Australian Government
Australian Signals Directorate

AFP
AUSTRALIAN FEDERAL POLICE

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

# ACSC Annual Cyber Threat Report
# **July 2019 to June 2020**

Australian Cyber Security Centre

cyber.gov.au

## Contents

## Executive Summary

The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) is the leading operational arm for the Australian Government responsible for strengthening the nation's cyber resilience, and for identifying, mitigating and responding to cyber threats against Australian interests. The ACSC also manages ReportCyber on behalf of federal, state and territory law enforcement agencies, providing a single online portal for individuals and businesses to report cybercrime.

The Australian Federal Police (AFP) investigates cybercrimes against the Commonwealth Government, critical infrastructure and systems of national significance or those with impact on the whole of the Australian economy. The AFP works collaboratively with domestic and international partners to enhance cyber capabilities and make Australia a costly, hostile environment for cybercrime.

The Australian Criminal Intelligence Commission (ACIC) is Australia's national criminal intelligence agency. Its role is to discover and prioritise cybercrime threats to Australia, understand the criminal networks behind them and support the Australian Government's response by working closely with law enforcement, intelligence and industry security partners in Australia and internationally. The ACIC develops comprehensive intelligence to understand the cybercrime environment, its evolution, and serious and organised cybercriminal activities and share this with our partners.

On average, the ACSC assists six entities to respond to cyber security incidents each day. At any one time, the ACSC is managing dozens of incidents simultaneously. Some incidents can take weeks or months to resolve depending on their complexity.

To manage the very broad range of cyber incidents reported, the ACSC uses a Cyber Incident Categorisation Matrix to triage and prioritise responses and mitigations required for each cyber incident. The Matrix helps the ACSC categorise the severity of the incident and allocate resources accordingly through assessing an incidents significance and impact.

The ACSC is a participant of the National Cyber Security Committee (NCSC), which provides strategic oversight and coordination of response efforts among Commonwealth, state and territory governments in the event of a national cyber incident. The NCSC's role in responding to a national cyber incident includes facilitating the exchange of threat intelligence and solutions to enhance each jurisdiction's situational awareness and response activities and to oversee the development of nationally consistent public information. The NCSC is also responsible for setting the Cyber Incident Management Arrangements (CIMA) level, which provides Australian governments with guidance on how they will collaborate in response to, and reduce the harm associated with, national cyber incidents.

The ACSC and our law enforcement partners ACIC and AFP, have developed this inaugural report to provide important information about emerging cyber security and cybercrime threats impacting different sectors of the Australian economy. It includes best-practice mitigation advice for implementation by individuals and organisations, so they can reduce the likelihood and impact of malicious cyber activity.

This report outlines key cyber threats and statistics over the period 1 July 2019 to 30 June 2020. Over this period, the ACSC responded to 2,266 cyber security incidents and received 59,806 cybercrime reports at an average of 164 cybercrime reports per day, or one report every 10 minutes.

## Key cyber threats

Malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. Phishing and spearphishing remain the most common methods used by cyber adversaries to harvest personal information or user credentials to gain access to networks, or to distribute malicious content. Over the past 12 months the ACSC has observed real-world impacts of ransomware incidents, which have typically originated from a user executing a file received as part of a spearphishing campaign.

Ransomware has become one of the most significant threats given the potential impact on the operations of businesses and governments. Cybercriminals often illicitly obtain user logins and credentials through spearphishing, before utilising remote desktop protocol (RDP) services to deploy ransomware on their targets. Recovering from ransomware is almost impossible without comprehensive backups.

While our cyber adversaries are becoming more adept, the likelihood and severity of cyber-attacks is also increasing due to our growing dependence on new information technology platforms and interconnected devices and systems. The 5G mobile network will underpin Australia's transition to a more digital economy, and Internet of Things (IoT) devices will enable greater information flows and efficiencies than ever before.

The 5G network and IoT devices have the potential to be revolutionary, but they require new thinking about how best to adopt them securely. Insecure or misconfigured systems make it very easy for hackers looking to compromise networks, cause harm and steal information. Specifically, the increased use of consumer IoT devices such as internet-enabled home assistants, TVs, fridges, baby monitors and home security systems will create more vulnerabilities in networks.

Australians need to be mindful that cyber adversaries are constantly looking for vulnerabilities and weaknesses in systems and networks. The ACSC continues to identify many products and services being adopted and implemented by organisations that lack 'secure by design' principles. Applying the fundamentals of good cyber security as individuals, business owners and government agencies is vitally important and in many ways Australians are not necessarily learning from past experience.

The ACSC responds to hundreds of cyber security incidents each year. Many of these could have been avoided or substantially mitigated by good cyber security practices. Implementing ASD's Essential Eight security controls will substantially reduce the risk of compromise, and help to prevent the most common tactics, techniques and procedures (TTPs) used by malicious cyber adversaries.

Equally, many of the methods used by cybercriminals to steal personal and financial information can be easily mitigated through measures such as not responding to unsolicited emails and text messages, implementing multi-factor authentication and never providing another party with remote access to your computer. It is critically important that individuals and businesses understand the cyber threat and are taking active steps to mitigate the risks.

## Cybercrime threat in Australia

Cybercrime is one of the most pervasive threats facing Australia, and the most significant threat in terms of overall volume and impact to individuals and businesses. The Australian Competition and Consumer Commission's (ACCC) Targeting Scams 2019 report, identified Australians lost over $634 million to scams in 2019. While the true cost of cybercrime to the Australian economy is difficult to

quantify, industry estimates have previously placed cyber security incidents as high as $29 billion annually[1].

Cybercriminals follow the money. Australia's relative wealth, high levels of online connectivity and increasing delivery of services through online channels make it very attractive and profitable for cybercrime adversaries. Of particular concern are transnational cybercrime syndicates and their affiliates, who develop, share, sell and use sophisticated tools and techniques. There are lucrative underground marketplaces offering cybercrime-as-a-service (CaaS), or access to high-end hacking tools that were once only available to nation states. These marketplaces also offer less technical but equally valuable cybercrime enablers including personal information and other sensitive data such as compromised user credentials.

As a consequence, illicit tools, services and data can be purchased and used with minimal technical expertise to generate alternative income streams, launder the proceeds of cybercrimes and traditional crimes, or undertake network intrusions for non-financial purposes.

[1] https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/

## Cyber security incidents

Over the reporting period, the Australian Cyber Security Centre (ACSC) responded to 2,266 cyber security incidents (Figure 1). During this period, there were two notable spikes in October 2019 and April 2020. The spike in October 2019 was associated with a widespread Emotet malware campaign (Case Study 1). During April 2020, the ACSC was operating at an elevated CIMA level in response to COVID-19 themed cybercrime. Throughout the pandemic, there was an increase in reported spearphishing campaigns and an increase of COVID-19 themed malicious cyber activity.

Between 10 and 26 March 2020, the ACSC received over 45 pandemic themed cybercrime and cyber security incident reports, with the Australian Competition and Consumer Commission's (ACCC) Scamwatch receiving over 100 reports of COVID-19 themed scams.

During March 2020, cybercriminals quickly adapted their phishing methods to take advantage of the COVID-19 pandemic. To help Australians identify threats, the ACSC released two updates about COVID-19 malicious cyber activity:

- https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity
- https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020

The ACSC categorises each incident we respond to on a scale of Category 1, the most severe, to Category 6, the least severe. Of the 2,266 incidents, the largest proportion were assessed as being 'Category 5 – Moderate Incident' (36.5%, n=828) followed by 'Category 4 – Substantial Incident' (33.3%, n=754). These categories broadly represented malicious cyber activity such as targeted reconnaissance, phishing emails and malicious software impacting larger organisations, key supply chain and Commonwealth and state government entities.

**Figure 1: Cyber security incidents, by month (1 July 2019 to 30 June 2020)**

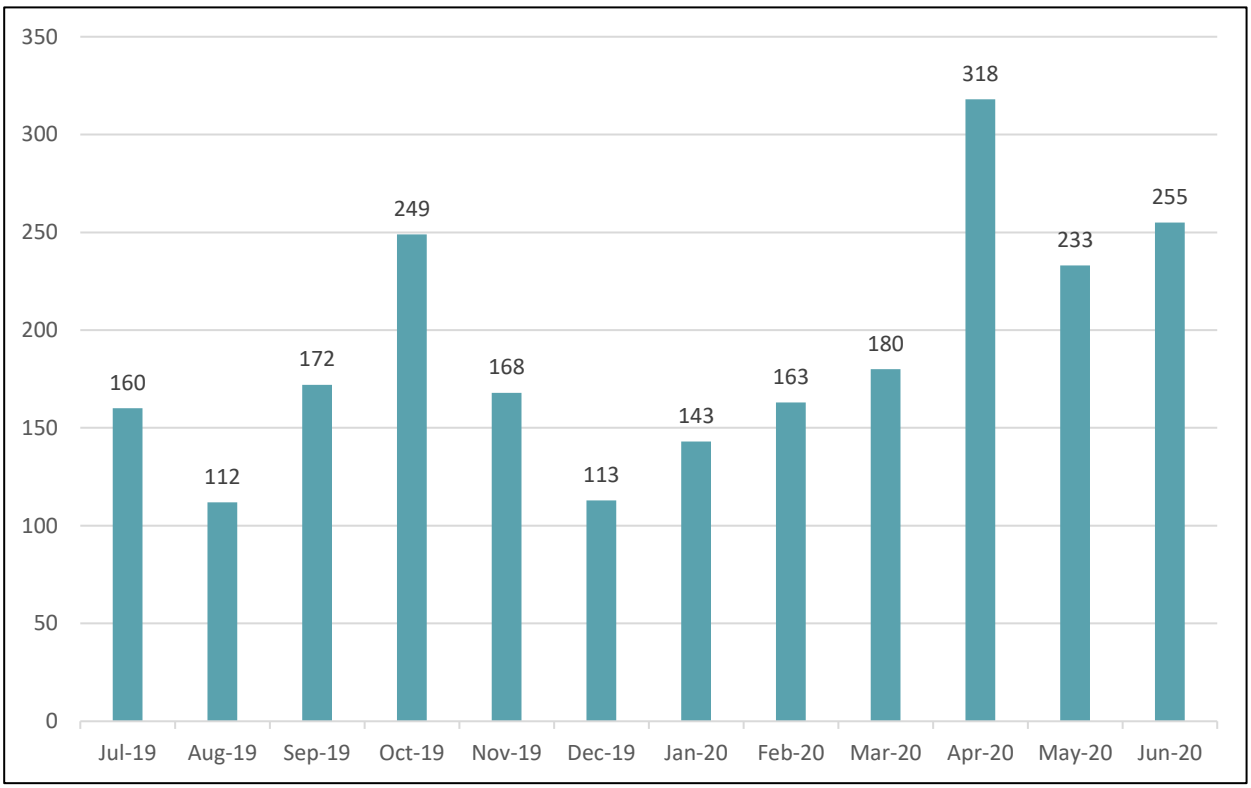
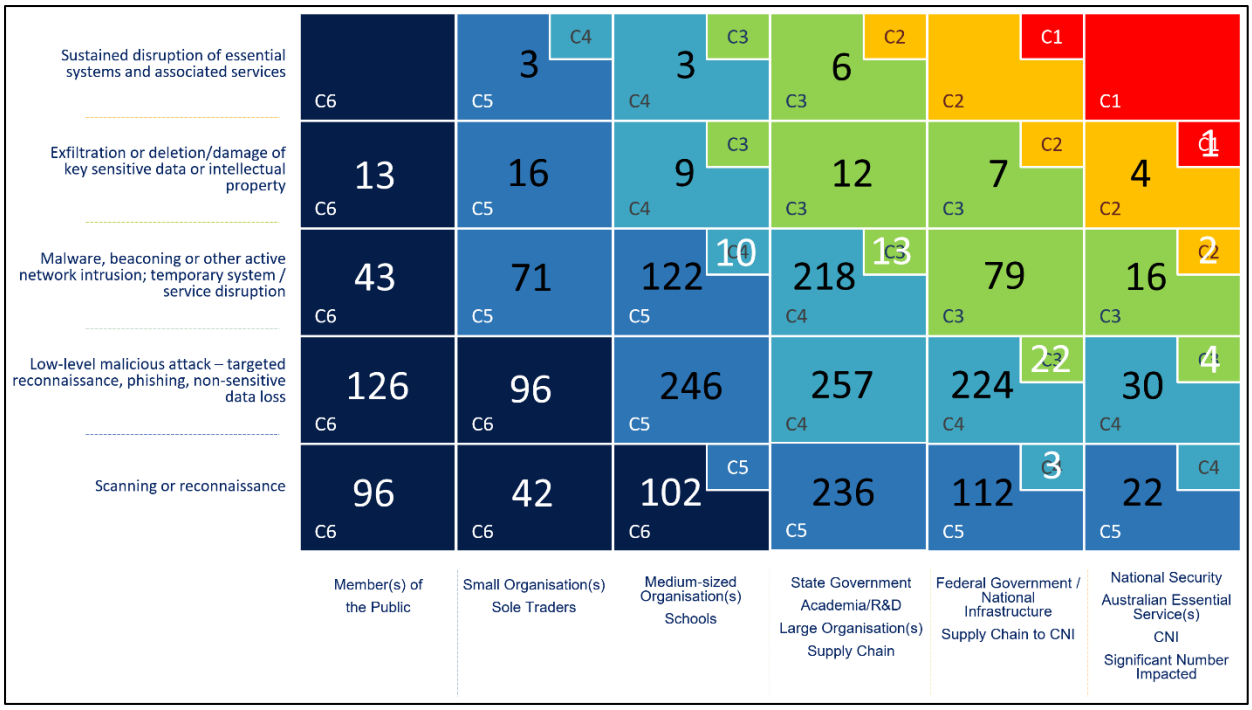
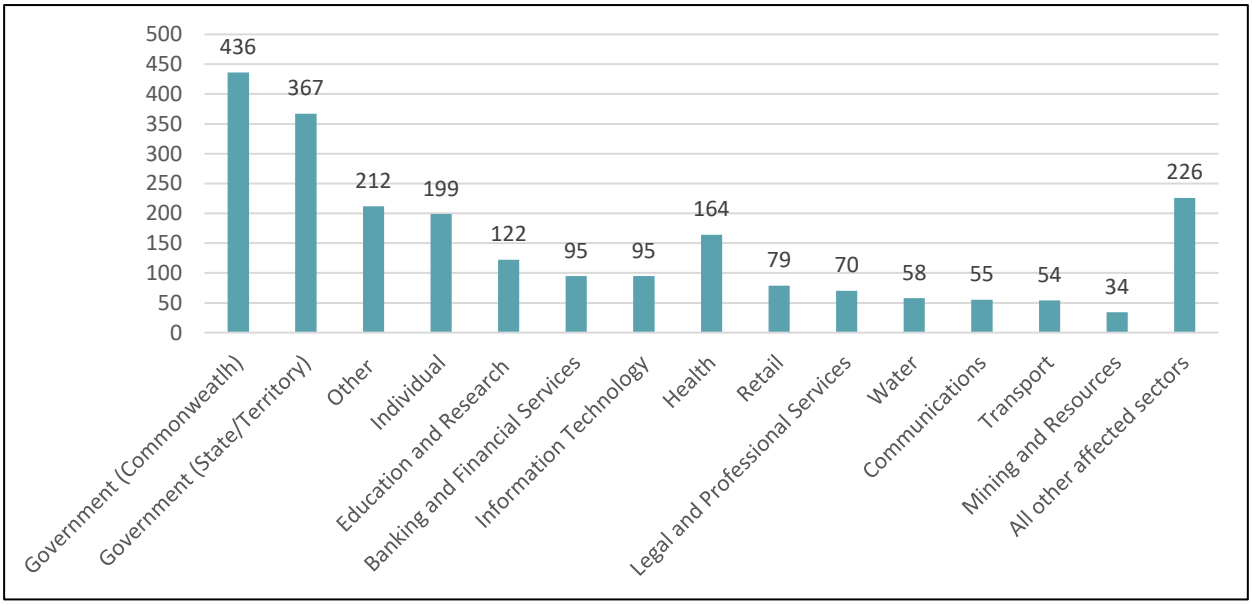


**Figure 2: Cyber security incidents, by categorisation (1 July 2019 to 30 June 2020)**




## Sectors Affected

**Figure 3: Cyber security incidents, by affected sector (1 July 2019 to 30 June 2020)**

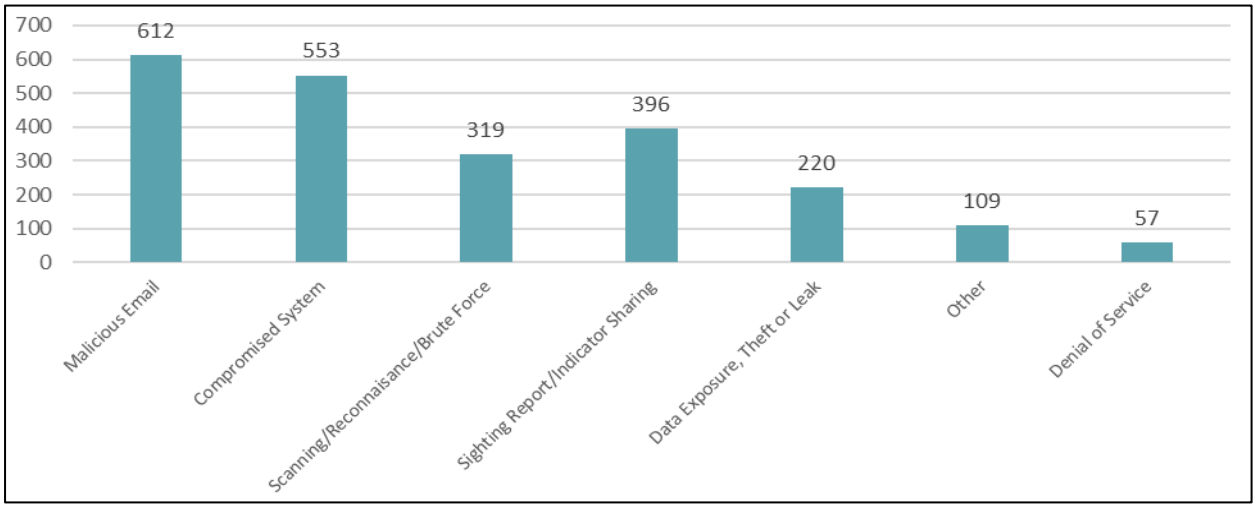



As shown in Figure 3, a large proportion of incidents are reported by Commonwealth, state and territory governments (35.4%, n=803). The comparatively higher volume of reports from Commonwealth, State and Territory Governments is due to their close working relationship with the ACSC and their willingness to report incidents. Australia's critical infrastructure sectors including electricity, water, health, communications and education represented around 35% of the incidents responded to by the ACSC.

## Types of Incidents

The most common type of cyber security incident was 'malicious email' (27%, n=612). Phishing and spearphishing emails have consistently remained the most common cyber security incidents reported to the ACSC. Adversaries continue to use phishing as a means of obtaining initial access into a network including through compromising user credentials or installing malware after a recipient clicks on a malicious link or attachment. The second most common incident was a 'compromised system', (24.4%, n=552). This category relates to incidents where an adversary has accessed or modified a network, account, database or website without authorisation.

**Figure 4: Cyber security incidents, by type (1 July 2019 to 30 June 2020)**




Although malicious emails are currently, and will likely continue to be, the most common type of incident reported to the ACSC, it is important to ensure security is applied throughout a network (defence-in-depth) and across personal devices.

## National Cyber Security Incident

On 19 June 2020, the Prime Minister of Australia publicly announced the Australian Government is aware of and alert to the threat of cyber-attacks. The ACSC identified this threat as a Category 1 cyber incident, as it involved the sustained targeting of Australian governments and companies by a sophisticated state-based actor. The ACSC published an Advisory titled 'Advisory 2020-008: Copy-paste compromises' which was derived from the adversary's heavy use of tools copied almost identically from open source.

The Advisory details the tactics, techniques and procedures (TTPs) identified during the ACSC's investigation of the cyber campaign. The Advisory also identifies, based on these TTPs, that implementation of the following two mitigations would have greatly reduced the risk of compromise:

- Prompt patching of internet-facing software, operating systems and devices
- Use of multi-factor authentication across all remote access services

The ACSC responds to hundreds of cyber security incidents each year that have been the result of very poor cyber security practices. To further protect against cyber security intrusions, the ACSC recommends implementing ASD's Essential Eight security controls will substantially reduce the risk of compromise and help to prevent the most common TTPs used by malicious cyber adversaries.

**Case Study 1: Widespread exploitation of vulnerable systems via Emotet malware**

The Emotet malware campaign, first identified in 2014 as a banking Trojan disseminated via email, targets sensitive personal and financial information. It continues to evolve, enabling the download of malicious code such as ransomware onto infected devices. In October 2019, the ACSC identified that adversaries were using Emotet in a widespread campaign to target hundreds of vulnerable systems across Australia. At its peak, the ACSC detected over **4,500** malicious emails per day including nearly **50** variations of malicious emails used to infect systems. The campaign resulted in the networks and systems of at least **22** Australian organisations being infected.

In response, the National Cyber Security Committee (NCSC) activated Australia's Cyber Incident Management Arrangements (CIMA) to 'Level 3 – Alert'. These arrangements empowered cooperation between the ACSC and State and Territory governments to undertake increased monitoring, intelligence sharing and widespread distribution of mitigation advice to vulnerable organisations, emphasising the need to implement urgent protections.

In November 2019 the NCSC successfully mitigated the threat posed by Emotet during this campaign through coordinating the development, collection and sharing of indicators and tradecraft, as well as public messaging by Australian Governments to ensure organisations took appropriate action to mitigate the threats. As a result, the CIMA was returned to 'Level 5 – Normal Conditions'.

## ReportCyber

The ACSC's online reporting tool ReportCyber assists members of the community to report different types of cybercrime. It also provides a reference number that victims can present to organisations (such as telecommunications carriers, banks, and credit reporting bodies) as part of recovery efforts.

ReportCyber is available at https://www.cyber.gov.au/report

Reporting of incidents helps the Australian Government better understand the online threats impacting our community. The reported information is referred to federal, state or regulatory agencies within the relevant jurisdiction for investigation and in some cases, police action.

On 30 June 2020, the Government announced a $1.35 billion Cyber Enhanced Situational Awareness and Response (CESAR) package to boost protection and cyber resilience for all Australians. Under the Government's CESAR package, the ACSC will continue working with AFP and ACIC to enhance capabilities to prevent and disrupt cybercrime targeting Australia. CESAR will also provide funding towards enhancing ReportCyber, improving the detection of widespread cybercrime campaigns and enabling the effective sharing of threat intelligence and cyber security advice to all Australians.

### Cybercrime Categories

ReportCyber captures the following categories of incidents:

- **Cyber abuse** – someone is bullying, harassing or stalking you online.
- **Online Image Abuse** – someone has shared online, or is threatening to share online, intimate images or videos of you.
- **Online shopping fraud** or **romance fraud** - you have been deceived into sending money or goods to someone online.
- **Identity theft** - someone has used your personal or business identity information and accessed your online accounts.

- **Email Compromise** - you received an email containing fraudulent information that deceived you and led you to send money.
- **Internet fraud** - you clicked on a phishing link or gave someone remote access to a computer or device, and money may have been taken from your account(s) (Case Study 2).
- **Ransomware or malware** - your system or devices have been compromised and someone may be demanding money.

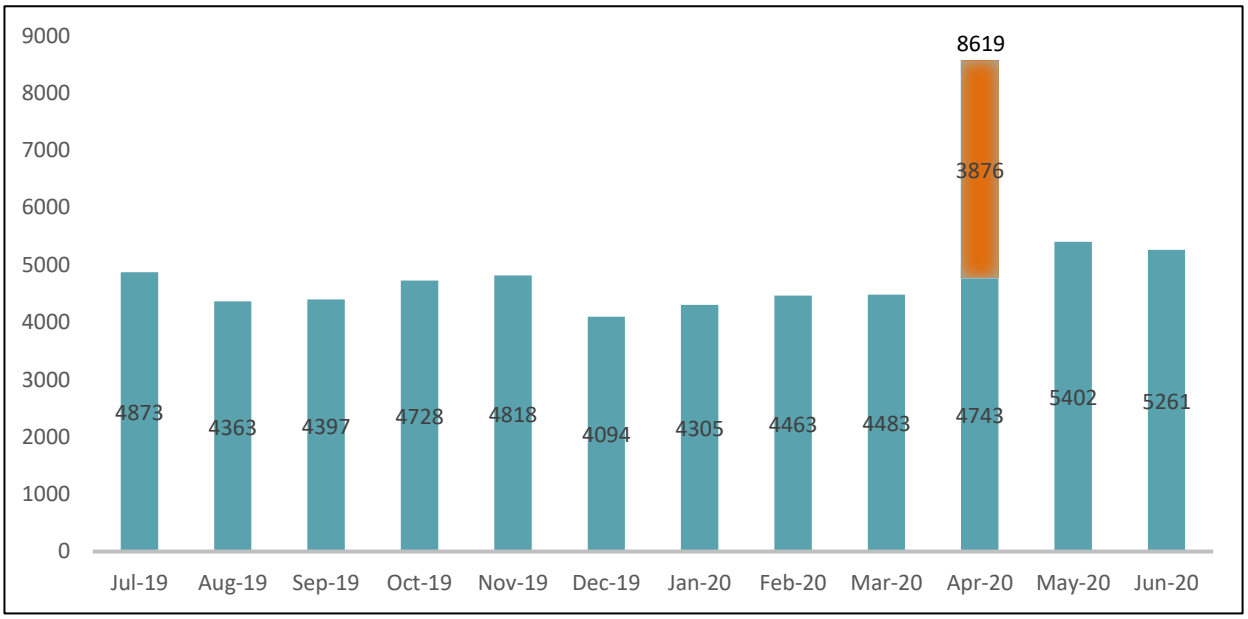
## Cybercrime Statistics

Since the launch of ReportCyber on 1 July 2019, there has been 59,806 cybercrime reports at an average of 164 per day or approximately one report every 10 minutes (Figure 5). This is a decrease from the previous year, with equivalent reporting of 64,567 between the period 1 July 2018 to 30 June 2019.

The most common category of cybercrime reported is 'fraud' (39.86%, n=23,841) which relates to criminals obtaining benefit through deception, such as investment, shopping or romance scams. Identity-related crimes incorporating the theft and misuse of personal information was the second most common category (32.4%, n=19,467) followed by 'cyber abuse' (22.15%, n=13,309) (Figure 6).

While the numbers show that fraud is the most common category, the ACSC assesses ransomware as the highest threat. This assessment is based on the fact that ransomware requires minimal technical expertise, is low cost and can result in significant impact to an organisation, potentially crippling core business functions. Further details on ransomware threats and mitigation techniques can be found under Threats – Ransomware (p.12).

**Figure 5: Cybercrime reports, by month (1 July 2019 to 30 June 2020)**




**Note:** Cybercrime within Australia is under-reported, as not all cybercrime incidents in Australia are submitted to ReportCyber. The ACSC urges victims of cybercrime to report all incidents to ReportCyber.

The notable spike in April 2020 relates to a bulk extortion campaign, resulting in 3,876 cybercrime reports, with 45% of cybercrime reports in April related to this one campaign. This was not related to COVID-19, but one or more adversaries had emailed thousands of Australians and threatened to release sensitive information to the recipient's friends and family unless they paid an amount in untraceable

crypto currency. The ACSC issued an alert on this campaign through cyber.gov.au, the StaySmartOnline service and social media channels, together with the ReportCyber portal.

**Figure 6: Cybercrime reports, by category (1 July 2019 to 30 June 2020)**

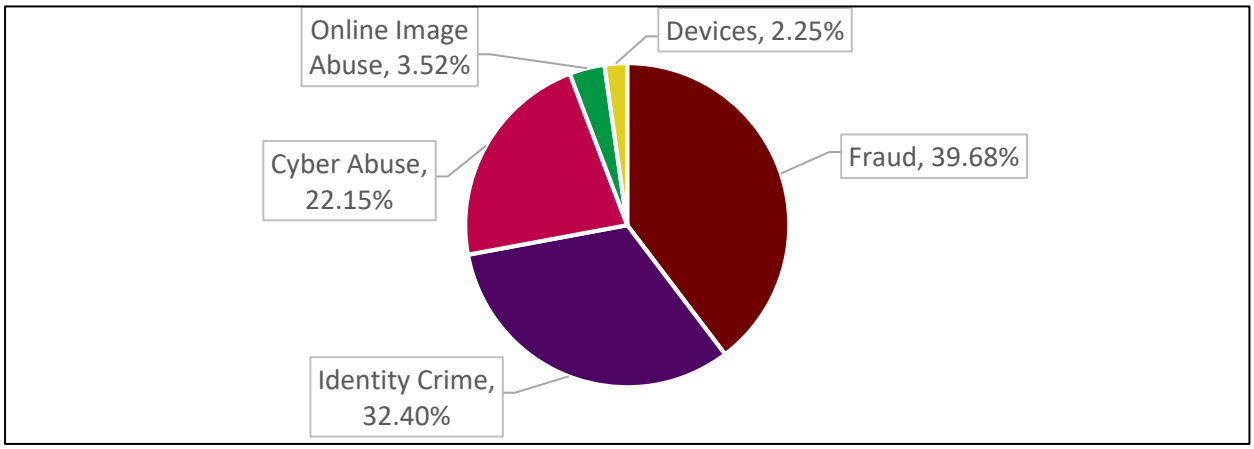
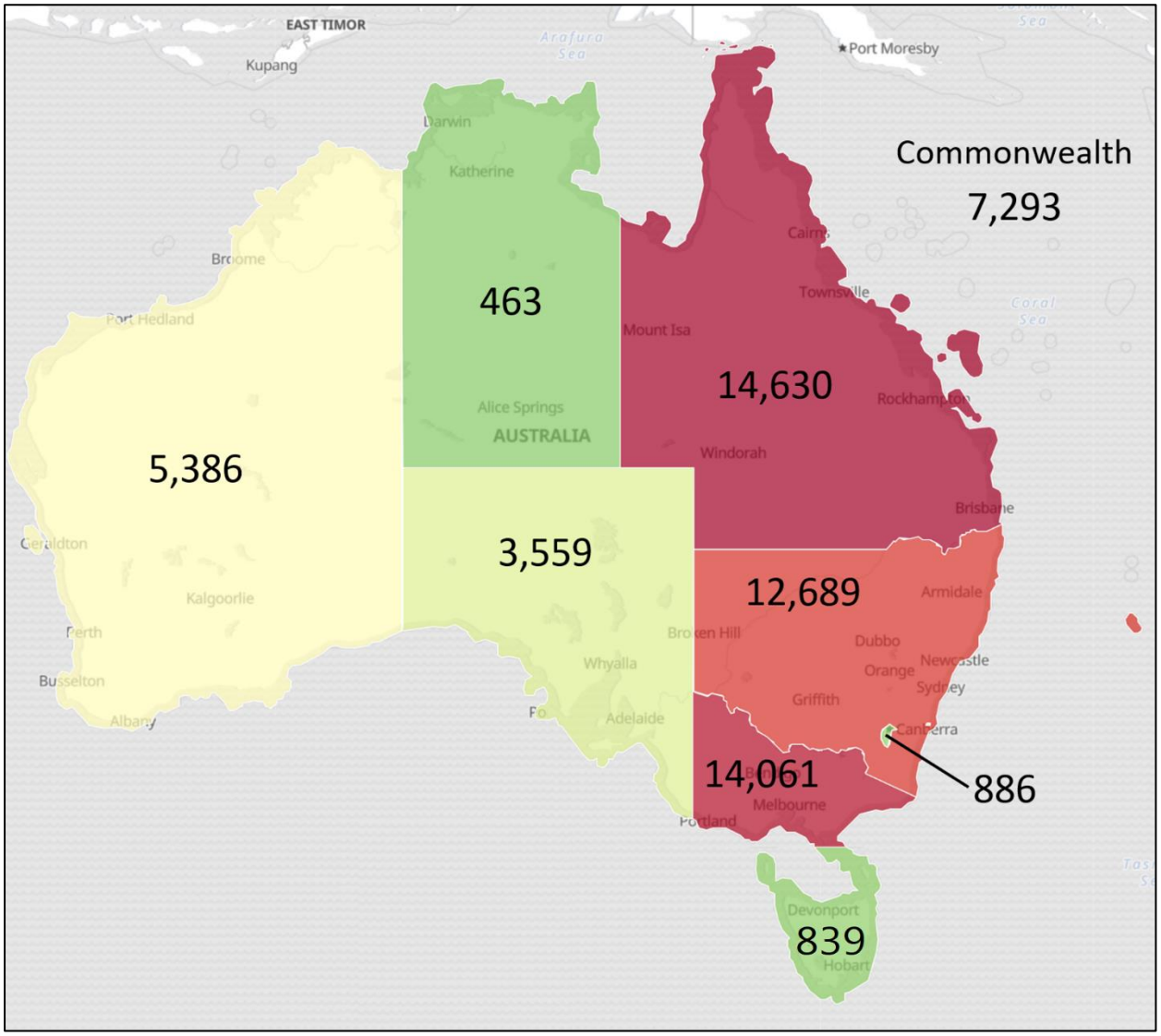



**Figure 7: Cybercrime reports, by jurisdiction (1 July 2019 to 30 June 2020)**



## Threats

### Ransomware

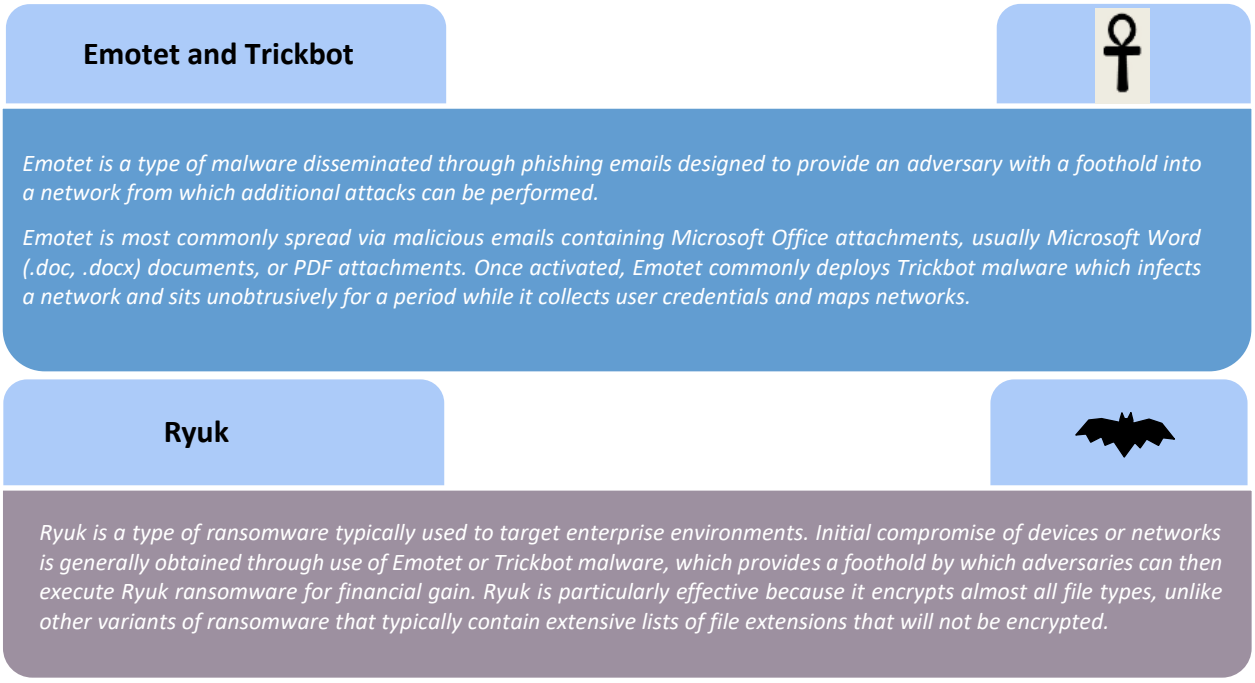
There are numerous adversaries offering various cybercrime techniques and tools through darkweb marketplaces. This is referred to as cybercrime-as-a-service, enabling traditional organised crime groups to quickly and easily begin generating alternative income streams. Over the last 12 months, ransomware has become one of the most significant cyber threats facing the operation of private sector organisations. This is due to the low-cost and minimal technical expertise required, with significant impact to core business functions, resulting in organisation paying large ransoms.

Ransomware can cripple organisations that rely on computer systems to function, by encrypting all connected electronic devices, folders and files and rendering systems inaccessible. Cybercriminals will then demand a ransom in return for the decryption keys, often in the form of untraceable crypto currencies such as Bitcoin. In a number of recent incidents the ACSC has observed cybercriminals tailoring their ransom demands based on a victim's financial standing.

While there are numerous different malware and ransomware variants, the ACSC has responded to several incidents affecting organisations in Australia where an adversary has used a combination of Emotet and Trickbot as the initial access into a network and then deployed Ryuk ransomware.

Figure 8 provides a further breakdown and description of how each of these malicious pieces of software work.

**Figure 8: A description of Emotet and Trickbot, and Ryuk**




The ACSC has observed cybercriminals exfiltrating data prior to ransomware being deployed as a tactic to increase the likelihood that their victims will pay the ransom and increase profit from the sale and/or re-use of compromised information.

Though ransom demands may exceed millions of dollars, affected organisations have reported experiencing other substantial financial impacts and data losses associated with recovering from a

ransomware incident, regardless of whether they paid the ransom. These additional costs include rebuilding and hardening networks, implementing additional IT security controls, time and money spent on data recovery and absorbing the impact of lost productivity and revenue incurred while offline.

Organisations that make regular backups offline and secure important and sensitive information effectively remove the need to pay ransom demands. Paying a ransom does not guarantee decryption of data. Open source reporting indicates several instances where an entity paid the ransom but the keys to decrypt the data were not provided. The ACSC has also seen cases where the ransom was paid, the decryption keys were provided, but the adversary came back a few months later and deployed ransomware again. The likelihood that an Australian organisations will be retargeted increases with every successful ransom payment.

Victims report paying ransoms when they are unable to recover, restore or reassemble encrypted data via other means. Isolating regular data backups from the main network and the internet can help to protect copies of vital information, enabling quick and easy restoration of data without paying the ransom.

The ACSC has observed sophisticated cybercriminals conducting significant victim research on networks they have compromised prior to deploying ransomware. Cybercriminals will locate and target backups which have not been isolated from the network or internet, maximising the impact of their ransomware and increasing the likelihood of victims paying ransoms to them.

The ACSC strongly advises against paying ransom demands as this only serves to fuel the market and there is no guarantee the adversary will provide the decryption keys. It is generally much easier and safer to restore data from a backup than attempting to decrypt ransomware affected data.

### Phishing and Spearphishing campaigns

Phishing is a method of stealing confidential information by sending fraudulent messages to a victim. It remains the most prevalent method used by cyber adversaries to target Australian organisations. Phishing campaigns can be sent via email, SMS, social media, instant messenger or phone call. They can look extremely sophisticated and convincing, often replicating legitimate messages from reputable senders.

The ACSC has observed numerous phishing emails that feature official logos and branding, together with the same font and layout as the organisation they pretend to come from. Phishing emails typically include a ‘call to action’ tricking recipients into giving out sensitive personal information, including passwords and bank details.

Unlike phishing campaigns which are generic and commonly sent out in thousands, spearphishing is a more advanced and targeted method of phishing. Spearphishing campaigns are typically well-crafted and designed to target a particular set of recipients.

In developing a spearphishing email, adversaries use tactics such as social engineering to research, identify and target high-value individuals within particular organisations. This can include using information found via professional and personal social media networks, and publicly available industry information such as annual reports, shareholder updates and media releases. The more refined and genuine a spearphishing email appears, the more likely users are to be deceived into opening malicious links and attached files.

**Case Study 2: Woman faces $30,000 in fraudulent charges following bank-themed phishing email**

In September 2019 a 63 year old woman received an email appearing to be from her bank, requesting her assistance to investigate suspicious transactions on her savings account. After clicking on a web-link contained in the email, she was directed to an imitation of her online banking website. The woman logged in with her details and provided her full name, date of birth, mobile number, bank account, credit card and Medicare details.

After a few hours the woman was concerned about the request and telephoned her bank who advised this was a scam and quickly put blocks on her account. However, the woman later discovered the scammers had opened three credit cards in her name and spent $30,000 on multiple luxury items, including watches and handbags. With assistance from her bank and law enforcement, the woman was able to dispute the charges, however it took several days and hours of telephone calls to replace bank cards and update all her passwords and account details.

### Business email compromise

Business email compromise (BEC) is a common attack vector available within CaaS markets. BEC targets businesses and their employees for financial gain, by using socially engineered messages or compromised email accounts. This methodology involves fraudulently requesting payment transfers or changing account details on invoices or payrolls, to redirect funds into bank accounts controlled by the cybercriminal.

The ACSC and our law enforcement partners have seen a significant increase in BEC over the last 12 months and expect these incidents will continue to increase in prevalence.

**Case Study 3: Consulting firm is tricked into sending $240,000 to fraudster in Malaysia**

In September 2019 a 36-year-old woman who works in the finance section of an Australian consulting firm received an email from her boss requesting urgent payment of an invoice to a supplier in Malaysia. At the time her boss was on a work-related trip to Malaysia and the email was sent from his personal email account which he had used on previous work trips. The woman quickly organised payment of the AUD$240,000 invoice from the company account and replied to the email, providing a screenshot of the transaction. When her boss returned a few days later, he discovered his personal email account had been compromised and the funds had been paid into a fraudster's account. The matter was referred to police for assessment.

### Exploitation of vulnerabilities

Cyber adversaries are constantly scanning network services to build a list of future potential soft targets for exploitation. They look for misconfigured devices, open ports and databases and vulnerabilities in hardware appliances or unpatched software. As soon as a vulnerability in a widely used software application is identified, adversaries can quickly deploy exploits on to the networks they already know are susceptible to attack.

The exploitation of both the Citrix and Telerik vulnerabilities were some of the most sophisticated tradecraft observed being used by adversaries between 2019 and 2020.

### Case Study 4: Adversaries targeting Citrix Vulnerability CVE-2019-19781

On 17 December 2019, Citrix disclosed the existence of a vulnerability in Citrix Application Delivery Controller (ADC) and gateway devices known as CVE-2019-19781. If exploited successfully, this vulnerability would allow an adversary to execute code, gain unauthorised access to resources and deploy malware on an affected Citrix device.

The ACSC released information on 25 December 2019 and 30 January 2020 about the Citrix vulnerability to alert organisations to advise on how to detect and mitigate compromises resulting from the Citrix vulnerability.

On 10 January 2020, a technical proof-of-concept script was released publicly outlining how the Citrix vulnerability could potentially be exploited. From this date the ACSC observed adversaries scanning and attempting to exploit the Citrix vulnerability.

Although Citrix did not have software patches available upon vulnerability disclosure, they provided an interim protection measure while they developed a patch. Citrix released software patches for this vulnerability from 19 to 24 January 2020.

The ACSC observed actors using this vulnerability to compromise networks, to then deploy ransomware, cryptominers and other malicious software.

### Case Study 5: Adversaries targeting Telerik Vulnerability CVE-2019-18935

Telerik offers a variety of products that provide functionality to web pages. In some cases, Telerik products may be installed as a third-party component included in web applications and therefore, may be invisible to the user. Successful compromise of Telerik software has been associated with the deployment of malicious tools such as webshells by adversaries. These webshells allow for unauthorised data access, use and disclosure.

On 11 December 2019, a security vulnerability was published that affects some Telerik products, known as CVE-2019-18935. The ACSC became aware of sophisticated adversaries scanning for unpatched Telerik versions allowing exploitation of this latest vulnerability. Exploitation would allow an adversary to run code on a compromised server without authorisation.

On 3 March 2020, the ACSC released a technical advisory to warn users of the vulnerability and the increased risk of exploitation, including instructions on how to detect and mitigate compromise.

## Cyber security advice for individuals

Cybercriminals and adversaries most commonly seek to steal the personal and financial information of individuals to generate profit. They do this directly by tricking you into providing information through scams or online frauds, or stealing information indirectly via malicious software they put on your devices. You can help protect yourself against the most common cybercrimes by:

- Limiting the amount of personal information including about your friends and family, being shared online or sent to other people and organisations that you don't know. Always pause and ask yourself, do they really need my date of birth or driver licence details?
- Being suspicious of any unsolicited requests for personal information or urgent requests for money, whether by phone or email. Before opening an email, clicking on a link, or opening an attachment, consider who is sending it to you and what they are asking you to do.
- Never giving someone remote access to your computer.
- Undertaking research for websites, such as review pages, before making payment for goods or services online. Remember, if it seems too good to be true, it almost certainly is!
- Turning on two-factor authentication (2FA) for all essential services such as email, bank and social media accounts, as this way of 'double-checking' identity is much stronger than using a password. 2FA requires you to provide two forms of authentication before you - or anyone pretending to be you - can access your account.

Australian Government agencies will **never** call you and request access to your computer, or threaten to arrest you if you don't make immediate payment of a debt. If in doubt, just hang up the call, and identify a publicly available number for the claimed department or agency. **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 cybercriminals:

**PASSPHRASES.** You should consider replacing your old passwords with a much stronger passphrase, which represents the lock on the front door of your online security. Passphrases are much harder to crack than a password. Never re-use the same one across multiple online accounts. Using a second layer of authentication (e.g. through 2FA) 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 the software on 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 cybercriminals who 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.

## Stay connected and up to date on cyber security

For more information about how to secure your online information, read our *Easy Steps Guide*:

- https://www.cyber.gov.au/advice/EasyStepsGuide

The ACSC's *Stay Smart Online* program also 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.

## Cyber security advice for businesses

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

- *Small Business Cyber Security Guide* https://www.cyber.gov.au/publications/small-business-cyber-security-guide
- *Strategies to Mitigate Cyber Security Incidents*, including the Essential Eight, which provides prioritised mitigation strategies to help cyber security professionals in all organisations mitigate cyber security incidents caused by various cyber threats. https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents
- *Security Configuration Guides* for popular mobile phone 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)

Staff will always be an organisation's greatest asset and greatest risk – especially when it comes to cyber security. One wrong click by a staff member, whether intentional or not, can destroy networks.

Improving staff awareness of cyber security issues and threats, including the risk environment for your organisation, needs to be a priority for all businesses, and there are some easy and effective ways to do it. Review the following guide on Improving Staff Awareness.

**Want more information? These publications and more are available at** ACSC Publications

## How to report a cyber security incident, cybercrime, scam or a data breach

an **individual**

**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.

a **small** or **medium business**

**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

from **government**

**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.

in **big business** or **infrastructure**