workplace that is safer, more secure and more resilient to threats. Organisations can build and foster a strong security culture by creating an environment that **ENABLES**, **ENCOURAGES** and **EDUCATES** individuals towards security-savvy behaviours. Individuals can contribute by taking active responsibility for the role they play in protecting themselves, what they know and can access.

ENABLE

Workplaces **ENABLE** security-savvy behaviours by establishing a mature, reliable security framework which nurtures:

- **leadership**—where management places a high value on security—and demonstrate this
- **compliance**—where the workplace security framework is a robust foundation for employees to work within
- **correction**—where security issues are managed quickly in a fair and rigorous manner with a focus on correction rather than reprimand—unless reprimand is appropriate

ENCOURAGE

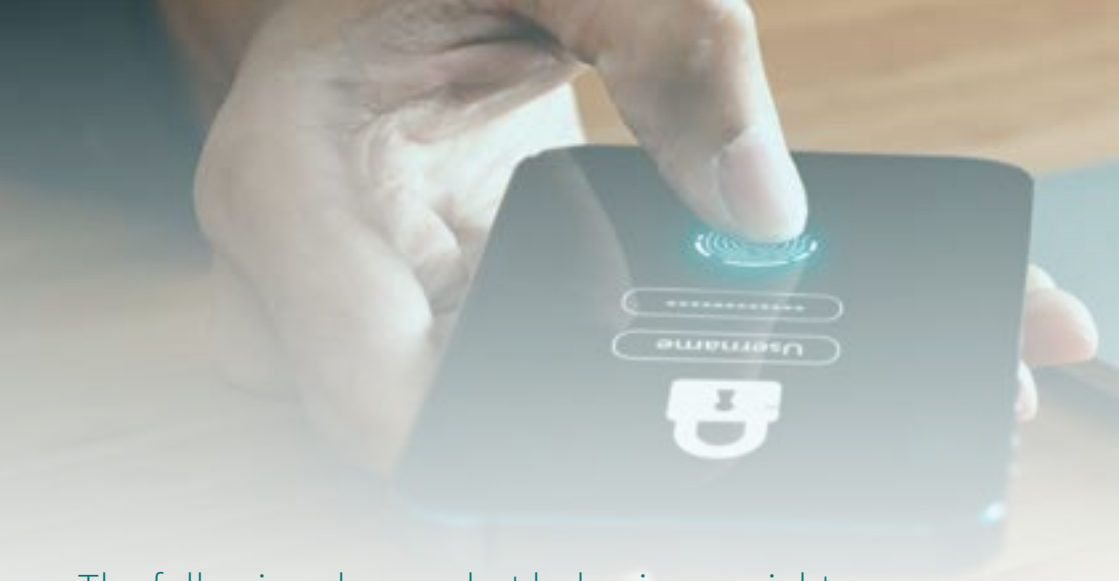
Workplaces **ENCOURAGE** security-savvy behaviours by supporting employees' engagement in the wellbeing and prosperity of the workplace. Workplaces should encourage:

- **ownership**—where employees take responsibility for their role in protecting the workplace from harm
- **innovation**—where ideas for improving security and reporting security incidents are encouraged
- **discipline**—where all employees consistently adhere to policies and procedures
- **reporting**—where employees understand the value of reporting, and report appropriately
- **confidence**—where employees are comfortable reporting security concerns, challenging concerning behaviour and seeking help if required

EDUCATE

Workplaces should **EDUCATE** employees on the security behaviours expected of them. Well-trained staff are more likely to raise security concerns and proactively comply with security measures. Workplaces should focus on improving:

- **communication**—where all staff are aware of their workplace security measures and why they exist
- **awareness**—where employees understand the threat, the importance of security and the part they play



The following shows what behaviours might be observed in an environment with a strong security culture

Screensaver message: This month's cyber security tip is to create strong passwords using passphrases.

- Staff know and practise good cyber security, such as not clicking on unknown or suspicious email links.
- Computer screens and sensitive materials are secured when not in use.
- Screensaver messages are used as reminders to enhance security awareness.
- Regular security awareness training, activities and/or campaigns occur.

I want to work on this sensitive document from home but I need to be sure I can access it securely. I'll ask my line manager or security team for advice before I do anything.

- Security policies and procedures are clearly communicated and easily accessible to all staff.
- Employees know what the threat is, why security is important, what is expected of them and how their efforts contribute.

Hi Security Team, I'd like to report that I didn't patch my corporate laptop with the latest software, and now it's behaving strangely. I'm concerned something may have been compromised as there is sensitive material on there. Can you help me?

- Employees feel confident to ask for help when they are unsure of a security procedure.
- Employees are confident and comfortable reporting security breaches, including their own.
- Employees are supported and educated when an unintentional security breach occurs.

I noticed you were going to do X. It's more secure to do Y. Let me show you.

- Workplaces have clearly defined security principles, and long and short-term security goals.
- There is high compliance with security policies and procedures by all employees, including management.
- Suitable infrastructure and resources are provided to support the security behaviours expected of all employees.
- Security knowledge is shared.

I know X has already left for the day but I see a sensitive document still on their desk. I'll lock it away for them.

- Good security practices are praised.
- Colleagues support each other to observe good security behaviours.

CEO to Board: I'm interested in this proposal but let's explore the potential security implications before making a decision.

- Security is considered when making decisions.
- Managers champion and display good security habits and behaviours.

Hey, I can't see your access pass for this area. Can you show me please?

- Sensitive information is used, handled, stored and disposed of securely.
- Employees take action (inquire, assist, report) when they observe a security issue.
- Sensitive information isn't shared without the need to know.
- Sensitive conversations are held in secure spaces.
- Electronic devices are patched regularly and discouraged from being in sensitive areas.
- Sensitive areas aren't accessed without the need-to-go.

Line manager: I've noticed X has been keeping unusual hours lately and accessed sensitive material not relevant to their role. I will need to explore if there is a reasonable explanation and/or seek advice from the security team.

- Security incidents and concerning behaviours are addressed promptly.
- Personnel frameworks exist to manage employees before they are employed, throughout their employment, and after they separate from the workplace.
- Managers are aware of the insider threat and take action when an employee's behaviour changes.

RUOK?

- Employees proactively or willingly participate in security frameworks (such as annual security reviews and training activities).
- Employee wellbeing is valued, and support systems are provided.


NITRO
PROTECT
YOUR RESEARCH
Collaborate with care

Protect your research, collaborate with care

Foreign powers seek to identify personnel who have or can access unique, privileged, or commercially sensitive information so they can reproduce technology, gain military advantage or get the upper hand in trade deals or policy negotiations. Even seemingly innocuous information may be aggregated with other information to fill intelligence gaps or identify individuals for possible future targeting.

Espionage and foreign interference can negatively impact your institution—and your career—in a number of ways. For example, if a foreign researcher accesses and publishes your unpublished research or data, it can deprive you of the opportunity to publish and commercialise your work, and could make it more difficult for you and your institution to attract funding in future.

However, even legitimate academic engagement with partners can cause damage to the national interest and present a national security threat—for instance, if it results in the inadvertent transfer of sensitive science and technology research, expertise and/or data to a foreign power. This is particularly the case if the research or data relates to dual-use technology or military capability.

Suspicious approaches could include:

- receiving requests to collaborate on research with foreign institutions or researchers in areas that are associated with critical or dual-use technology
- receiving unsolicited requests—including from foreign diplomats—for your expert opinion
- receiving financial donations from foreign or foreign-linked entities—they can be trying to gain access to or influence sensitive research or research personnel
- unusual, unsolicited, or persistent attempts to access research papers or material, including unpublished data
- invitations—both solicited and unsolicited—to participate in international conferences, which may include excessive offers of hospitality or gifts, such as all-expenses-paid trips
- foreign delegations wanting to enter sensitive research facilities, such as laboratories, for tours or meetings.

ASIO has developed the *Protect your research, collaborate with care* campaign to provide advice on what you can do to protect yourself and your institution from harm, including being aware of the threat, conducting due diligence and reporting suspicious approaches. Visit www.asio.gov.au/protect-your-research for more information.

Case studies

In September 2023, representatives of a foreign scientific academy visited an Australian research institution and distributed flyers encouraging Australian researchers to apply for a foreign research initiative to 'promote global research mobility'.

Your people are your talent; protecting them ensures that your business or institution will maintain its advantage into the future. Visiting delegations are one way foreign powers can target your organisation and its strengths. When hosting a foreign delegation, consider in advance what access you will give them to your facilities, your systems and your people.

In July 2023, representatives of an Australian university reported they had seen research jobs in critical technology fields advertised on LinkedIn that offered the chance to work remotely for universities in a foreign country, without any requirement to travel offshore

LinkedIn is a popular way foreign powers and their proxies target Australian businesses and institutions to extract your critical knowledge and expertise. Mitigate this threat by raising staff awareness of LinkedIn approaches and requiring staff in critical works areas to regularly declare any outside interests that could be seen as a conflict.


NITRO
REPORT
PRYING
MINDS
Be aware
Be discreet
Be responsible

Report prying minds

Security is a shared responsibility and you can help by reporting suspicious approaches or activity.

WHAT

could make you susceptible to approaches by foreign spies?

- being stressed about personal or financial matters
- getting into situations where sensitive material could be easily compromised
- being concerned about the safety of family members.

WHERE

could foreign spies target you?

- at social, religious or other gatherings
- through dating or other social media platforms
- through seemingly benign or coincidental interaction.

HOW

can foreign spies coerce you into providing them with information?

- by creating a sense of personal connection or obligation
- by making you feel a sense of indebtedness
- by providing you with financial incentives, gifts, networking opportunities or preferential access.

Report anything that seems suspicious, ongoing, unusual or persistent. Remember this as SOUP.

Suspicious

You receive a social media request from a foreign national you've never met or heard of before, and they have an extensive list of foreign contacts, none of whom you know.

Ongoing

You meet someone in an official capacity and they contact you afterwards to continue the association, either officially or unofficially.

Unusual

You receive an unsolicited email from a professor in another country asking you to host a visiting scholar while they work with you for a period of time.

Persistent

You attend a weekly social gathering where someone repeatedly asks detailed questions about your work duties.

Australian Government personnel and security clearance holders should report SOUP to the Contact Reporting Scheme (CRS) through their security team or directly to ASIO via cr@asio.gov.au. The CRS is a vital tool that helps ASIO uncover the harmful activities of foreign powers in Australia, including how they target government personnel, information, and facilities. Contact reporting is a requirement for individuals who hold a security clearance.

Industry personnel and non-security clearance holders can report SOUP to your security team and directly to ASIO through the Notifiable Incidents, Threats and Reportable Observations (NITRO) portal—nitro.asio.gov.au. The NITRO portal is a secure online tool to report concerns, directly to ASIO, about espionage, insider threats or foreign interference. Secure what you know through NITRO.

ASIO uses reports into the CRS and NITRO to identify espionage and hostile foreign intelligence activity and concerning patterns of activity. The information you provide helps ASIO understand the bigger picture and your report could be the missing piece of the puzzle. ASIO will treat your report with the same confidentiality and discretion applied to all national security matters.

Case study

In 2022, an Australian university was approached by a private company to collaborate on research into alternate energy sources. The university undertook due diligence, and discovered the company was one of several interrelated companies linked to a foreign government, which all had opaque funding arrangements and limited footprints in Australia.

Information doesn't need to be classified for it to be valuable: foreign powers and their proxies frequently target sensitive information that can give them a commercial advantage. 'Shell companies'—which may be registered in Australia but have a limited footprint here — are a well-known way foreign powers acquire sensitive intellectual property, data and expertise and move it offshore. Conduct thorough due diligence to protect your interests, and report suspicious approaches to your institution's security team, and to ASIO through the NITRO portal.

Frequently asked questions

I received a message through a professional networking site or social media from someone based overseas, seeking my views on issues related to my work. Should I report it?

Yes. Any contact with a foreign national that seems unusual or suspicious should be reported. If you can take screenshots of the messages and associated accounts, these are also useful to include.

I've become friends with someone through my weekend sport (or language classes, work or children's school) and they seem to be a foreign national. I'm going to keep seeing them socially. Should I report it?

Yes. As a clearance holder, ongoing contact with foreign nationals outside your official duties should be reported as part of your clearance holder obligations.

I was at a birthday party for my child's friend, and one of the parents there asked me questions about my job that seemed quite probing and made me feel uncomfortable. Should I report it?

Yes. You should always report someone seeking information about sensitive topics, beyond what is needed or appropriate for the conversation or situation, regardless of their nationality. Trust your instincts if something makes you feel uncomfortable.

I have regular liaison with a foreign government as part of my work, and have been invited to the national day function at their embassy. Should I report it?

No. This is part of your official duties but ensure your attendance is corporately recorded (of course, if anything happens at the event that you consider suspicious, you should report it).

I've received a number of requests for connections on social media sites from people I don't know, who seem to be based overseas. Should I report this?

Yes. Approaches on social media that seem unusual or suspicious should be reported.

I went overseas on a work trip. Do I need to report all my contacts from the time I was overseas?

No. You should only report contacts or incidents that are suspicious, ongoing, unusual or persistent (outside corporately recorded professional relationships).

I got a phone call or text message claiming to be from a business but it seemed suspicious. Should I report it?

Maybe. In the first instance, an internet search may be able to tell you whether the contact is a scam. If you've tried this and you're still unsure, report it.


NITRO
THINK BEFORE
YOU LINK
Recognise
Realise
Report
Remove

Think before you link

Be discreet and secure online

Publicly promoting your institution's research is an important part of academic life. However, foreign powers and their proxies can use this information to identify researchers working on critical or dual-use technology and target them to acquire it. Where possible, create policies that sensibly limit how much of this information is shared online.

Be discrete about what you post online and to whom. Without knowing it, you may reveal information about yourself, what you know or can access, which malicious agents can use to target you. Consider carefully what you post online about your accesses, what you're working on, who you meet with and where you travel to as this could provide insights to a foreign power.

Also, be aware that not everyone you meet online is who they say they are. The Think Before You Link campaign, developed in concert with our United Kingdom, United States and Canadian security partners, provides information on how to prevent online targeting by foreign intelligence services. We know that foreign spies are mining social and professional networking profiles for Australian clearance holders and government and industry professionals with access to sensitive information. We also see them using professional networking sites to approach potential targets for grooming and as a precursor for recruitment activity.

We are not telling you to stop using social media and professional networking sites. We understand these are an important part of how we live and work. We are asking that you be aware of the risks, to think about what you are putting online and who you connect with, and to take action if you suspect you are being targeted.

Check before you connect

Your new connections aren't always who they say they are, and this can put you and your orgainisation at risk.

Remember the four Rs

Recognise
the profile?

Realise
the potential threat

Report
to your security manager

Remove
them from your network

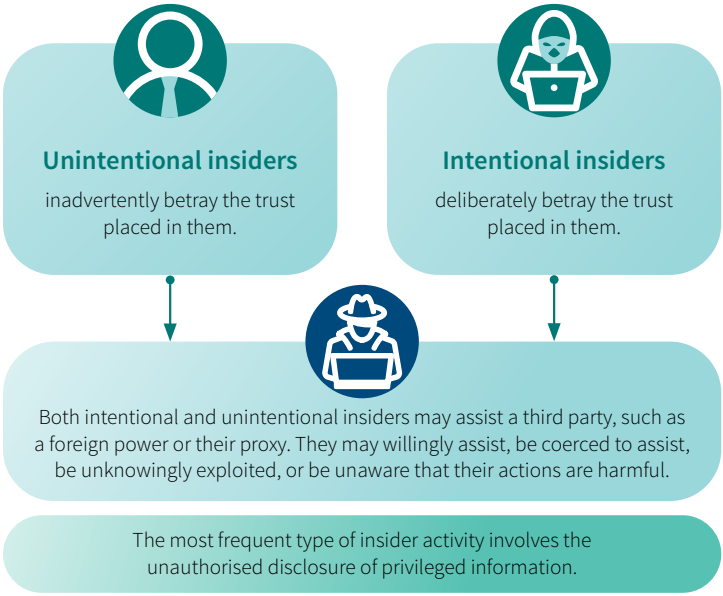
Case study

In March 2023, several employees of an Australian think tank were approached by a consultant via LinkedIn and asked to participate in phone interviews about their knowledge of Australia's AUKUS arrangements and defence industry. The employees were told they could name their own fee for the interview, which would take 30-45 minutes.

Beware of any offer that seems too good to be true—particularly if it is made in exchange for sensitive or other non-public information. You never know who the end beneficiary of this information could be. Report these kinds of approaches to your institution's security team, and to ASIO through the NITRO portal.

Counter the insider threat

Insiders are current and former employees or contractors who have legitimate or indirect access to a workplace's people, information, techniques, activities, technology, assets or facilities. Insiders may conduct activities that could harm the workplace, be detrimental to Australia's national security, undermine Australia's sovereignty and prosperity, or even pose a threat to life.



Examples of unintentional insider activity include:

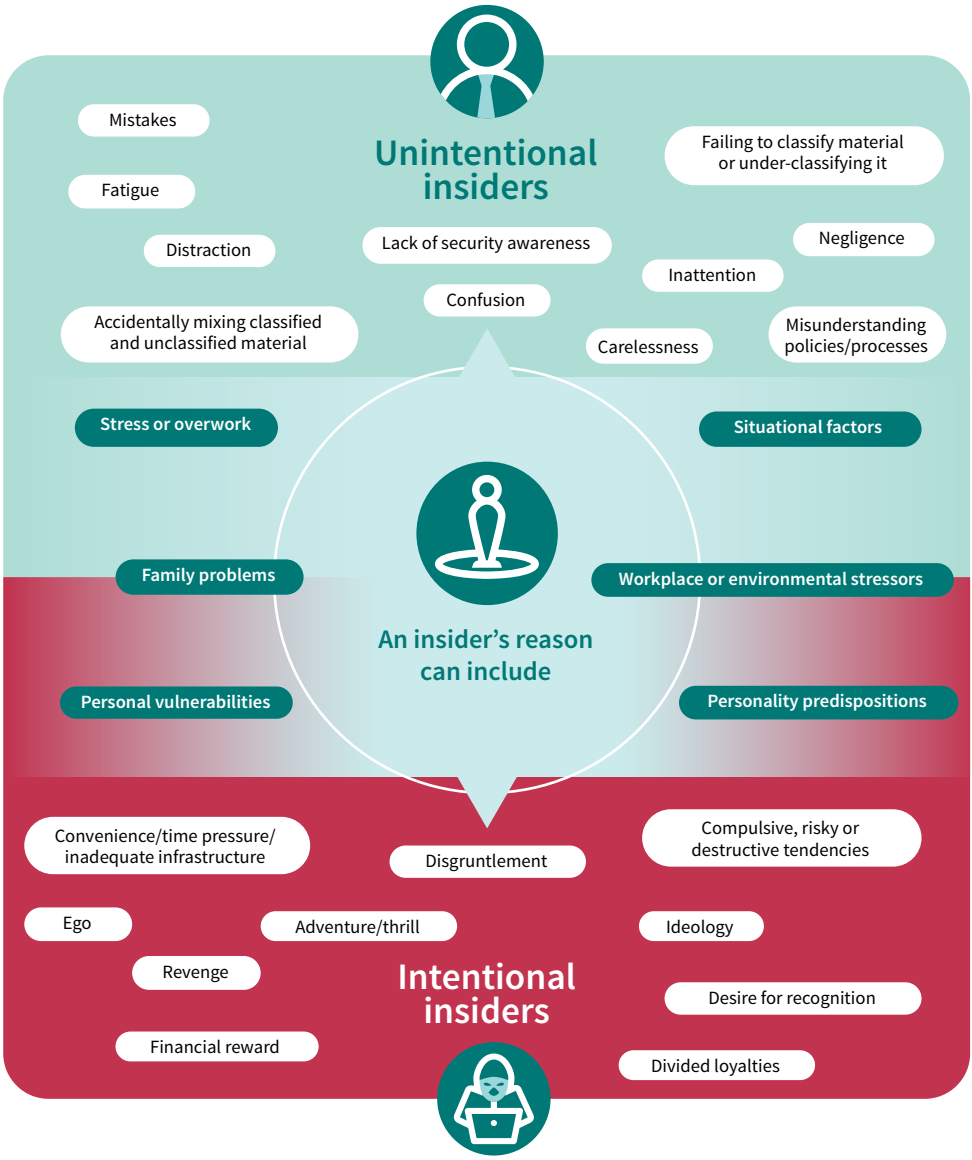
- absent-mindedly clicking on email links that lead to malicious network compromise by a third party
- misplacing a workplace-issued security pass, electronic device or sensitive document
- being unknowingly exploited by a third-party, such as a foreign power, competitor, friend or associate
- carelessly oversharing privileged information at a social gathering or in a public place
- mistakenly providing information to a colleague who doesn't have an appropriate security clearance or valid need to know.

Examples of intentional insiders include individuals who:

- publicly disclose classified or privileged information as an act of revenge
- share sensitive intellectual property with a third party—such as a foreign power—in exchange for payment or other personal benefit.

Insiders can have varied and often complex reasons for conducting harmful activities and may conduct those activities intentionally or unintentionally.

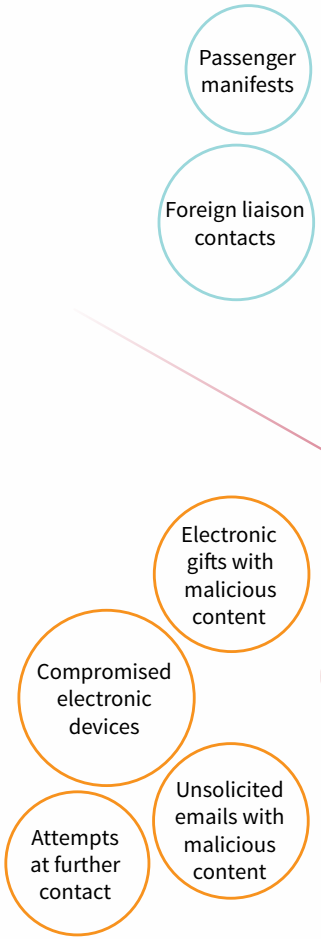
Organisations can harden themselves to the insider threat, and limit the damage if compromise occurs, by establishing a counter insider threat program (CITP). A CITP is a set of measures to manage the risk of, and deter, detect, respond to and recover from, the insider threat. Organisations that implement the *Protective Security Top 10* will have all the elements in place for a CITP.



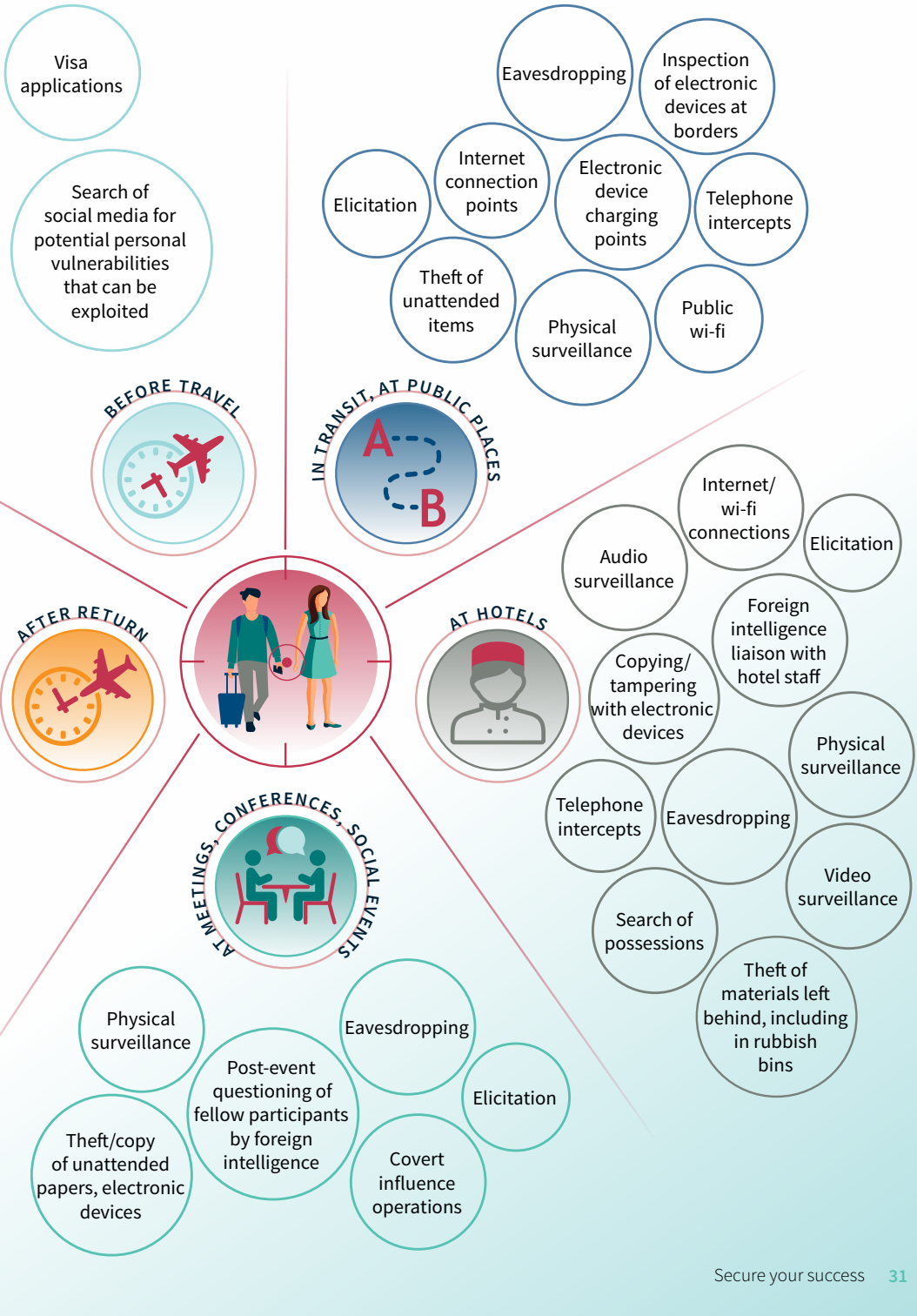
Be security-aware when you travel

Espionage and foreign interference can occur anywhere, including Australia; however, foreign intelligence services can operate more easily in their home countries where they control the environment and can draw upon a wide range of resources. This home ground advantage means Australians offshore are more vulnerable to targeting by foreign powers. Individuals can also be relaxed or distracted while travelling which creates opportunities for exploitation or unintentional compromise of information.

The following shows how you can be compromised before, during and after travel.



How security can be compromised before, during and after travel


Visa applications
Search of social media for potential personal vulnerabilities that can be exploited
BEFORE TRAVEL
Eavesdropping
Inspection of electronic devices at borders
Internet connection points
Elicitation
Electronic device charging points
Telephone intercepts
Theft of unattended items
Physical surveillance
Public wi-fi
IN TRANSIT, AT PUBLIC PLACES
A
B
Internet/ wi-fi connections
Elicitation
Audio surveillance
Foreign intelligence liaison with hotel staff
AT HOTELS
Copying/ tampering with electronic devices
Physical surveillance
Telephone intercepts
Eavesdropping
Video surveillance
Search of possessions
Theft of materials left behind, including in rubbish bins
AFTER RETURN
AT MEETINGS, CONFERENCES, SOCIAL EVENTS
Physical surveillance
Eavesdropping
Post-event questioning of fellow participants by foreign intelligence
Elicitation
Theft/copy of unattended papers, electronic devices
Covert influence operations

The following shows how you can protect yourself while travelling

Secure your information

- Don't leave luggage unattended.
- Don't put official documents in check-in luggage.
- Keep sensitive documents with you, and be aware hotel safes can be accessed.
- Don't post information about your travel on social media.
- Use official/group contact information for visa applications.

Protect your devices

- Don't leave electronic devices unattended.
- Don't use public or hotel wi-fi.
- Don't use public charging points.
- Don't take personal electronic devices.
- Don't store electronic devices in hotel safes.

Contact reporting

- Report all suspicious, ongoing, unusual or persistent contact while overseas to your agency security adviser.
- Be aware contact can occur before, during and after your travel.

Guard your conversations

- Don't have sensitive conversations where you can be overheard.
- Consider who needs to know information about your travel.
- Report suspicious questioning.

Protect electronic devices

Electronic devices make our lives easier in many ways, but they also make it easier for foreign powers to steal personal and sensitive information. Electronic devices can be compromised in a number of including:

- vulnerabilities in the operating system and applications
- malware on a website you browse or an application you download that enables remote access to your camera and microphone
- physical tampering when not in your possession.

Turning your phone off does not disable all connectivity. Your phone's power switch signals the phone to go into, and out of, a deep power-saving mode; however, the phone may still be running some functions. Some malware can imitate a shutdown sequence while leaving its own software routines running.

Consider: How many of your apps work without enabling the camera and/or microphone? Do you disable the camera and microphone in ALL your apps when not using them? Do you take your device into secure areas and/or have sensitive discussions near your device?

Are you aware that once you grant an app access to your camera and microphones, it can:

- access both the camera and microphones at any time
- record audio and take photographs and videos without alerting you
- upload the audio, photographs and videos to an internet repository
- run real-time voice and facial recognition code to detect facial features or expressions and find existing photographs of you on the internet.

Protect yourself by doing the following things.

- Never take your phone into areas or meetings where sensitive information is discussed.
- Keep your phone and app software up-to-date.
- Only download reputable apps and consider how much you trust the operators of your apps: look at their reputation and country of origin; check what access the app requires; and read reviews and do research before selecting apps.
- Use your phone manufacturer's video and audio apps rather downloading apps from the App Store or Google Play.
- Revoke camera and microphone access to apps.
- Disable auto Multimedia Messaging Service (MMS) downloading.
- Think carefully before clicking any link and think carefully when browsing the internet.

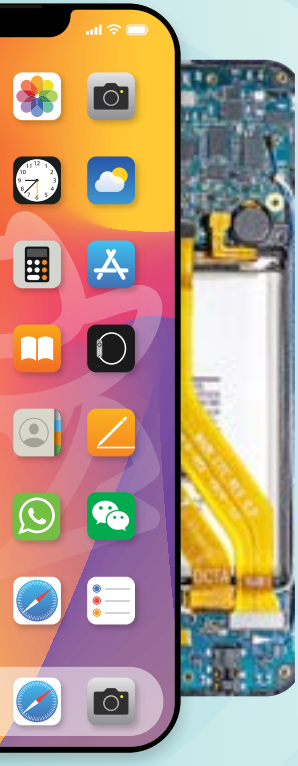
Device security

Why target my device?

- Privileged or sensitive information
- Camera and microphone access
- Login credentials
- Personal and biometric data
- Location data
- Contact lists
- Encrypted messaging apps (e.g. Signal, WhatsApp, WeChat)

How can my device be compromised?

- Physical access by hostile actors—both in Australia and overseas
- One-click access: malware installed by phishing emails and texts
- Zero-click access: malware installed without any interaction from the user



Take steps to avoid compromise…

Maintain ***physical security*** of your device.

Use ***complex passwords*** which are changed regularly and *two-factor authentication*.

Think before you click—even where an email appears to be from a ***trusted source***.

Install ***software updates***.

Switch off device daily.

… but treat your device as compromised

Never take *devices into sensitive meetings*.

Consider what is said and done in the vicinity of devices.

Consider what *information is stored on your device*.

Limit apps' ***access*** to your device's *microphone*, *camera* and *location data.*

Mythbusters

Myth: I'll know my device is compromised because the battery will drain faster than usual.

Fact: Incorrect. While some malware can drain the battery, other malware may not affect battery life.

Myth: I'll know my device is compromised because it will be hotter than before.

Fact: Incorrect. While a phone compromise will cause an increase in temperature, it may not always be noticeable. Further, there can be many other reasons why a phone could run hotter—for example, light and heat from the sun, and activities that make the battery run harder such as apps running in the background and the screen brightness being turned up.

Myth: Only apps that require intrusive permissions can lead to compromise.

Fact: Incorrect. Most apps ask for certain permissions when installing. Even apps that don't initially request access may turn permissions on during an update, without you knowing about it. These permissions can provide access to the microphone, camera, photos, contacts, location, files or storage. Be selective about which apps you download and which permissions you allow, and regularly review your apps and their settings to see which permissions they are using.

Myth: If my device has been compromised, my data usage will increase.

Fact: Correct. You will use more data if your phone is compromised as the malware on your device will increase your data usage. However, videos, apps and updates can also use a lot of data, so it can be difficult to determine the reason for an increase in data usage.

Myth: It's very unlikely my device would be compromised because only a niche set of skills and high-end technology is capable of that.

Fact: Incorrect. Sophisticated technology and skills are no longer required to compromise a device like a mobile phone. Instructional material is available on the internet and the necessary software is readily available and affordable. Even with basic equipment and knowledge it can be difficult to detect a compromise, as this software still allows access to a range of functionality on the device including camera, microphone and locational data.

The following YouTube links show how easy it is to install malware on your phone:

- https://www.youtube.com/watch?v=QiM35PmI2dQ
- https://www.youtube.com/watch?v=yBseGNVPIGQ
- https://www.youtube.com/watch?v=CaJZTjOdM7g

Myth: Hackers can only obtain data if users download a malware file.

Fact: Incorrect. A phone can be compromised in a range of ways, including when you open an executable file in an email, or visit websites that surreptitiously share files. Think before you open an attachment and avoid visiting websites you're unfamiliar with, especially if you've been prompted to open them via an email link.

Myth: A hacker requires physical access to your phone to compromise it.

Fact: Incorrect. A hacker can easily load software on your phone if they have physical access, but there are other ways. These include the use of unsecure wi-fi (public wi-fi), flaws in the operating system, downloading malicious apps and inadvertently installing malware by opening links in nefarious emails.

Secure what you know with NITRO

asio.gov.au

24-14779