Cybercrime in Australia
July to September 2019
Australian Cyber Security Centre
Contents

Executive summary ............................................................................................................................. 3
ReportCyber ...................................................................................................................................... 3
Strengthening cyber security and combating cybercrime ............................................................... 4
Cybercrime statistics ....................................................................................................................... 5
State and Territory breakdown: ReportCyber submissions, July-September 2019 ...................... 5
Reported financial losses ............................................................................................................... 5
Top five cybercrime types targeting Australians ............................................................................ 6
Protecting yourself from common cybercrimes .............................................................................. 8
Cyber security advice for individuals and businesses .................................................................... 9
Stay connected and up to date on cyber security ........................................................................... 9
How to report a cyber security incident, cybercrime, scam or a data breach ............................. 10
Executive summary

The Australian Signals Directorate’s Australian Cyber Security Centre (ACSC) leads government efforts to improve cyber security.

Australia continues to be targeted by cyber criminals who pose a threat to Australia’s national security and economic prosperity. Cyber criminals are increasingly well resourced, and target some of the most vulnerable members of our community, our families and our small businesses, emptying their bank accounts and stealing their personal information.

The ACSC monitors cyber threats across the globe 24 hours a day, seven days a week, 365 days a year. This enables us to rapidly alert Australians to cyber security issues, and deliver guidance on what to do in response.

We provide advice and information about how to protect customers and data, networks and systems, and businesses. When there is a cyber security incident, we provide clear and timely advice to individuals, small to medium enterprises, big business, and critical infrastructure operators.

Through initiatives such as Stay Smart Online, we provide advice to all Australians on how they can protect themselves from, and reduce the risk of, cyber security threats. We are committed to fostering our nation’s cyber security resilience, and making Australia the safest place to connect online.

ReportCyber

ReportCyber was introduced on 1 July 2019 as the successor to the Australian Cybercrime Online Reporting Network (ACORN). ReportCyber enables Australians and small to medium enterprises to report cyber issues and cybercrime.

After a report is submitted, it is automatically triaged and delivered to the appropriate police jurisdiction for possible investigation.

All reports made via ReportCyber contribute to the evolving cybercrime intelligence picture, enabling the ACSC and Australian law enforcement agencies to target online criminals and their networks.

The statistics used in this report are drawn from a range of sources available to the ACSC, including the ReportCyber platform, together with information shared by our partners and stakeholders. The data is current at time of writing, but ACSC has not independently verified the data from external sources.


Note: Not all cybercrime incidents are submitted to ReportCyber, as some individuals may report through other government or law enforcement channels.
Strengthening cyber security and combating cybercrime

The ACSC is currently delivering a number of initiatives to combat cyber threats and cybercrime to make Australia the safest place to connect online.

Our **Government Uplift** program provides expert cyber security advice to selected government organisations to improve their cyber security maturity. We will collaborate on uplift sprints with state and territories in 2020 to build their capacity.

**Stay Smart Online** educates the general public on how to protect themselves online. Our **Stay Smart Online Week** is an annual initiative to raise the cyber security awareness of all Australians, including small and medium businesses. This year it is focused on helping Australians reverse the threat of cybercrime by encouraging them to take simple steps to improve their online security.

We deliver the **ReportCyber** cybercrime reporting tool, enabling Australians to report cyber issues and cybercrimes, and assist police with their investigations and response to these reports.

Through our **Joint Cyber Security Centres**, we partner with international Computer Emergency Response Teams (CERTs), hundreds of large industry partners and critical infrastructure providers, and with local organisations and businesses.

Our **National Exercise Program** team works with government and industry to test and strengthen their cyber security arrangements. In the last 12 months, we conducted 25 cyber security exercises, across seven industry sectors and government agencies, and delivered 20 cyber security exercise training workshops to 198 participants.

In June 2019, the ACSC hosted a Capture-The-Flag exercise in Perth, with 30 top cyber security incident responders from 10 Association of Southeast Asian Nations (ASEAN) competing with their Australian counterparts to further strengthen regional cyber defences and cooperation.

Through our 24/7 hotline **1300 CYBER1**, we assist and respond to incidents affecting everyone, including government, industry, critical infrastructure and small to medium enterprises.
Cybercrime statistics

State and Territory breakdown: ReportCyber submissions, July-September 2019
In the first three months of operation, 13,672 reports were made to ReportCyber. This equates to an average of 148 reports per day, or one every 10 minutes. Of these 13,672 reports, 11,461 contained sufficient information to be referred to state and territory law enforcement agencies. The ACSC responded to the remaining 2,211 cases providing tailored cyber security advice to the reporter.

The distribution of reports referred to state and territory police is shown in Figure 1 below, with Victoria receiving the greatest proportion (3,023; 26.4%), followed by Queensland (2,997; 26.1%) and then New South Wales (2,930; 25.6%).

![Figure 1: Cybercrime reports to the ACSC, by jurisdictions (1 July to 30 September 2019)](image)

Reported financial losses
Individuals and small to medium enterprises lodging cybercrime reports on ReportCyber can indicate the amount of money they lost, for example through identity theft, online fraud or remote access scams.

Over the first quarter of reporting, the headline numbers in relation to reported financial loss were:

- Average financial loss per report $6,000
- More than $890,000 in reported losses each day
- Annual estimated losses to cybercrime of $328 million.
Top five cybercrime types targeting Australians

Between July and September 2019, the following five cybercrime types were most commonly reported to the ACSC:

1. **Identity theft**
   Identity theft has become one of the most common and costly crime types affecting Australians each year. Fuelled by lucrative dark web markets for stolen personal information, cyber criminals actively seek to compromise the identity of their victims, which they on-sell to other malicious actors or use to open bank accounts, apply for credit cards or purchase goods online.

   **Case Study**
   A 26 year old woman was looking for a room to rent and responded to an advertisement on a popular Australian website. The person who posted the ad informed the woman that they were currently overseas on holiday, but would return to Australia in a week. In order to secure the room, she was told to provide her full name and date of birth, together with copies of her identity documents. The woman sent through copies of her passport, birth certificate, driver’s licence and employment history. The advertiser then requested three months of rent in advance before they would provide a copy of the lease. It was at this point the woman suspected that she might be the victim of a scam. Subsequent investigation discovered that the scammer used the woman’s stolen personal information to apply for a credit card in her name and purchase over $10,000 worth of airline tickets, electronics and luxury items.

2. **Online fraud and shopping scams**
   Online fraud and shopping scams involve criminals obtaining financial advantage through deception, commonly by creating a webpage that imitates a well-known brand or shopping site, or tricking people into paying for goods or services that are never delivered.

   **Case Study**
   A 22 year old man received a text message from what he thought was his bank, indicating that an issue with his account had been detected. The text message contained a link taking him to a fake bank login page, where he provided his bank login and driver’s licence details. Within a matter of hours, cyber criminals had emptied his bank account, and the man lost over $20,000.

   **Case Study**
   A 35 year old man sought to purchase a new vehicle online. He found an online business advertising the exact model of car he was looking for, at a heavily discounted price. The online business claimed to offer delivery with a seven day return policy if the buyer wasn’t satisfied. The man paid $25,000 in advance for the car, and a further $4,000 for shipping. The car never arrived and the website disappeared.
3. **Bulk extortion**
Cyber criminals contact hundreds of victims a day by phone or email, and use social engineering to create a situation in which the victim is pressured into handing over money.

**Case Study**
A 38 year old woman received a phone call from a person claiming to be from the Australian Taxation Office. The scammer threatened the woman with an arrest warrant in relation to ‘unpaid taxes’, and claimed that in order to avoid a criminal record, she needed to transfer $8,000 into a bank account. The victim was provided bank account details, and not only paid the amount, but also provided the scammer with her Tax File Number, home address, and other sensitive personal information.

4. **Online romance scams**
Cyber criminals prey on vulnerable people, and online romance scams are a key example of this. Scammers will initiate online conversations through popular dating apps and spend months and sometimes years forming a ‘relationship’ with the victim. Once they have built a sense of trust, they start making requests for money, commonly for urgent medical issues or other unforeseen expenses.

**Case Study**
Through a popular dating app, a 73 year old widower met a woman online who claimed she was based in Dubai. The conversation quickly moved to email correspondence and over a period of 13 months they formed a relationship. The ‘woman’ convinced the victim to transfer significant sums of money to pay for medical treatments, property investments, holidays, and luxury goods. The victim even paid for her travel to Australia so they could meet in person. It was only when she cancelled at the last minute that the victim became suspicious. In the end, the victim lost over $430,000 in this online romance scam.

5. **Wire-fraud and business email compromise**
Cyber criminals exploit the trust between businesses and their suppliers to divert money into their accounts. This can occur through a business email compromise, where the scammer compromises the email account of the supplier and sends through a fraudulent invoice that contains the scammers’ bank details. Alternatively, the scammer registers a business domain name online that impersonates a legitimate company, or convinces the payroll or accounts area to change the bank details for an existing supplier.

**Case Study**
A logistics company in regional Australia received an email from one of their long-time suppliers advising that their bank account details had changed. It looked legitimate, as it came from the head of the supplier’s email account. A few days later, the company received an invoice that contained the correct purchase order, date of pickup and delivery numbers for services that had been provided. The new bank account details were also included. The company paid the invoice, worth over $200,000. After being contacted by the head of the supplier a few weeks later to enquire about their outstanding account, the company realised they had been scammed. The company contacted their bank but were unable to retrieve the funds.
Protecting yourself from common cybercrimes

Identity theft and online fraud are the two most commonly reported cybercrime categories, making up over 40% of reports received by the ACSC over the quarter.

You can help protect yourself against common cybercrimes by:

- Limiting the amount of personal information that you post online, including about your friends and family.
- Being suspicious of any unsolicited requests for personal information or urgent requests for money, whether by phone or email.
- Never giving someone remote access to your computer.
- Undertaking research for websites, such as review pages, before making payment for goods or services online.
- Remembering that Australian Government agencies will never request payment in the form of gift cards.

Australian Government agencies will never call you and request access to your computer, or threaten to arrest if you don’t make immediate payment of a debt.

If in doubt, just hang up the call; identify a publicly-available number for the department or agency that the caller has claimed to be from. Do not call back on any number provided by the caller or observed via caller ID.

You can also take the following practical steps to improve your personal cyber security and that of your organisation or business. Implementing this advice will help you stay one step ahead of cyber criminals:

**PASSWORDS.** Passwords are the lock on the front door to your online identity. Make sure you have strong passwords, a pass-phrase is even better, and never re-use the same password across multiple online accounts. Using a second layer of authentication, like an SMS code or a fingerprint, is also strongly encouraged.

**SCAM MESSAGES (PHISHING).** Think twice before clicking on web-links in emails, messages and social posts, particularly as phishing messages are getting increasingly sophisticated. If you receive an email or text message that asks for your personal details, your password or bank details, just delete it - whether you are at home or at work.

**UPDATES.** When you get a reminder to update your computer, phone or applications, you should do it promptly. Better still, set it to auto-update. It will help you protect your information and identity from cyber criminals that are always looking to exploit weaknesses in software.

**PUBLIC WI-FI.** Be wary when using public Wi-Fi. It is possible for others to see what you are doing over public Wi-Fi networks, so don’t do online banking or online shopping or send sensitive information.
Cyber security advice for individuals and businesses

The ACSC has produced a range of advice and publications that individuals and organisations can use to strengthen the cyber security of their devices, networks, and applications. This includes:

- Step-by-step guides for turning on two-factor authentication for various social networks (Twitter; Facebook; Apple ID; Gmail).
- Security configuration guides for popular mobile telephone devices (Apple iOS 12 devices; Samsung Galaxy S9 and S9+ devices).
- Technical advice on how to harden workstations and defend against malicious emails (Hardening Guides).

Other ACSC publications include:

**Travelling Overseas with Electronic Devices**

Targeting of electronic devices during overseas travel is a real and persistent threat, with corporate and personal laptops, phones, tablets and removable media (such as USB drives and SD cards) all known to have been compromised with malicious software.

*Read more: Travelling Overseas with Electronic Devices.*

**Essential Eight Maturity Model**

The ACSC has developed strategies to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies is known as the Essential Eight Maturity Model.

*Read more: Essential Eight Maturity Model.*

**Australian Small Business Cyber Security Guide**

The ACSC has developed guidance to help small Australian businesses protect themselves from the most common cyber security incidents.


These publications and more are available at [ACSC Publications](#).

**Stay connected and up to date on cyber security**

[Stay Smart Online](#) provides simple, easy to understand advice on how to protect yourself online, as well as up-to-date information on the latest online threats and how to respond.

Subscribe to the free Stay Smart Online [alert service](#) for the latest online threats and how they can be managed.

You can receive alerts by liking the [Stay Smart Online Facebook](#) page, or on Twitter @CyberGovAu.
How to report a cyber security incident, cybercrime, scam or a data breach

Report cybercrime to ReportCyber. The ACSC hosts the ReportCyber online reporting portal on behalf of Australian law enforcement agencies. This portal enables you to report your matter directly to specialist Australian police areas across the country.

Contact your bank. If you’ve sent money or personal banking details to a scammer, contact your bank immediately.

Recover your identity. If you think you’ve been the victim of identity theft, act quickly. For advice, contact iDcare on 1300 432 273, or use their free Cyber First Aid Kit to help you identify what you need to do.

Report it to the eSafety Commissioner. If you find offensive or illegal online content, or you are a victim of serious cyberbullying, report it to the eSafety Commissioner.

Report scams to Scamwatch. If you receive a suspicious email or text message, report it to Scamwatch.

For government, critical infrastructure and large businesses

Report to the Australian Cyber Security Centre

Email asd.assist@defence.gov.au or call the 24/7 Hotline for urgent advice or assistance on 1300 CYBER1 (1300 292 371).

Consider your obligations to the Office of the Australian Information Commissioner

If your organisation has had a breach of data that is likely to result in serious harm to any individuals whose personal information is involved in the breach, you may have legal obligations under the Notifiable Data Breaches Scheme. The Office of the Australian Information Commissioner runs the Notifiable Data Breaches Scheme.