



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre

Stakeholder kit

Cyber Security Awareness Month 2025

Table of contents

About this kit3

Key messages4–6

Editorial content7–9

Social media posts10–14

Get social15

Further resources16

About ASD’s ACSC17

Get in touch18

About this kit

Building our cyber safe culture

The whole of Australian Government theme for Cyber Security Awareness Month 2025 is ***Building our cyber safe culture***.

This October presents a great opportunity for all Australians to take action to safeguard themselves online. To do this, the Australian Government encourages the community to focus on these 3 key actions:

1. Install software updates to keep your devices secure.
2. Use a unique and strong passphrase on every account.
3. Always set up multi-factor authentication.

Further resources for the general community are available at actnowstaysecure.gov.au/cybermonth2025.

Join ASD's ACSC to take action this Cyber Security Awareness Month

At the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) we want to ensure the nation's cyber security practitioners and decision-makers can take action using the most up-to-date information on the latest threats and advice.

As the Australian Government's technical authority on cyber security, this Cyber Security Awareness Month, ASD's ACSC will focus on vital technical

mitigations and advice businesses and organisations should implement as part of their cyber security strategy.

To do this, each week in October will cover a different theme to help organisations to take action.

These themes cover key measures Australian businesses and organisations can do to maintain robust cyber security in the current threat environment and into the future. The themes are:

Week 1: Event logging (1-8 October).

Week 2: Legacy technology (9-15 October).

Week 3: Supply chain and third-party risk (16-22 October).

Week 4: Quantum readiness (23-31 October).

How you can help

This kit provides key messages and content to help you take action this Cyber Security Awareness Month.

We encourage you to use and adapt the resources in this kit to amplify the key messages to your technical audiences.

Additionally, keep an eye out for publications released on cyber.gov.au in October for Cyber Security Awareness Month 2025.

By sharing these materials with your networks, you can help us in the fight against cybercrime and better protect Australian organisations and individuals.

Key messages

General messages

- This Cyber Security Awareness Month, the Australian Government theme is ***building our cyber safe culture***.
- For simple steps and resources to take action and safeguard yourself online, visit actnowstaysecure.gov.au/cybermonth2025.
- For those who need more than the basics, join ASD's ACSC this Cyber Security Awareness Month.
- This Cyber Security Awareness Month take action to protect your networks and digital infrastructure now and into the future.
- Follow along as ASD's ACSC addresses a new theme each week, to support Australian organisations, businesses and cyber security professionals to take action and build a robust cyber security posture.
- Event logging, legacy technology, supply chain and third-party risk, and quantum readiness are all part of the conversation.
- **Join ASD this Cyber Security Awareness Month 2025 and take action at cyber.gov.au/CAM2025.**

Tactics to consider

You can use the key messages and resources in this kit to raise awareness of Cyber Security Awareness Month messages, and the importance of cyber security:

- ✓ Tell your technical audiences, stakeholders, staff and customers about Cyber Security Awareness Month and share the general and technical key messages.
- ✓ Feature content and information about Cyber Security Awareness Month in internal and external newsletters and on your website.
- ✓ Forward to your communications team to repurpose this content across your internal and external communications channels.
- ✓ Share content from this kit on social media and encourage the audience to take action.
- ✓ Provide talking points to your managers, senior leaders and executive for meetings, events and engagements to start the conversation about cyber security.
- ✓ Direct people to cyber.gov.au/CAM2025 to learn how to take action on their cyber security.

Week 1: Event logging

- You can't defend what you can't see. Event logging shines a constant light into what's happening within your networks.
- Effective logging helps detect the threats that might have gone unseen.
- Malicious cyber actors thrive when organisations lack effective logging, as it gives them an invisibility cloak to move unseen within networks.
- Organisations should implement best practice logging by review ASD's **Best practices for event logging and threat detection** publication at cyber.gov.au/CAM2025.

Week 2: Legacy technology

- Legacy technology is outdated hardware and software that is no longer supported by vendors.
- Malicious actors can use legacy tech vulnerabilities as an open door to access to your systems.
- Organisations often put off replacing legacy tech because of the cost, but replacing it is less expensive than a cyber attack. In 2023-24, the average cybercrime cost to a small business was almost \$50,000.
- Modern tech keeps pace with changing threats thanks to frequent updates and patching. Legacy systems don't. There's no security peace of mind in legacy tech.
- Replacing legacy tech can take time, so consider temporary protective steps like segmenting your networks and implementing logging and monitoring. More advice is available at cyber.gov.au/CAM2025.

Week 3: Supply chain and third-party risk

- Always consider the cyber security of your providers. The risks of those who supply you are also yours.
- Supply chain and third-party risks must be part of your organisation's cyber security strategy, as malicious cyber actors have used supply chains to break the chains of your network security.
- Supply chain weaknesses have led to data breaches, system outages and theft of precious commercial data.
- Manage third-party risk by adopting products and services that are secure in their very design. More advice is available at cyber.gov.au/CAM2025.

Week 4: Quantum readiness

- The adoption of post quantum cryptography is crucial right now for safeguarding digital infrastructure into the future.
- ASD encourages all organisations to be prepared by 2030 by moving to more secure forms of encryption.
- Your organisation's communications, information and data are at risk. Start the process of transitioning to quantum-resistant cryptographic algorithms now.
- ASD's guide, **Planning for post-quantum cryptography**, is at cyber.gov.au/CAM2025.

Editorial content

Use this suggested content across your communication channels, including newsletters, staff intranet pages, website news or blog articles, and customer or stakeholder emails.

Editorial 1: Take action on your cyber basics this Cyber Security Awareness Month

The theme for this year's Cyber Security Awareness Month is 'Building our cyber safe culture'.

To do this, Australians are reminded to take action on 3 simple steps:

1. Install software updates to keep your devices secure.
2. Use a unique and strong passphrase on every account.
3. Always set up multi-factor authentication.

For those who need more than the basics, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), will publish content to help you take action to protect your networks and digital infrastructure now and into the future.

Each week ASD's ACSC will focus on a different technical theme:

1. Event logging
2. Legacy technology
3. Supply chain and third party risk
4. Quantum readiness

Learn how to take action on your cyber security at cyber.gov.au/CAM2025.

Editorial 2: Don't fly blind – take action and use event logging

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is emphasising taking action this Cyber Security Awareness Month – event logging is one of the 4 key technical themes being covered.

You can't defend what you can't see. The increased prevalence of malicious actors employing Living Off The Land (LOTL) techniques highlights the importance of taking action to implement and maintain an effective event logging solution.

Security information and event management (SIEM) tools use event logs to analyse network activity, helping network administrators understand what is happening within a network.

When used effectively, event logging is a vital mitigation in an organisation's cyber security arsenal.

It helps alert network defenders to cyber security events (like critical software configuration changes) and the presence of malicious actors.

Don't fly blind – use event logging as part of your cyber security mitigations. Take action at cyber.gov.au/CAM2025.

If your data has been stolen or leaked, learn how to report and recover from a [data breach](#) and [account compromise](#) on cyber.gov.au/report

Editorial 3: Don't let legacy tech define your legacy – take action on old tech

Take action and make sure your legacy technology isn't a threat this Cyber Security Awareness Month.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is taking action this Cyber Security Awareness Month – legacy technology is one of the 4 key technical themes being highlighted.

Legacy technology includes any technology no longer supported by the vendor.

We know how difficult it can be to keep up with the latest technology but ensuring it is up to date is less expensive than a major cyber incident.

Legacy technology can leave an organisation's most important data, networks and devices vulnerable to a cyber attack.

Because of a lack of vendor support, legacy technology does not receive the security updates or bug fixes necessary to protect against cyber incidents, making it more vulnerable to attack.

The most effective strategy to reduce the risk from legacy technology is to take action and replace it. If not feasible, or if replacement takes time, adopt temporary measures like network segmentation and advanced logging and monitoring to reduce the associated risks.

Learn how to take action on your cyber security at cyber.gov.au/CAM2025.

If your data has been stolen or leaked, learn how to report and recover from a [data breach](#) or [account compromise](#) on cyber.gov.au/report

Editorial 4: Shut the backdoor: Take action to make sure your supply chain is secure

Supply chain cyber security should be treated as seriously as your own. Take action this Cyber Security Awareness Month.

Cyber supply chain risk management should form a significant component of any organisation's overall cyber security strategy.

An effective cyber supply chain and third-party risk management strategy supports the secure supply of products and services through their lifespan.

Cyber supply chain risk is present if a supplier, manufacturer, distributor or retailer are involved in products or services used by an organisation.

As part of this strategy, businesses should ensure take action to:

- ✓ identify the supply chain
- ✓ understand cyber supply chain risk
- ✓ set cyber security expectations
- ✓ audit for compliance
- ✓ monitor and improve cyber supply chain security practices.

Further information on each of these steps is available on cyber.gov.au/CAM2025.

If your data has been stolen or leaked, learn how to report and recover from a [data breach](#) or [account compromise](#) on cyber.gov.au/report

Editorial 5: Are you ready to take the Quantum leap?

Quantum computing will have significant impacts on cyber security.

Are you ready to take action for post-quantum cryptography? A cryptographically-relevant quantum computer will render common public-key encryption protocols insecure.

This means communications and data you once thought secure could be at a greater risk of compromise.

It is vital relevant staff are educated on what this technology will mean for cyber security. Consider decommissioning technologies that cannot be upgraded.

Take action and prepare your business or organisation by using the LATICE framework:

- ✓ **Locate** and catalogue the use of traditional asymmetric cryptography
- ✓ **Assess** the value and sensitivity of systems and data protected by traditional asymmetric cryptography.
- ✓ **Triage** systems using traditional asymmetric cryptography and prioritise individual systems for transition.
- ✓ **Implement** post-quantum cryptographic (PQC) algorithms throughout systems.
- ✓ **Communicate** with vendors and stakeholders, and **educate** and train relevant stakeholders on the PQC transition.

Don't wait – take the quantum leap to prepare for post-quantum cryptography. Learn how to take action on your cyber security at cyber.gov.au/CAM2025.

Social media posts

Use the suggested post text and links below on your social media channels. Feel free to adapt or tailor these messages to your audience and channels.



Post 1: Cyber Security Awareness Month

Platform	Purpose	Suggested post text
Facebook, Instagram and LinkedIn	Raise awareness/educate	<p>October is Cyber Security Awareness Month, which is the perfect opportunity to take action by building on the basics and tackling the technical to help boost Australia's cyber security posture.</p> <p>Follow along with ASD's ACSC and learn more about crucial cyber security mitigations like event logging, legacy technology, supply chain and third-party risk, and quantum readiness.</p> <p>Learn how to take action on your cyber security at 🔗 cyber.gov.au/CAM2025</p>
X (Twitter)	Raise awareness/educate	<p>Cyber Security Awareness Month is the perfect time to take action on crucial cyber security mitigations like event logging, legacy technology, supply chain and third-party risk, and quantum readiness.</p> <p>Learn how to take action on your cyber security at 🔗 cyber.gov.au/CAM2025</p>



Post 2: Event logging

Platform	Purpose	Suggested post text
Facebook, Instagram and LinkedIn	Raise awareness/educate	You can't defend what you can't see.
		Event logging is crucial for detecting threats and keeping your most vital networks and data secure.
		Take action on your event logging this Cyber Security Awareness Month 👉 cyber.gov.au/CAM2025
X (Twitter)	Raise awareness/educate	You can't defend what you can't see.
		Get up to speed with event logging this Cyber Security Awareness Month.
		Take action and learn more here 👉 cyber.gov.au/CAM2025

Post 3: Legacy technology

Platform	Purpose	Suggested post text
Facebook, Instagram and LinkedIn	Raise awareness/Educate	<p>Legacy IT increases the risk that an organisation will experience a cyber security incident.</p> <p>It can also make a cyber security incident much more impactful. Take action – don't let legacy tech define your legacy.</p> <p>Take action on your legacy technology this Cyber Security Awareness Month  cyber.gov.au/CAM2025</p>
X (Twitter)	Raise awareness/Educate	<p>Don't let legacy tech define your legacy – it increases the risk that an organisation will experience a cyber security incident.</p> <p>Take action on your legacy technology this Cyber Security Awareness Month  cyber.gov.au/CAM2025</p>

Post 4: Supply chain and third party risk

Platform	Purpose	Suggested post text
Facebook, Instagram and LinkedIn	Raise awareness/Educate	Treat supply chain security as seriously as your own.
		Malicious actors use supply chains as a point to enter networks and leave organisations vulnerable to cyber-crime.
		Supply chain risk management must be part of every cyber security strategy.
		Take action on your supply chain security during Cyber Security Awareness Month  cyber.gov.au/CAM2025
X (Twitter)	Raise awareness/Educate	Treat supply chain cyber security as seriously as your own.
		A vulnerability in a supply chain could allow a malicious actor to access important information and networks.
		Take action on your supply chain during Cyber Security Awareness Month  cyber.gov.au/CAM2025

Post 5: Quantum readiness

Platform	Purpose	Suggested post text
Facebook, Instagram and LinkedIn	Raise awareness/Educate	<p>Are you ready for post-quantum cryptography? Don't wait – take the quantum leap to keep your organisation's communications, information and data secure.</p> <p>Learn more about post-quantum cryptography and take action this Cyber Security Awareness Month</p> <p>👉 cyber.gov.au/CAM2025</p>
X (Twitter)	Raise awareness/Educate	<p>Are you ready for post-quantum cryptography?</p> <p>Don't play catch up. Use the LATICE framework to help you transition – locate, assess, triage, implement, communicate, educate.</p> <p>Learn more about post-quantum cryptography and take action this Cyber Security Awareness Month</p> <p>👉 cyber.gov.au/CAM2025</p>

Get social

Join the conversation by following ASD's social media channels and share the latest cyber security social content with your followers. By sharing ASD's social content you can help your followers improve their cyber security.

Please use the following hashtags when you share or post to help Australians stay secure online: #CyberMonth2025



[@ASDGovAU](https://twitter.com/ASDGovAU)



[Australian Signals Directorate](https://www.linkedin.com/company/australian-signals-directorate/)



[asd.gov.au](https://www.asd.gov.au)



[Australian Signals Directorate](https://www.facebook.com/australian-signals-directorate/)

Further resources

Become an ASD Partner

Want priority access to the latest resources and advice?

Join ASD's free [Cyber Security Partnership Program](#) as a Business Partner or Network Partner to receive cyber security alerts, advisories and up-to-date advice, as well as join initiatives to uplift the cyber resilience of Australian organisations.

Responding to cyber incidents

For immediate assistance during a cyber incident, **call the 24/7 Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).**

ASD is not a regulator; we are here to help you respond to and recover from cyber incidents. Make sure to report cyber threats, incidents and vulnerabilities early and often at cyber.gov.au/report or call our 24/7 hotline.

If you request support, we can provide you with immediate advice and assistance, which may include:

4. information on how to contain and remediate an incident
5. intelligence and advisory products to help you with your incident response
6. linking you to Australian Government entities that may further support your response.

Every report helps us build a national cyber threat picture and informs the development of our advice and guidance.

About ASD's ACSC

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security.

Who we help

Our advice and assistance is for the whole economy, including:

- critical infrastructure and systems of national significance
- federal, state and local government
- small and medium businesses
- academia
- charities and not-for-profit organisations
- the Australian community.

What we do

ASD brings together capabilities to improve Australia's national cyber resilience. Its services include:

- providing the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, on 1300 CYBER1 (1300 292 371)
- publishing alerts, technical advice, advisories and notifications on significant cyber security threats
- monitoring cyber threats and intelligence sharing with partners
- helping Australian entities respond to cyber security incidents

- enhancing the cyber security resilience of Australian entities with exercises and uplift activities
- enabling Australian organisations and individuals to engage with the ASD's ACSC and fellow partners through ASD's Cyber Security Partnership Program.

The most effective cyber security is collaborative and our partnerships are key. We thank contributors to the development of our guidance and the organisations who help uplift Australia's cyber security by sharing the latest cyber security advice, alerts and guidance.

Further assistance

ASD is not a regulator; we are here to help you recover from cyber incidents. Make sure to report cyber threats, incidents and vulnerabilities early and often at cyber.gov.au/report or call 1300 292 371 (1300 CYBER1).

Your report helps us build a national cyber threat picture and informs the development of our advice and guidance.

Get in touch

If you would like to subscribe to receive future stakeholder kits from ASD's ACSC or have any questions, please email our Public Communication team at asd.publiccomms@defence.gov.au.



Australian Government
Australian Signals Directorate

ASD

**AUSTRALIAN
SIGNALS
DIRECTORATE**

ACSC

**Australian
Cyber Security
Centre**