



Australian Government
Australian Signals Directorate

cyber.gov.au

Stakeholder Kit

Annual Cyber Threat Report 2025–26

Contents

About this kit	3
The Annual Cyber Threat Report	3
How you can help	3
Key messages	4
For all Australians	4
For all businesses and organisations	5
For critical infrastructure	6
Case Studies	7
Case study 1 Multi-stage social engineering – Scattered Spider	7
Case study 2 Vishing attack targets Australian bank	8
Editorial content	9
Communicating to everyday Australians	9
Communicating to businesses	10
Further resources	11
Campaign resources	12
Campaign factsheets	13
About ASD's ACSC	14
Get social	15



About this kit

The Annual Cyber Threat Report

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has released the seventh [Annual Cyber Threat Report 2025-26](#) (ACTR), marking its flagship public assessment of Australia's cyber threat environment.

Cyber threats continue to evolve in scale, speed and sophistication and as emerging technologies such as artificial intelligence (AI) reshape the cyber landscape, understanding the threat environment has never been more important.

Drawing on operational and intelligence insights, the report provides:

- an overview of the cyber threat landscape
- the cost of cyber incidents
- how ASD is responding
- **practical advice** to help all Australians strengthen their cyber resilience
- case studies of real-world cyber incidents and their impacts.

How you can help

Cyber security is a shared responsibility and we want all Australians to understand the current threat environment and be well equipped to take action.

This kit provides key messages, ready-to-use content and supporting resources to help you promote the findings of the ACTR through your communication channels and networks.

Tactics to consider

- Share the report with staff, leaders, stakeholders and customers.
- Incorporate key messages into social media content, newsletters, websites and internal communications.
- Use the editorial content and campaign resources to promote cyber security awareness.
- Support the adoption of practical cyber security measures.
- Highlight the role reporting plays in strengthening Australia's collective cyber resilience.
- Promote the reporting of cyber incidents and suspicious activity to ASD throughout the year.

Key messages

For all Australians

- The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has released our seventh Annual Cyber Threat Report 2025-26 (ACTR).
- The ACTR provides an overview of the cyber threats affecting Australian individuals, businesses, organisations and critical infrastructure entities, along with practical advice to help strengthen cyber resilience.
- In 2025-26 the ACSC received over 82,000 cybercrime reports to Report Cyber, that's one report every 6 minutes.
- Average self-reported cost of cybercrime per report for individuals remained consistent with last year (\$33,000).
- Australia continues to face an increasingly complex and evolving cyber threat environment. Cybercriminals and state-sponsored cyber actors continue to target Australians, businesses and critical infrastructure.
- **Artificial intelligence** is reshaping the cyber threat landscape, helping malicious cyber actors operate with greater speed, scale and sophistication.

Key action to protect yourself online

Strong cyber security starts at home. Begin with the basics:

- Apply updates to devices, systems and applications when they become available.
- Perform regular backups.
- Turn on multi-factor authentication for online accounts.
- Set long, unique passwords.
- Learn to recognise scams and report them .
- **Sign up to our alerts and advisories** so you know the threat.
- Check and manage privacy settings.
- Think before you share on **social media**.

For all businesses and organisations

Refer to the previous messages for all Australians, plus:

- During 2025-26, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has continued to observe malicious cyber actors targeting Australian businesses and organisations.
- State-sponsored actors continue to target Australian businesses and organisations to support their strategic, political and economic objectives. They may also seek to pre-position on networks for future disruptive activities.
- Cyber security is a business risk, not simply an IT issue. Organisations should take proactive steps to strengthen resilience against an increasingly complex threat environment.
- Organisations should operate with an assumed breach mindset and plan for how (not if) they would respond to and recover from a cyber-incident.
- Artificial intelligence is delivering significant productivity benefits, but it is also enabling malicious cyber actors to identify vulnerabilities, develop exploits and conduct attacks at greater speed. It is critical that organisations understand and prepare for AI-enabled cyber threats.
- Supply chain vulnerabilities continue to create opportunities for malicious cyber actors. Organisations should understand and manage third-party cyber security risks.
- Stay informed through ASD's Cyber Security **Partnership Program** and resources available at cyber.gov.au
- Average self-reported cost of cybercrime per report for businesses up 16% overall (\$93,500).
 - **Small business:** \$55,400 (consistent with last year)
 - **Medium business:** \$141,300 (up 45%)
 - **Large business:** \$148,100 (down 27%).

Key actions to help strengthen organisational resilience

- Replace or mitigate **legacy technology**.
- Implement best-practice **event logging**.
- Manage **supply chains**, including by choosing products and services that are **secure by design**.
- Prepare for **post-quantum cryptography**.
- Prepare for **AI-enabled cyber threats**.

For critical infrastructure

Refer to the previous messages, plus:

- Critical infrastructure (CI) underpins Australia's economy, security and way of life.
- CI entities are an attractive target for state-sponsored cyber actors and cybercriminals
- State-sponsored actors may also pre-position on networks for disruptive activities during periods of crisis or conflict.
- Organisations should treat cyber incidents as a matter of 'when', not 'if' and prepare for disruption before it happens.
- **Supply chain** resilience, operational preparedness and effective incident response planning are critical components of cyber resilience.
- Early **reporting** enables ASD to provide assistance quicker and supports our understanding of the cyber threat environment.
- Critical infrastructure organisations should:
 - continue to strengthen cyber resilience through preparedness, collaboration and proactive engagement with ASD's ACSC.
 - prepare for disruption before it occurs and regularly test their ability to respond to, and recover from, cyber incidents.
 - apply ASD guidance, including ASD Essentials and CI Fortify, to strengthen resilience and support the continuity of essential services.
 - be prepared to isolate their systems for 3 months.
- Top 3 ANZSIC divisions for CI incidents:
 - Financial and Insurance Services (30%)
 - Public Administration and Safety (21%)
 - Electricity, Gas, Water and Waste Services (17%).

For advice and publications relevant to your organisation, visit the **ASD Essentials**, **CI Fortify**, **Operational Technology environments** and **Critical Infrastructure Uplift Program (CI-UP)** on cyber.gov.au

Common techniques contributing to critical infrastructure incidents*

- **Phishing (36%)** – Adversaries used malicious emails, messages, or other communications to deceive users and gain initial access to systems or credentials.
- **Valid accounts (16%)** – Adversaries obtained and misused legitimate user accounts to access networks and systems without triggering traditional security controls.
- **Drive-by compromise (10%)** – Adversaries gained access when a user visited a compromised or malicious website, resulting in the unintended download or execution of malicious content.

Annual Cyber Threat Report 2025–26

Case Studies

Case study 1 | Multi-stage social engineering – Scattered Spider

On 30 July 2025, ASD's ACSC and international partners released an updated joint advisory in response to recent activity by [Scattered Spider](#) threat actors against commercial facilities sectors, subsectors and other sectors.

Scattered Spider threat actors typically engage in data theft for extortion and use several [ransomware](#) variants, most recently deploying ransomware alongside their usual [tactics, techniques, and procedures](#) (TTPs). While some TTPs remain consistent, Scattered Spider threat actors often change TTPs to remain undetected.

Scattered Spider has been observed researching organisations to identify usernames, passwords, personally identifiable information (PII), and to conduct SIM swaps. The threat actors then use layered [social engineering](#) techniques, which frequently occur over several calls. The social engineering attempts are designed to first learn what steps are needed to conduct password resets from helpdesks. Once that information is identified, the threat actors continue to conduct phone calls to employees and help desks to gather password reset specific information of a targeted employee.

Finally, the threat actors conduct spear [phishing](#)¹ calls to convince IT help desk personnel to reset passwords and/or transfer multi-factor authentication tokens. At which point, the threat actors perform account takeovers against the users in single sign-on environments. These social engineering attempts are enriched by access to personal information derived from social media, open-source information, commercial intelligence tools, and database leaks.

Visit [Multi-factor authentication](#) and [Connecting to public Wi-Fi](#) for more information.

1. Spear phishing is "a form of phishing that targets a specific person or group" (Australian Cyber Security Centre [ACSC], n.d.). For further information, see the ACSC Glossary and ACSC guidance on phishing.

Case study 2 | Vishing attack targets Australian bank

In August 2025, a bank reported to ASD an incident involving two phone calls to its internal help desk, in which the callers impersonated staff members to obtain information.

The callers impersonated a Melbourne-based employee, using staff details such as the employee's ID number, and claimed they were unable to connect with colleagues via Microsoft Teams. The calls indicated that the threat actor had conducted prior intelligence gathering on the organisation. Questions focused on a specialised financial services team located in Melbourne and Sydney and demonstrated insider knowledge.

The threat actors were manipulative, confrontational, and aggressive throughout the phone calls, employing a range of social engineering techniques to pressure help desk staff into compliance. They successfully obtained names, job titles, and corporate phone numbers for several staff members, potentially exposing employees to increased targeting by social media, and exposing the bank to an increased likelihood of follow-on attacks.

The bank noted that the targeted team and individuals were not public figures and this lack of visibility made it easier for the threat actors to manipulate help desk staff, as the staff did not immediately perceive the requests as suspicious. During its investigation, the bank determined that the calls likely originated from a call centre or office environment, as multiple voices were audible in the background. Furthermore, the calls were not made using Voice over IP (VoIP) technology and were confirmed to have originated from Hong Kong. Recent media coverage of vishing² tactics targeting help desks prompted the bank to report the incident to ASD.

Since the incident, the bank's cyber security team has led an awareness campaign and supported team leads with additional training. Incidents involving elements of social engineering remain common in reports to ASD as threat actors leverage vulnerabilities wherever they exist, technical or human.

Visit [Protect yourself from scams](#) and [Social engineering](#) for more information. Report a cybercrime or cyber incident at [cyber.gov.au/report](#) or call the 24/7 Australian Cyber Security Hotline on **1300 CYBER1** (1300 292 371).

2. Vishing is a form of social engineering where malicious actors impersonate staff or executives to extract sensitive information or perform actions such as password resets. Malicious actors may also use AI tools such as voice cloning or deepfake technology to sound convincing and may spoof caller IDs to make their calls appear legitimate (Australian Cyber Security Centre [ACSC], 2026).

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.

Communicating to everyday Australians

Annual Cyber Threat Report highlights evolving cyber security risks to Australians.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has released the seventh **Annual Cyber Threat Report 2025-26**, highlighting the cyber threats affecting Australians and the steps we can all take to stay secure online.

The report shows that cybercriminals and state-sponsored cyber actors continue to target Australian individuals, businesses and critical infrastructure. In 2025-26, one cybercrime was reported every six minutes, demonstrating the scale of cybercrime.

Artificial intelligence is reshaping the cyber threat landscape, helping malicious cyber actors operate with greater speed, scale and sophistication.

The good news is that strong **cyber security starts with simple actions**. All Australians can reduce their risk by:

- Applying updates to devices, systems and applications when they become available
- Performing regular backups
- Turning on multi-factor authentication for online accounts
- Setting long, unique passwords
- Learning to recognise scams and report them
- Signing up to our alerts and advisories so you know the threat
- Checking and managing privacy settings
- Thinking before sharing on social media

If you experience a
cyber-incident or spot
suspicious activity, report it:



online at
cyber.gov.au/report or



call **1300 CYBER1**
(1300 292 371)



Communicating to businesses

2025-26 Annual Cyber Threat Report

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has released its seventh Annual Cyber Threat Report (ACTR).

This year's report highlights the growing impact of artificial intelligence (AI) on the cyber threat landscape. While AI delivers significant productivity gains, it also helps malicious cyber actors to identify vulnerabilities, develop exploits and conduct attacks with greater speed, scale and sophistication. During the 2025-26 financial year, ASD's ACSC received **more than 82,000 cybercrime reports**, averaging **one report every 6 minutes**. They also responded to more than 1,500 cyber security incidents and issued over 4,400 notifications to Australian entities about potentially malicious cyber activity, an increase of 80 per cent on last year.

The report reinforces that cyber security is a business risk, not simply an IT issue. Organisations should adopt an assumed-breach mindset and prepare for disruption before it occurs. Supply chain and third-party risks continue to increase exposure to cyber threats. To help organisations navigate this evolving threat environment, we recommend 5 priority actions.

- Replace or mitigate **legacy technology**.
- Implement best-practice **event logging**.
- Understand and manage **supply chain** and third-party risk by choosing products and services that are **secure by design**.
- Prepare for **post-quantum cryptography**.
- Prepare for **AI-enabled cyber threats**.

Critical infrastructure entities should also prepare to isolate systems and networks for up to 3 months.

Visit cyber.gov.au to access tailored guidance and resources, including **ASD Essentials**, **CI Fortify**, **Operational Technology environments** and **Critical Infrastructure Uplift Program (CI-UP)**.



Average self-reported cost of cybercrime per report for businesses up 16% overall (\$93,500)*.

Small business: \$55,400
(unchanged)

Medium business: \$141,300
(up 45%)

Large business: \$148,100
(down 27%).

Further resources

Artificial intelligence and cyber security

AI is reshaping the cyber threat landscape, creating new opportunities for both defenders and malicious cyber actors alike. ASD's ACSC provides guidance to help organisations understand AI-related cyber security risks, securely adopt AI technologies, and strengthen resilience against AI-enabled threats. Visit [Artificial Intelligence](#) to access practical advice, guidance and publications on AI and cyber security.

Critical infrastructure security

Australia's critical infrastructure continues to be an attractive target for malicious cyber actors. ASD's ACSC works closely with critical infrastructure owners and operators to strengthen cyber resilience through guidance, uplift activities, operational engagement and information sharing.

Visit [cyber.gov.au](#) to access resources including [ASD Essentials](#), [CI Fortify](#), [Operational Technology environments](#) and [Critical Infrastructure Uplift Program \(CI-UP\)](#).

Become an ASD partner

Join ASD's [Cyber Security Partnership Program](#) as a Business Partner or Network Partner to receive timely cyber security alerts, advisories, guidance and information. With more than 149,500 partners, the program helps strengthen cyber resilience through collaboration and information sharing.

Responding to cyber incidents

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

You can also report cyber threats, incidents and vulnerabilities online at [cyber.gov.au/report](#).

Every report helps ASD's ACSC better understand the cyber threat environment and provide faster support to those affected.

Campaign resources

The following resources are available to support promotion of the Annual Cyber Threat Report 2025-26 through organisational communication channels and stakeholder networks.

Video resources

The ACTR campaign video provides an overview of Australia's cyber threat landscape and highlights practical actions organisations and individuals can take to strengthen cyber resilience.

Watch the video [here](#).



Campaign factsheets

The factsheets provide practical information and key messages relevant to different audiences.

- Download factsheet for Individuals, Businesses & Organisations and Critical Infrastructure [here](#).




Annual Cyber Threat Report 2025-26

Factsheet for individuals

The threat landscape

Australians continue to be targeted by cybercriminals through scams, identity fraud and the theft of personal information, usernames and passwords often for financial gain. Artificial intelligence (AI) is reshaping the cyber threat landscape by lowering barriers to entry for cybercriminals and enabling malicious activity to be conducted with greater scale, speed and sophistication. As a result, phishing emails, scam messages and impersonation attempts are becoming more convincing and harder to detect. As cyber threats continue to evolve, every Australian has a role to play in strengthening their cyber security through simple, proactive action.

Key facts and statistics



Received over
82,000
cybercrime reports



1,500+
cyber security
incident responses



4,400+
notifications issued
to organisations



One report
was made every
6 minutes



\$33,000
average self-reported
cybercrime cost per
individual report



37,500+
calls answered by the Australian
Cyber Security Hotline
(102 per day on average)



Identity theft
remained the top
reported cybercrime
over the last 5 years




Annual Cyber Threat Report 2025-26

Factsheet for businesses and organisations

The threat landscape

Cybercrime remains a significant threat to Australia, with malicious cyber actors continuing to target businesses and organisations for financial gain through scams, extortion and the theft of data and credentials. State-sponsored actors also continue to target Australian organisations to advance their strategic, political and economic objectives, including seeking access for potential future disruptive activities. Artificial intelligence (AI) is also compounding these challenges, by enabling malicious cyber actors to operate with greater scale, speed and sophistication.

Key facts and statistics



Received over
82,000
cybercrime reports



1,500+
cyber security
incident responses



4,400+
notifications issued
to organisations



One report
was made every
6 minutes



\$93,500
average self-reported
cybercrime cost per
business report
(up 16%)



51%
of cyber incidents
were reported by industry
(i.e. non-government
organisations)



\$141,300
average self-reported
cybercrime cost for
medium businesses
(up 45%)




Annual Cyber Threat Report 2025-26

Factsheet for critical infrastructure

The threat landscape

Critical infrastructure (CI) underpins Australia's economy, security and way of life, making it an attractive target for cyber actors seeking financial gain, espionage opportunities or strategic advantage. Artificial intelligence (AI) is reshaping the threat landscape by lowering barriers for cyber actors and increasing the scale, speed and sophistication of malicious activity. At the same time, the growing interconnectedness of systems, operational technology and supply chains is increasing the threat surface and potential impact of cyber incidents.

Key facts and statistics



Received over
82,000
cybercrime reports



1,500+
cyber security
incident responses



4,400+
notifications issued
to organisations



One report
was made every
6 minutes



\$148,100
average self-reported
cost of a cybercrime
incident
(Large Business)



150+
cyber security incidents
responded to involving
critical infrastructure
entities



**Top sectors
for CI incidents**
Financial & Insurance Services (30%),
Public Admin & Safety (21%),
Electricity, Water & Utilities (17%)

Stakeholder Kit | Annual Cyber Threat Report 2025-26

13

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.

What we do

ASD's ACSC brings together capabilities to improve Australia's national cyber resilience across the Australian economy. Our services include:

- providing the Australian Cyber Security Hotline, 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 sharing intelligence with partners, including through the Cyber Threat Intelligence Sharing platform
- helping Australian organisations respond to cyber security incidents
- supporting collaboration between more than 149,500 Australian organisations and individuals through ASD's ACSC Cyber Security Partnership Program.

Cyber security is a shared responsibility, and collaboration remains essential to strengthening Australia's cyber resilience. ASD's ACSC works closely with government, industry, critical infrastructure operators, academia and the broader community to share information, strengthen preparedness and respond to emerging cyber threats.

If you need help with a cyber-security incident

Cyber security incidents, whether actual or potential, can be reported to ASD at cyber.gov.au/report or by calling 1300 CYBER1 (1300 292 371).

ASD is not a regulator or law enforcement body. Rather, we are an intelligence agency that can help strengthen your incident response with information that you won't find elsewhere, working directly with your incident responders and third-party providers.

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



Get in touch

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

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.



[@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)