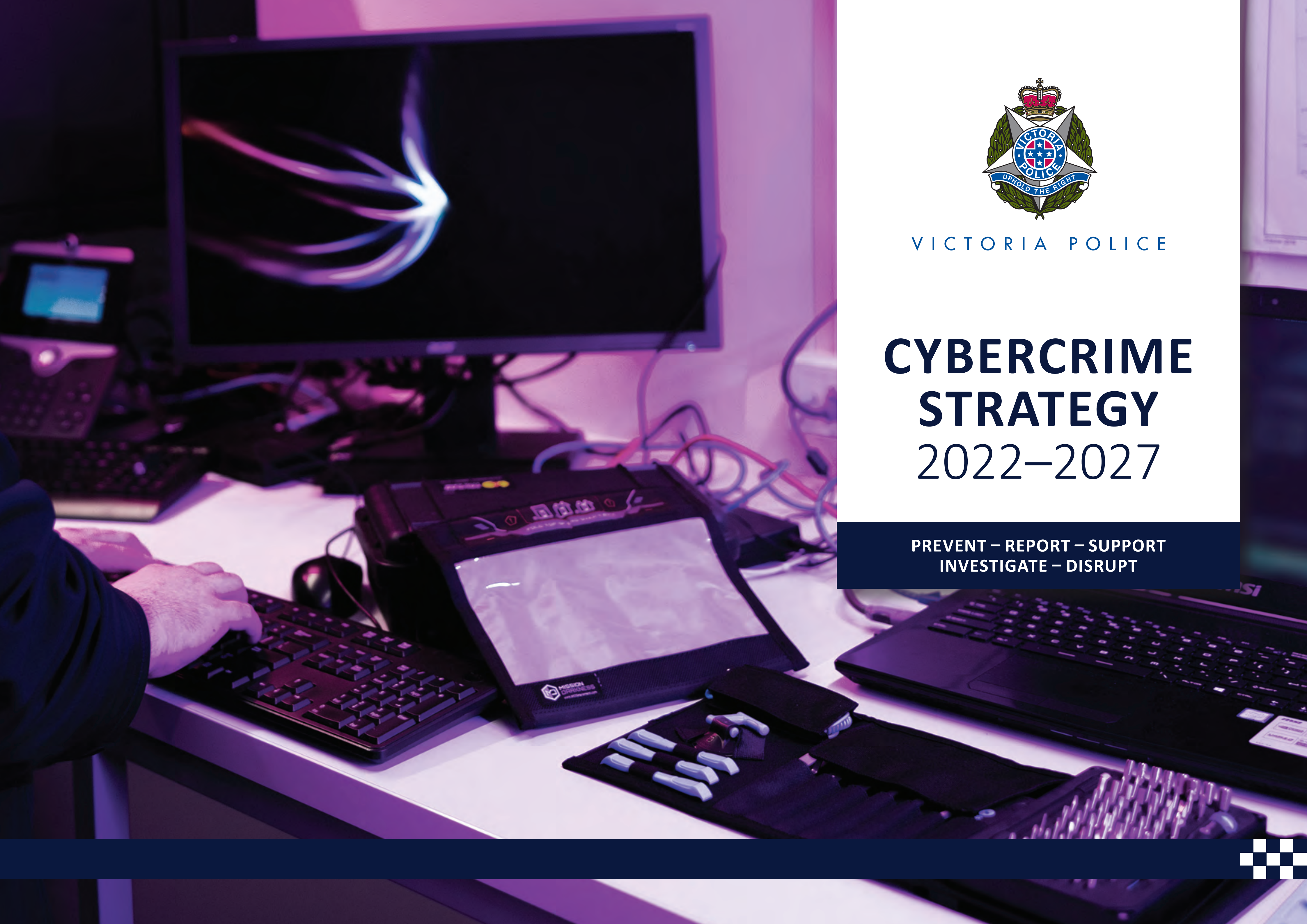


VICTORIA POLICE

CYBERCRIME STRATEGY 2022–2027

PREVENT – REPORT – SUPPORT
INVESTIGATE – DISRUPT

Message from the Deputy Commissioner

Technology is central to the way we live our lives. Technology also has an impact on the frequency and reach of many crimes. Cybercrime is a broad term used to describe crimes against computers such as hacking and any other crime enabled by technology, such as online scams and child exploitation. Most often, police respond to crimes that involve technology in some way. Technology has changed the landscape of when, where and how crimes are committed. The Victoria Police Cybercrime Strategy 2022–2027 will guide Victoria Police as it builds capability and works with strategic partners and the community to meet the challenges and impacts of cybercrime.

Victoria Police remains unwavering in its commitment to minimising the impact that cyber-dependent and technology-enabled crime have on the Victorian community. That is why we have deepened our understanding of the harms cybercrime can have on individuals, families, businesses, industry and government in Victoria. This strategy outlines our role and priorities in preventing and responding to cybercrime now and into the future.

Our objective is to work together to build a **cyber safe and secure Victoria**. A cyber safe and secure Victoria means all Victorians, including individuals, families, businesses, community groups, critical infrastructure and essential services, and government are safe to connect, engage and do business online. To realise this, we will modernise the way we work across the organisation to prevent, detect, disrupt and investigate cybercrime, and support victims when they report a cybercrime. We will renew our focus on preventing cybercrime through community awareness and disruption, and will continue to enhance our specialist capabilities in cybercrime law enforcement. We will maintain our collaborative work with our partners—including law enforcement agencies, government and industry—and build capability to better respond to existing and emerging cybercrime threats facing Victorians.

Victoria Police is not alone in tackling the large, complex and fast-moving threat that cybercrime presents. Alongside our strategy is a detailed action plan. We will actively invest in our capacity and capability to deliver outcomes for the Victorian community. We can and will do more to reduce the harm from cybercrime across Victoria.

ROSS GUENTHER
Deputy Commissioner
Public Safety and Security

What is **cybercrime**?

Cybercrime is used to describe ways of offending using technology. A broad range of crime types can be cybercrime, including crimes against the person (such as stalking and extortion) and against property (such as hacking and online scams).

For Victoria Police and our partners, **cybercrime** has two aspects:

→ CYBER-DEPENDENT CRIME

Crime directed at computers or other information communications technologies (ICTs).

→ TECHNOLOGY-ENABLED CRIME

Crime where computers or ICTs are an integral part of an offence.

Cybercrime that targets networked devices (including computers, smart phones and smart watches, and tablets), such as hacking and denial of service attacks, is described as cyber-dependent crime, because without computing technology these offences cannot be committed. Technology-enabled crimes are offence types that can occur without technology, but often see an increased scale, reach or harm by the use of technology in how they are committed. For example, frauds and scams, identity crime, child abuse, stalking and harassment, family violence and politically and ideologically motivated violence.

The most common reasons people commit cybercrime is to cause harm to, or receive a benefit at the expense of a victim.

Technology may also be incidental to a crime. For example, an offender might arrange to commit a crime by mobile phone, or it might place them at a crime scene. In this instance, the mobile phone and its offence-related contents are vital pieces of digital evidence for police.

In 2020, the World Economic Forum identified **cyberattacks**, together with **data fraud or theft**, as **TWO** of the

⚠ **TOP 10 GLOBAL RISKS**

facing the world today[1]

Our **mission**

The *Victoria Police Act 2013* legislates that our role is to serve the Victorian community and uphold the law to promote a safe, secure and orderly society.

The functions of Victoria Police include the following:

- Preserving the peace;
- Protecting life and property;
- Preventing the commission of offences;
- Detecting and apprehending offenders; and
- Helping those in need of assistance.

In relation to cybercrime, our mission is to provide a modern policing service to help build a **cyber safe and secure Victoria**. We aim to reduce harm by lowering instances of cybercrime, holding offenders to account, and helping victims recover.

The Victoria Police Cybercrime Strategy 2022–2027 delivers the strategic plan to achieve our mission. Through this plan Victoria Police will fulfil our roles and functions to address cybercrime and work with our partners to achieve improved community safety outcomes.

The Strategy provides a roadmap for all employees of the organisation so that they understand how their role and work aligns to the overarching mission to tackle cybercrime and produce better outcomes for Victoria.

> “Technology and the way criminals use it is constantly changing. Victoria Police must keep evolving, building, reforming, and adjusting our capabilities for cybercrime. We cannot set and forget.”
>
> SUPERINTENDENT, CYBERCRIME DIVISION

Cybercrime is a **global** problem that affects Victoria

Cybercrime does not respect national borders. Offenders and victims do not need to be in the same place. Cybercrime can strike anywhere, against anyone who is connected to the internet. Industry estimates that cybercrime will cost the world USD$10.5 trillion annually by 2025.[2]

Victoria is not immune to the global threat of cybercrime. Victoria's relative wealth, high saturation of digital connections and growing reliance on the internet make it an attractive target for cybercriminals.

Cybercrime is recognised nationally as a key facilitator of serious and organised crime, and is a national security concern.[3]

In the 2020–21 financial year, there were

OVER 67,500 CYBERCRIME REPORTS

made to ReportCyber, an increase of nearly 13% from the previous financial year.[4] Self-reported losses from cybercrime in the 2020–21 financial year totalled more than $33 billion.[5]

In the 2020/21 financial year, there were nearly **6,000 additional cybercrime reports** made to ReportCyber and referred to Victoria Police than in the previous year.[6]

Victorians submitted an online cybercrime report

EVERY 26 MINUTES

averaging 55 reports a day.[7]

Cyberattacks on critical infrastructure or serious cyber security emergencies may result in significant harm for all or part of the Victorian community.

In extreme circumstances, these attacks may result in loss of life and extensive damage to property, infrastructure or the environment. For example, in 2019, ransomware disrupted health service providers and hospitals in Gippsland and south-west Victoria, delaying surgeries and other medical services. Approximately a quarter of cyber security reports to the Australian Cyber Security Centre during the 2020–21 financial year were associated with Australia's critical infrastructure or essential services.[8]

Criminals, including serious and organised crime groups in Victoria, use the **anonymising features of cryptocurrency** to facilitate a range of offending, such as drug trafficking and money laundering.

This creates additional challenges for Victoria Police's ability to detect, investigate and prosecute such crimes.

Technology is also used to facilitate **violence against children**.

According to the Australian eSafety Commissioner, approximately **27%** of domestic violence cases involved technology-facilitated abuse of children.[9]

The live streaming of child abuse has been identified as an emerging trend on social media.

> "While rapid growth in Internet and computer technology has enabled economic and social growth, an increasing reliance on the Internet has created more risks and vulnerabilities, and opened up new possibilities for criminal activity."
>
> INTERPOL GLOBAL CYBERCRIME STRATEGY[10]

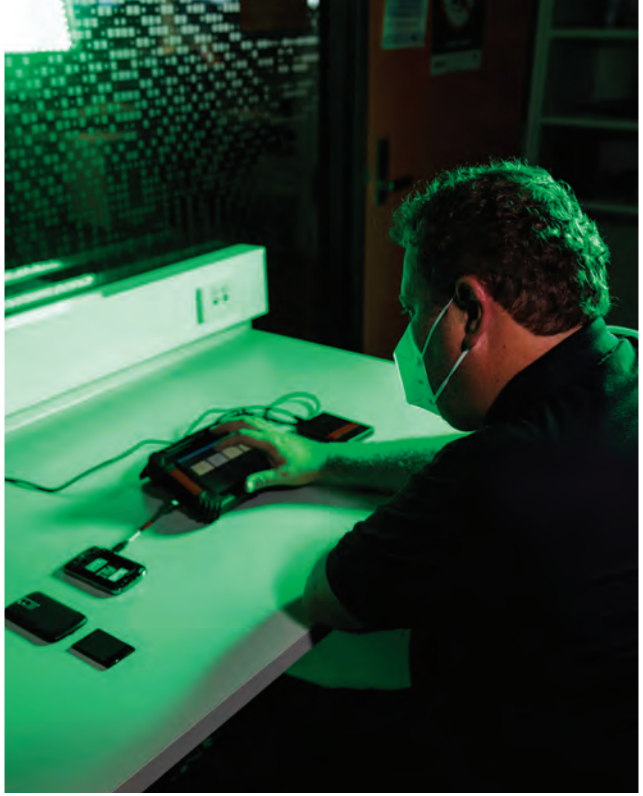
There is significant growth in Victoria Police's demand for **digital forensic services** to collect digital evidence, as technology is increasingly used to commit different crimes.

OUR PARTNERS INCLUDE:

- Academia
- Australian Cyber Security Centre
- Australian Centre to Counter Child Exploitation
- Australian Criminal Intelligence Commission
- Australian Government
- AUSTRAC
- Commonwealth and other state and territory law enforcement agencies
- Communities
- Industry
- International law enforcement partners
- Office of the eSafety Commissioner
- Support services
- Victorian Government

A problem accelerated by the **COVID-19 pandemic**

The COVID-19 pandemic has accelerated society's reliance on digital technology. People are spending more time online and are reliant on technology to perform a range of everyday tasks: from working, to socialising with family and friends, to attending medical appointments and purchasing groceries. With more time spent online, Australians are increasingly vulnerable to cybercrime.



Victoria Police's Joint Anti Child Exploitation Team received a **400% INCREASE** in reports of **child abuse material related internet reports** in June 2020 compared to June 2019.

The Australian Cyber Security Centre found that more than **75%** of pandemic-related cybercrime reports involved Australians losing money or personal information.[11]

According to the Australian Competition & Consumer Commission,

VICTORIANS REPORTED AROUND
$49 million in losses
TO SCAMWATCH IN 2020

This is more than **double** the loss reported in 2019.[12]

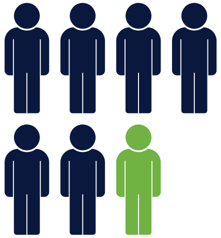
> "Vulnerability to cybercrime, particularly cyber-enabled crime such as cyber abuse and technology-facilitated abuse, has increased due to reliance and use of the internet during social isolation and work from home arrangements."
>
> THE DEPARTMENT OF HOME AFFAIRS[13]

The harm and cost to our **community**

Cybercrime causes large losses and widespread harm to the Victorian community.

Victims of cybercrime can suffer a range of harms, including financial, physical and sexual. Victims can also suffer serious psychological, emotional and social harms that can have a long-lasting impact on the victim. Victims can experience reputational damage, which can affect their personal and professional lives and cause serious mental health trauma.

Cybercrime also has significant economic costs.



ONE IN SEVEN
AUSTRALIAN ADULTS
—2.8 million people—
had been a **victim of cyber-dependent crime** in 2020.

ONE IN THREE had been a victim of cyber-dependent crime in their lifetime.[14]

The Australian Federal Police estimates that business email compromise scams – a cybercrime technique where legitimate funds transfers are redirected to alternative accounts – cost Australian businesses more than $79 million in the 2020–2021 financial year.

> ‘The [Australian Criminal Intelligence Commission] assesses that cybercrime is leading to severe and long-term harms, … beyond the financial losses incurred and include significant psychological, emotional and social harms. This is particularly pertinent in cases where the crime is psychosocial in nature, such as the non-consensual sharing of intimate images and cyberbullying.’
>
> THE DEPARTMENT OF HOME AFFAIRS[17]

Cyber-dependent crime is a highly profitable criminal activity and results in **significant financial losses** to Australians with only a small proportion of financial losses recovered by victims.[15]

The cost of cyber-dependent crime to Australian individuals in 2019 was

$3.5 billion

- **$1.9 BILLION**
  in money directly lost by victims.
- **$597 MILLION**
  spent dealing with the consequences of victimisation.
- **$1.4 BILLION**
  spent to prevent falling victim.

Victims **recovered** approximately $389 million.[16]

ONLINE GROOMING

David – through the eyes of the parent

WHAT HAPPENED?

David is a working dad with three children: Daniel and Matilda (7) and Angie (14). Angie has just commenced her second year of high school. Angie begged David for a smartphone. David finally relents and gives Angie his old smartphone. As a condition for receiving the phone, Angie must share her passcode and must leave the phone to charge overnight in the kitchen.

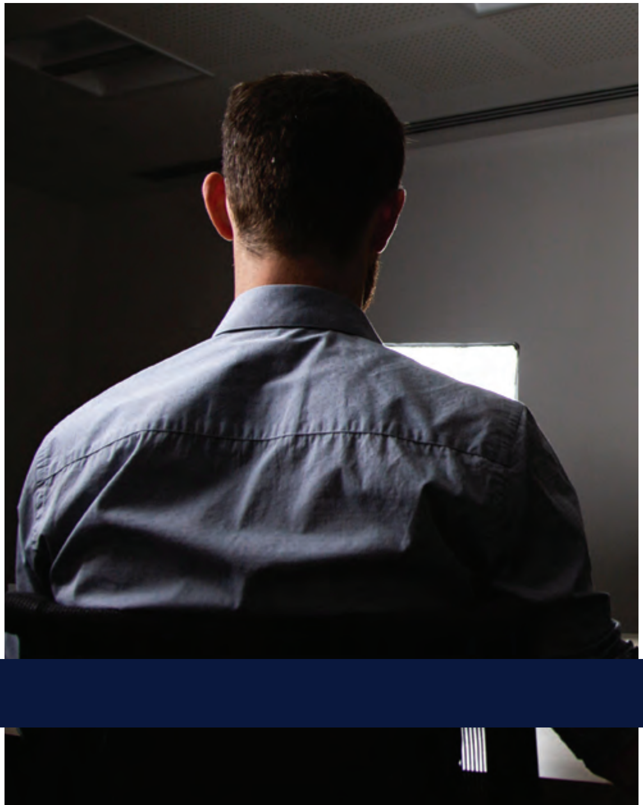
Angie spends a lot of time on her phone. David will often ask Angie what she is doing on the phone. He tries to monitor her use and keeps track of the phone bill. David has to start working long nights on a special project for work. David is not able to monitor Angie's phone use as closely. Soon, Angie begins to keep her phone in the room overnight.

As the months go by, David notices Angie's behaviour changes. She becomes withdrawn and irritable. Her school work starts to suffer. David receives a call from the school principal – the principal needs an urgent meeting with David. The principal tells David that a parent of one of Angie's friends told the principal that Angie is in contact with a man online who sends Angie inappropriate messages. David talks to Angie and learns that she met this man on a messaging app and they message constantly.

Online child grooming is befriending a child, and sometimes the family, to make the child more open to sexual abuse. A person who is found guilty of grooming in Victoria is liable to 10 years imprisonment.

HOW WAS DAVID AFFECTED?

David is horrified and feels like he has failed Angie. He feels he has neglected his duty as a parent. David is devastated that Angie did not tell him what was happening. David feels powerless to keep his child safe. David starts to suffer from anxiety, affecting his work and relationships.



ONLINE SCAMS

Amara – a retired widow

WHAT HAPPENED?

Amara received and accepted a friend request from Ferenc, a Hungarian serviceman on peacekeeping duties in Afghanistan. Ferenc and Amara grew closer together. Ferenc shared pictures with her and told Amara he had lost his wife to cancer. This was similar to Amara's own experience – her elderly husband died of cancer two years ago.

Ferenc said he was being posted to Cyprus but that his time in the military was nearly finished. Ferenc told Amara he wanted to set up a jewellery store when he retired. Ferenc told Amara he was coming to see her but had some trouble with his bank card not working in Cyprus and could not get funds to pay for an export tax on his gemstones. Taking out a loan, Amara transferred Ferenc $15,000 to cover the tax bill. Shortly after, Ferenc told Amara that he had been detained by local authorities in Malaysia on the way to Australia. He needed $20,000 to pay his legal and court fees.

Amara contacted the Malaysian police – they had no knowledge of Ferenc. When Amara told Ferenc she could not send the additional money, he responded with very angry messages, and then ceased contact altogether.

HOW WAS AMARA AFFECTED?

Amara was left confused and hurt. She feels betrayed and cheated. She knows in her head that this was a scam, but in her heart still feels that Ferenc might be out there and she has let him down. Amara had to re-enter the workforce to service the loan she took. She is also at risk of having her identity stolen because she shared a lot of personal information with the scammer calling himself Ferenc.

The majority of romance baiting scams in 2020 involved **cryptocurrency** INVESTMENT SCAMS[18]

Romance and dating scams involve scammers taking advantage of people looking for romantic partners, often via dating websites, apps or social media, by pretending to be prospective companions. They play on emotional triggers to extract money, gifts or personal details. **Romance baiting** encourages victims to take advantage of a fake investment opportunity.

In 2020, Australians reported a total of **$37 million** in losses from **dating and romance scams**[19]

Whilst traditional dating and romance scams tend to target older Australians, **almost half** of all losses to romance baiting scams come from people **under the age of 35**[20]

RANSOMWARE

Jin and Bella – small business owners

WHAT HAPPENED?

Jin and Bella run a family owned accounting firm that provides outsourced bookkeeping and accounts functions for small businesses across Victoria. The business operates through an online platform—client companies log in through a website portal and can take care of several bookkeeping needs for their businesses, such as tracking their expenses, processing receipts and calculating deductions.

Jin and Bella's business computers were infected with ransomware via a suspect email just before tax time. This ransomware locked down the business' platform so that clients were unable use the portal. The cybercriminals demanded $100,000 in Bitcoin, a cryptocurrency, to restore the network. Jin and Bella refused to pay. The cybercriminals threatened to publish the private information of Jin and Bella's clients. Jin and Bella did not know what to do. They did not have the money to pay the ransomware. Eventually, Jin and Bella contacted Victoria Police to report the crime.

The majority of Jin and Bella's clients were unable to submit their tax returns on time. Clients were extremely dissatisfied with the service.

Ransomware is a form of extortion using malicious software (malware) that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

The Australian Cyber Security Centre advises against paying ransoms. Payment of the ransom may increase an individual or organisation's vulnerability to future ransomware incidents. In addition, there is no guarantee that payment will undo the damage.

HOW WERE JIN, BELLA AND THEIR CLIENTS AFFECTED?

The reputation of Jin and Bella's business suffered and as a result, they lost clients. Jin and Bella experienced considerable stress and anxiety from the attack.

RANSOMWARE

The Australian Cyber Security Centre has observed cybercriminals successfully using ransomware to disrupt operations and cause reputational damage to Australian organisations across a range of sectors:

- Health
- State and Territory governments
- Transport
- Education and research organisations
- Retail

The Australian Cyber Security Centre reported a 15% increase in ransomware cybercrime reports in the 2020–21 financial year.[21]

MALWARE AND INTIMATE IMAGE ABUSE

Aisha – a teacher

WHAT HAPPENED?

Aisha is a teacher who unknowingly had malware called a Remote Access Trojan (RAT) downloaded onto her smart phone. Using the RAT, a cybercriminal accessed her email and text messages, and forwarded some private, intimate pictures to colleagues and family members in her contacts. The cybercriminal also posted these images, as well as some digitally altered "deepfakes", to several adult websites. Some of these images were found by students at Aisha's school.

Aisha did not make a report to Victoria Police, but tried to track down the websites where the images were posted to demand that they were taken down. She suspects that her ex-boyfriend – who has a history of control and emotionally abusive behaviour – was behind the attack, but she did not have any way to prove this.

HOW WAS AISHA AFFECTED?

Aisha has been devastated by these events—both privately and professionally. Although her school ultimately understood that she was a victim, the damage to her reputation was irreversible. This, coupled with the anxiety that her students had seen these personal and deepfake images of her, led to her giving up her teaching position at the school. This was her primary source of income.

11% of Australian adults have experienced **image-based abuse**[22]

Women aged 18 and over are **twice as likely** as men aged 18 and over to have experienced image-based abuse[23]

Deepfakes use artificial intelligence software to learn from large numbers of images or recordings of a person to create an extremely realistic but false depiction of them doing or saying something that they did not actually do or say.[24]

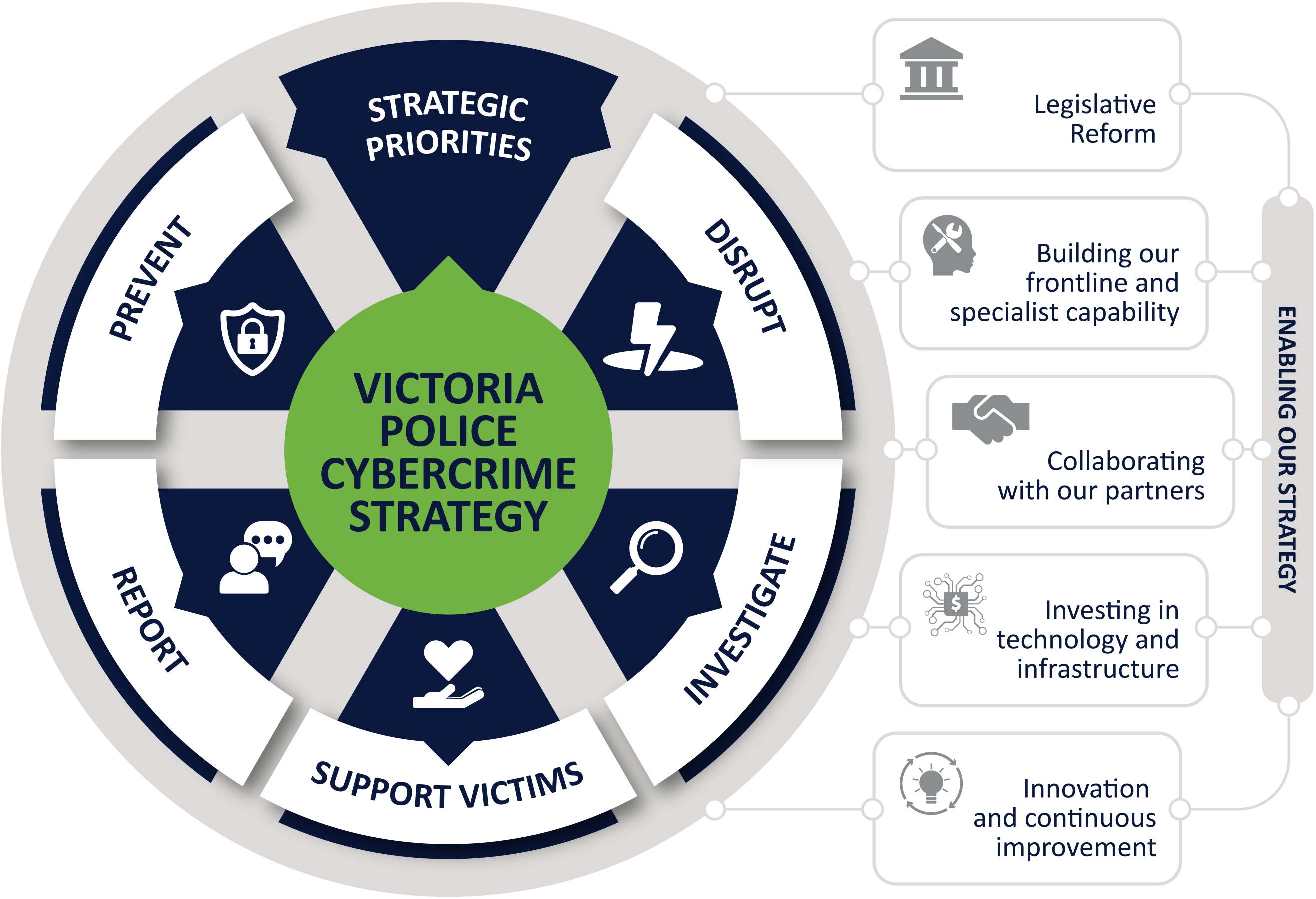
Image-based sexual abuse is the creation, distribution or threatened distribution of intimate, nude or sexual image or videos, without the consent of the person pictured. This includes images or videos that have been digitally altered using specialised software.

You can also report image-based abuse to the **eSafety Commissioner**.

STAFF
OFFICIAL DIARY PB13

Our **strategic** priorities

For Victoria Police to effectively perform our roles to tackle cybercrime and help achieve a cyber safe and secure Victoria, we have set five strategic priorities. The priorities will guide how we work across our organisation, with our partners and with the community over the next five years. These strategic priorities rely upon five critical enablers, which will make it possible for us to deliver the needed outcomes for Victoria.


STRATEGIC PRIORITIES
VICTORIA POLICE CYBERCRIME STRATEGY
PREVENT
DISRUPT
INVESTIGATE
SUPPORT VICTIMS
REPORT
Legislative Reform
Building our frontline and specialist capability
Collaborating with our partners
Investing in technology and infrastructure
Innovation and continuous improvement
ENABLING OUR STRATEGY

Prevent

Empowering the Victorian community with information to reduce their risk of becoming a victim of cybercrime is a vital component of prevention.

OUR ROLE

Victoria Police will actively work with our partners to raise awareness and educate the community about the threat of cybercrime so that all parts of our community feel empowered to protect themselves. We understand that our role in prevention is a shared responsibility. We will strengthen the relationships with our law enforcement, government and non-government organisation partners to support new approaches to cybercrime prevention, cyber safety and cyber security awareness campaigns.

We will work with our partners to reduce individual and community vulnerability to cybercrime threats, and to strengthen resilience to cybercrime across Victorian business, industry and local and state governments. Together, we will build Victoria's cyber awareness and reduce our community members' risk of becoming a victim of cybercrime.

WE WILL…

Partner with key Victorian and Commonwealth agencies (including the Victorian Department of Education and Training) to coordinate **awareness** raising efforts and provide **practical advice** on cybercrime, cyber security and cyber safety, tailored to individuals, families, business and industry.

Work with **industry and businesses** to support prevention efforts.

Develop and deliver new, accessible **cybercrime and risk mitigation resources** for the Victorian community (both online and available in stations).

Publish **accessible** prevention resources to support the diversity of Victoria's community.

Work with our **partners** to ensure our prevention messaging is nationally consistent.

Publish timely and relevant crime **prevention advice** for critical, common and hot topic cybercrime types through various communications channels.

SO THAT…

Individuals, families, businesses, industry and government are empowered with a better understanding of cybercrime, their vulnerability and key risk mitigation strategies.

WHAT WILL SUCCESS LOOK LIKE?

- ✓ The Victorian community has a better understanding of cybercrime vulnerability and how they can protect themselves.
- ✓ Victoria Police works collaboratively with strategic partners to support a range of effective prevention activities.

Report

Victoria police will simplify and streamline the process for reporting cybercrime.

Victoria Police understands that many individuals, families and businesses are reluctant to report a cybercrime to police. The processes for reporting and investigation can at times be unclear or difficult to navigate, so we are committed to making these easier to access and use.

OUR ROLE

Victoria Police will make reporting cybercrime easier for all Victorians. We will equip our frontline and specialists with the knowledge, skills and protocols they need to provide a consistent service to cybercrime victims. We will continue to work with our national partners to make online reporting easier.

CASE STUDY

LINKING ONLINE REPORTS TO STOP CYBERCRIME

Often online scams have victims all across Australia and offenders are located outside Victoria. Online cybercrime reports are referred to the most appropriate police agency, which may be an interstate police agency. This is done to link reports and coordinate police responses.

Often cybercriminals will create fake trader websites to sell non-existent items. In 2017, Queensland Police were able to arrest two foreigners on visitor visas in Queensland for pretending to sell barbeques and fitness goods on several websites. Fake invoices were sent, but the goods never arrived, and then the sellers cut contact with their victims. More than 200 people across Australia made reports online, including many Victorians.

In another case, hundreds across Australia received emails falsely claiming cybercriminals had a sexual video of them and threatening to release it to family, friends and employers unless a ransom was paid. Online reporting quickly identified the extortion campaign, allowed police to determine it was an empty threat, and allowed coordinated prevention messaging to be swiftly sent out to reassure communities.

WE WILL…

Work with our key federal and state law enforcement, government, non-government and industry **partners** to ensure Victorians can easily understand how to report cybercrime.

Ensure that when Victorians report a cybercrime they are provided **clear information** on how Victoria Police or our interstate police partners will respond.

Work with our partners to develop **official crime statistics** for cybercrime. Public crime statistics will let the Victorian Government and community know how much cybercrime affects Victorians and show our progress against our mission.

Reform the way Victoria Police reports, records, triages and actions cybercrime.

Develop and implement **consistent protocols** for responding to reports of cybercrime, centrally and locally, online and in-person.

Leverage Victoria Police **data** to identify, communicate, prevent and target cybercrime trends.

SO THAT…

- Victorians know how to and can easily report cybercrime.
- Victoria Police efficiently and consistently respond to reports of cybercrime, supporting better victim service delivery experiences and outcomes.
- Victim liaison, and communication following a report is efficient, consistent and meets community expectations.

WHAT WILL SUCCESS LOOK LIKE?

✓ Victoria Police responds to cybercrime reports efficiently and consistently according to victim type.

✓ Victorians are clear about Victoria Police's or our interstate police partner's response.

✓ Victoria Police is able to respond to emerging challenges through the use of enhanced intelligence to identify trends in reporting.

Support

Victoria police is committed to enhancing the way we support victims of cybercrime—whether victims are individuals, families, business of any size or government.

Victims of cybercrime in Victoria have not always been offered consistent, high-quality support. Victims have also not always been aware of the value of reporting cybercrime to Victoria Police, or the type of support that is available to them.

OUR ROLE

Victoria Police is committed to its core role in providing a victim-centric policing service for all victims of crime–including cybercrime. We will work to enhance service delivery for those in need of assistance after becoming victims of cybercrime. We acknowledge that different types of victims—individuals, families, small and medium business, industry and government—will require different types of assistance and support from Victoria Police.

We acknowledge that victim-centric policing in the context of cybercrime means further enhancing understanding of cybercrime across the organisation. We are committed to ensuring that every member of Victoria Police has the right skills and knowledge to provide high-quality, consistent victim support, regardless of crime type or method of reporting. We will continue to consult with the community and our partners to continuously improve our referral approaches to meet victim expectations and respond to emerging cybercrime trends.

Victim support can be enhanced through collaboration with our partners. Victoria Police will strengthen our relationships and identify opportunities to improve victim support across the system.

WE WILL...

- Ensure **victims of cybercrime** are provided with timely and relevant advice, support and follow up.
- Better equip our employees with the **expertise and knowledge** to police cybercrime.
- Use data to **identify trends** in cybercrime and use this analysis to aid our victim support work and that of our partners.
- **Consult with the community** to better understand what victims of cybercrime need.
- Work with our government and industry **partners** to ensure all Victorians have access to appropriate and timely victim supports.
- Publish **accessible** versions of victim support advice and resources for diverse community members.
- Work with our partners to identify **victim support service** available across the country to enable us to support interstate victims.

SO THAT...

- Victoria Police takes a victim-centric policing approach to responding to cybercrime and supporting victims.
- Victims receive an excellent service delivery response and are supported to understand their options for help.
- Victims understand cybercrime, how it is policed, their risks of repeat victimisation, and how to prevent further victimisation.

WHAT WILL SUCCESS LOOK LIKE?

- ✓ Victoria Police delivers high-quality, consistent support that meets the needs of different victims.
- ✓ Strengthened partnerships and enhanced victim support delivered through a collaborative approach.

Investigate

Victoria Police is committed to continuous improvement of our cybercrime investigation practices to adapt to emerging needs.

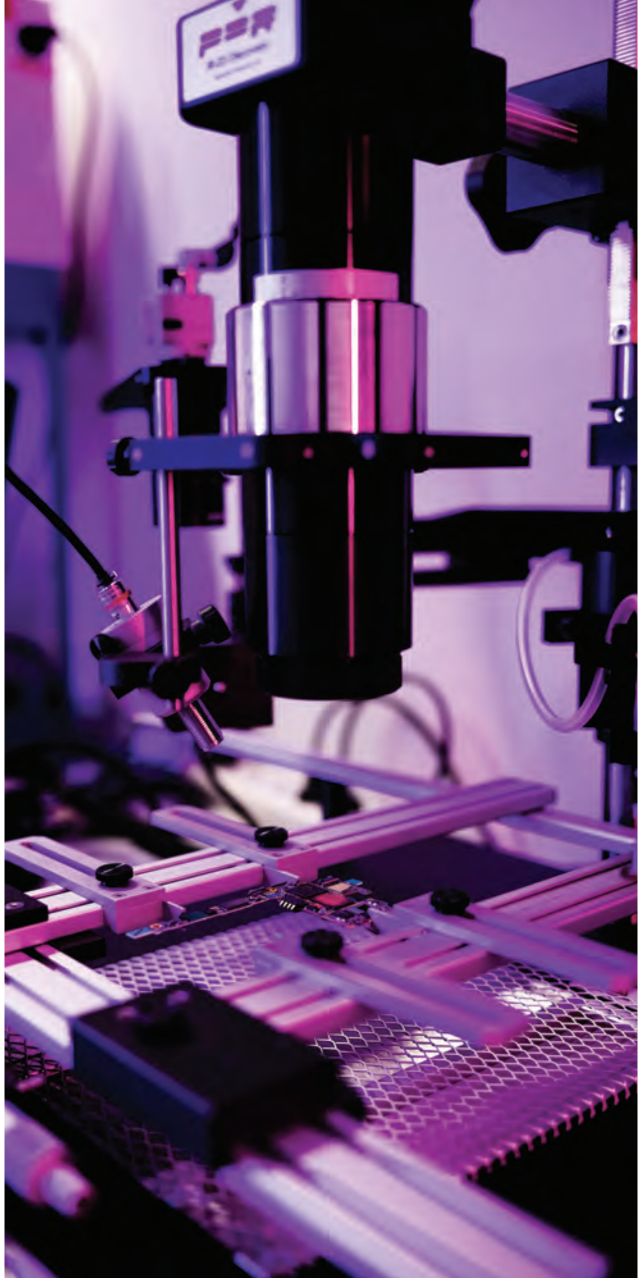
Approaches to investigation need to respond to new technology and the evolution of cybercrime to effectively prosecute cyber-dependent and technology enabled crime. Victoria Police will continue to focus on its policing capabilities to respond to cybercrime—from frontline members to specialist units.

A renewed focus in specialist knowledge, skills and policing techniques will be complemented by a dedicated investment in digital forensic technology across the organisation, given the increasing importance of digital evidence to so many crimes. For example, a smart phone might contain evidence of the crime, it might place an offender at a crime scene or exonerate them.

OUR ROLE

Victoria Police has responsibility for investigating cybercrime committed against the Victorian community, whether by Victorians or those elsewhere. It is our job to carry out the policing mission in *Victoria's Cyber Strategy 2021* and support the *National Plan to Combat Cybercrime*. We will enhance how Victoria Police pursues investigative activities (including evidence gathering) for cybercrime to maximise the impact on cybercrime and provide better outcomes for victims.

We will continuously improve our approaches to emerging technical challenges such as cryptocurrencies, encryption, darknets and other advancements.



CASE STUDY

INVESTIGATING AND DISRUPTING CYBERCRIME AGAINST VICTORIANS FROM OFFSHORE

When 128 Victorian schools and kindergartens were targeted by hoax bomb and active shooter phone calls, Victoria Police made the crucial break in the investigation to disrupt a global campaign of over 2,500 threatening calls worldwide.

The calls used encrypted communications and faked local phone numbers. They targeted schools, commercial airlines, police stations, hospitals and other businesses resulting in enormous costs and psychological harm, including evacuations of over 40,000 students and staff around Victoria, halt of businesses, and diversion of commercial flights.

Victoria Police cybercrime investigators worked closely with our national and international partners to investigate. Using innovative investigative techniques and specialist capabilities, and working with overseas service providers, Victoria Police identified a vendor selling threats-as-a-service on the darknet, the services used, call recordings online, and the offender located overseas.

Victoria Police provided this evidence to the overseas police cyber unit, resulting in the arrest and successful prosecution of the offender and stopping the calls worldwide.

WE WILL...

Continue to build the cybercrime **capabilities** of our workforce.

Pursue investigations into cybercrime that targets Victoria, whether by Victorians or those elsewhere. We will identify cybercrime **causing most harm** to communities and design investigations for greatest impact.

Partner with other law enforcement agencies to support contemporary, coordinated and responsive investigative practice.

Continue to invest in our **specialist capabilities** through targeted, alternative recruitment pathways and professional development strategies, and where appropriate, draw on our partnerships to support this process.

Ensure our **investments** in technology and infrastructure support contemporary investigative practice across the organisation.

SO THAT...

Cybercrime investigations are efficient, targeted and outcomes-focused.

WHAT WILL SUCCESS LOOK LIKE?

- ✓ Victoria Police pursue targeted, efficient and outcomes-focused cybercrime investigations.
- ✓ Victoria Police has the right capability, infrastructure and technology to investigate cybercrime and support successful prosecutions.

Disrupt

Disruption of cybercrime activity is one of the most effective strategies to prevent victimisation and reduce levels of community harm.

It is critical to stop cybercriminals before they cause more harm, to more people. Not all cybercrime offenders can be brought before Victorian courts, either because they are as yet unidentified or are overseas. In these cases, Victoria Police will disrupt the crime to protect the community. Disruption is achieved when intentional action leads to an offender being unable to operate at its usual level of activity, or when the number of future victims is reduced, for a period of time. Cybercrime disruption can involve a range of activities, including:

- Reducing the availability/scale of digital infrastructure, and denying offenders the ability to relocate or rebuild, such as account take overs or disabling digital forums or necessary cybercrime infrastructure.
- Denying offenders the financial proceeds of cybercrime.
- Covert online activities to infiltrate cybercrime operations.

OUR ROLE

Ethical disruption of criminal activity is a core element of Victoria Police's prevention and response functions. Victoria Police already uses disruption for a range of technology-enabled offences, such as online child abuse. We will continue to enhance our policing capabilities and work with our national and international law enforcement partners to ensure that we can disrupt existing and emerging types of cyber-dependent and technology-enabled crime. We will pursue disruption activity that is appropriate and effective.

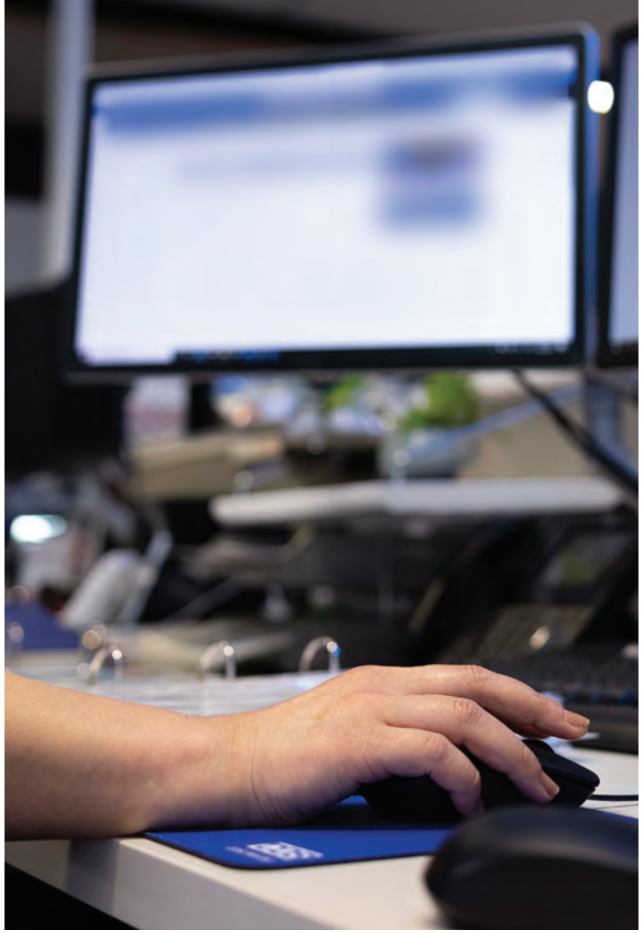
CASE STUDY

DISRUPTING BUSINESS EMAIL COMPROMISE (BEC)

In January 2021, a Victorian company contracted an overseas company to install fittings at a new construction site and arranged to pay for the upcoming work. They received emails instructing them to make the payments to another bank account. The company confirmed the account details via email, but email accounts at both companies had been compromised. Offenders registered fake domain names for both companies, which resulted in emails going to the cybercriminals. Almost AUD$3.6 million was sent to an account in a third country.

The contractor uncovered the deception when they telephoned to query not receiving the funds. The Victorian company reported to their bank and via ReportCyber, which referred the report to Victoria Police for investigation as part of the national BEC taskforce. Working with international partners, approximately $900,000 was recovered and a suspect overseas is under investigation.

In August-2021, the Victoria Police Cybercrime Squad identified and arrested an alleged mule handler in Victoria who ran mules across three states. Funds from BEC are often transferred into accounts of money mules or opened as a result of identity takeovers. Mule handlers assist the mule to exchange the stolen funds into gold bullion, cryptocurrencies, international money transfers or luxury goods to launder the proceeds of crime.



A 'money mule' is a person who receives money from a third party in their bank account and transfers it to another account, or withdraws it in cash to give someone else, often obtaining a commission for their efforts.

WE WILL...

Continue to build capability to work with our interstate, national and international **partners** to pursue tactical, high-impact offshore and onshore disruption activities.

Continue to use the most **contemporary policing** techniques to disrupt cybercrime.

Continue to invest in our **specialist capabilities** for cybercrime disruption through targeted, alternative recruitment pathways and professional development strategies.

Ensure we have the **right standards, oversight and accountability, and public reassurance** for cybercrime disruptions.

Pursue new and **innovative partnerships** with industry to disrupt cybercrime.

SO THAT...

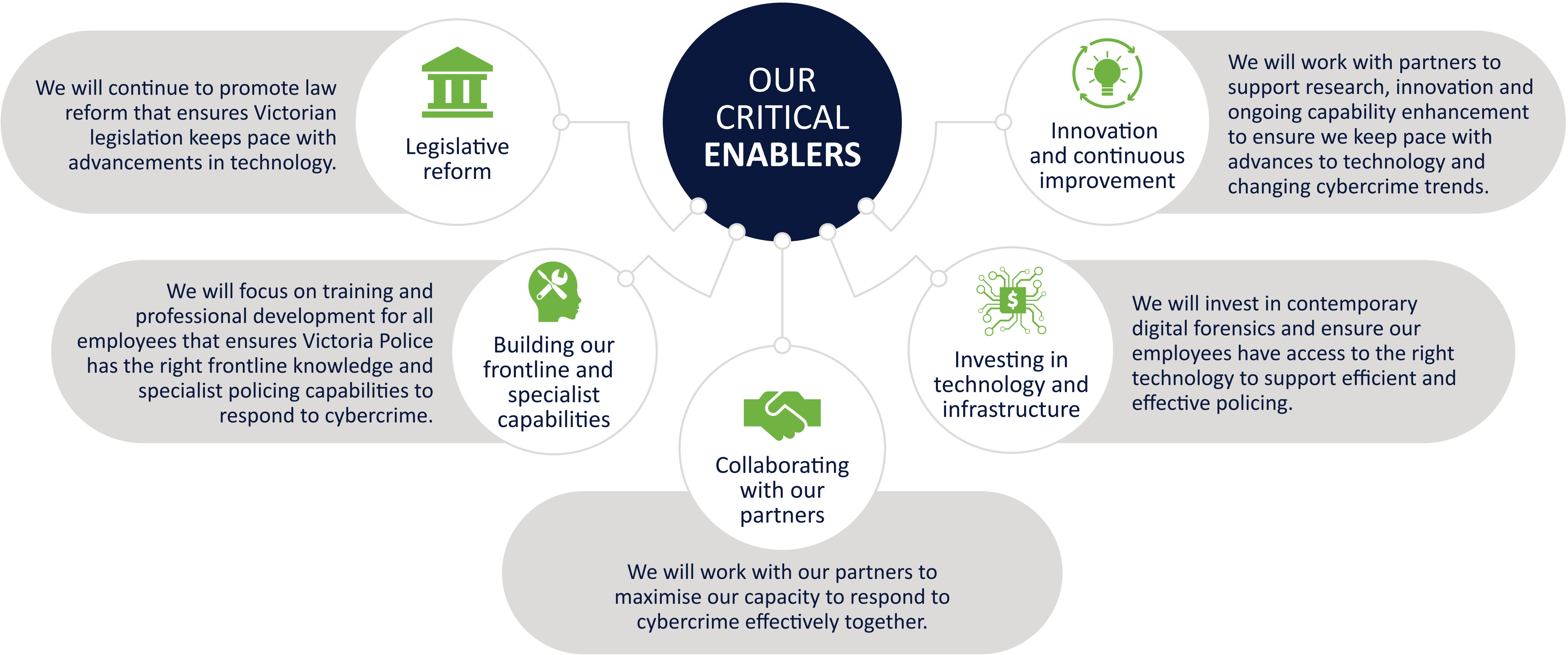
We disrupt and prevent instances of victimisation and reduce levels of cybercrime harm affecting the Victorian community.

WHAT WILL SUCCESS LOOK LIKE?

- ✓ Victoria Police disrupts cybercrime and reduces its harm to the Victorian community.
- ✓ Victoria Police continue to coordinate with other law enforcement agencies to pursue tactical, high-impact disruption activities.
- ✓ Victoria Police works proactively with industry to pursue disruption activities.

Critical **enablers**

Realising our strategic priorities relies on a number of critical enablers.



OUR CRITICAL **ENABLERS**

Legislative reform

We will continue to promote law reform that ensures Victorian legislation keeps pace with advancements in technology.

Innovation and continuous improvement

We will work with partners to support research, innovation and ongoing capability enhancement to ensure we keep pace with advances to technology and changing cybercrime trends.

Building our frontline and specialist capabilities

We will focus on training and professional development for all employees that ensures Victoria Police has the right frontline knowledge and specialist policing capabilities to respond to cybercrime.

Investing in technology and infrastructure

We will invest in contemporary digital forensics and ensure our employees have access to the right technology to support efficient and effective policing.

Collaborating with our partners

We will work with our partners to maximise our capacity to respond to cybercrime effectively together.

Collaborating for better outcomes

Victoria Police will work with our partners—including law enforcement, government and industry—to leverage our capacity to prevent, disrupt and respond to existing and emerging cybercrime threats, and to provide the best possible support to victims. Together, we will work to make sure Victorians are safe and secure online and in the community and are protected from cybercrime.

A call to **action**

Keeping Victorians safe from cybercrime starts with information and advice. Victorian Police encourages all members of our community and across industries to educate themselves so that they are cyber aware and can protect themselves and their businesses when online.

Visit the Victoria Police website for translations of this strategy.

If you know of someone committing or planning to commit a cybercrime

CALL CRIMESTOPPERS
1800 333 000

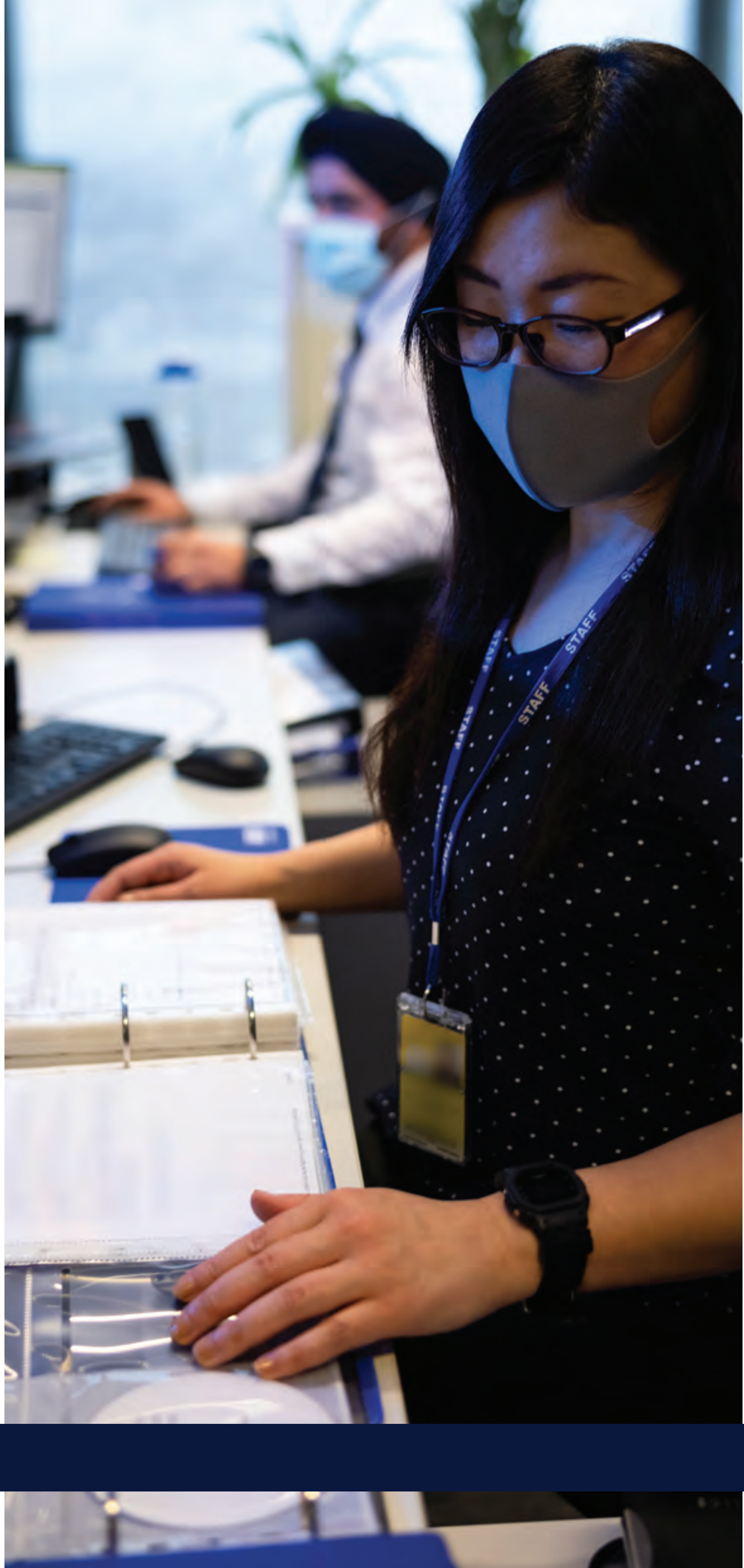
OR VISIT
crimestoppersvic.com.au

If you are a victim of cybercrime...
REPORT IT!

Australian Cyber Security Centre hosts ReportCyber, an online portal for reporting cybercrime incidents, on behalf of Australian law enforcement agencies.

The portal is designed for individuals, businesses, large organisations and government agencies to report a variety of cybercrimes. Reports are referred to the appropriate police agency.

Go to: **cyber.gov.au/report**



References

1 World Economic Forum, 2020, *The Global Risks Report* http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

2 CyberSecurity Ventures, 2020, *Cybercrime to Cost the World $10. Trillion Annually* by 2025, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

3 Department of Home Affairs, December 2020, *Discussion Paper: National Plan to Combat Cybercrime*; Victoria Police, October 2020, Crime Command Review: Technology-Enabled Crime Building Capability.

4 Australian Cyber Security Centre, 2021, *ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021*

5 Australian Cyber Security Centre, 2021, *ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021*

6 ReportCyber

7 ReportCyber

8 Australian Cyber Security Centre, 2021, *ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021*

9 eSafety Commissioner, *Children and Technology-Facilitated Abuse in Domestic and Family Violence Situations*, https://www.esafety.gov.au/about-us/research/children-and-technology-facilitated-abuse-domestic-and-family-violence-situations

10 INTERPOL, 2017, *Global Cybercrime Strategy: Summary, https://www.interpol.int/content/download/5586/file/ Summary_CYBER_Strategy_2017_01_EN%2520LR.pdf*

11 Australian Cyber Security Centre, 2021, *ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021*

12 Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on scams activity 2020*, https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202020%20v2.pdf

13 Department of Home Affairs, December 2020, *Discussion Paper: National Plan to Combat Cybercrime.*

14 Coen Teunissen, Isabella Voce and Russell Smith, 2021, *Estimating the cost of pure cybercrime to Australian individuals.* Statistical Bulletin no. 34. Canberra: Australian Institute of Criminology.

15 Coen Teunissen, Isabella Voce and Russell Smith, 2021, *Estimating the cost of pure cybercrime to Australian individuals.* Statistical Bulletin no. 34. Canberra: Australian Institute of Criminology.

16 Coen Teunissen, Isabella Voce and Russell Smith, 2021, *Estimating the cost of pure cybercrime to Australian individuals.* Statistical Bulletin no. 34. Canberra: Australian Institute of Criminology.

17 Department of Home Affairs, December 2020, *Discussion Paper: National Plan to Combat Cybercrime*

18 Australian Competition & Consumer Commission, 12 February 2021, *Romance Baiting Scams on the Rise*, https://www.accc.gov.au/media-release/romance-baiting-scams-on-the-rise

19 Australian Competition & Consumer Commission, 12 February 2021, *Romance Baiting Scams on the Rise*, https://www.accc.gov.au/media-release/romance-baiting-scams-on-the-rise

20 Australian Competition & Consumer Commission, 12 February 2021, *Romance Baiting Scams on the Rise*, https://www.accc.gov.au/media-release/romance-baiting-scams-on-the-rise

21 Australian Cyber Security Centre, 2021, *ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021*

22 Office of the eSafety Commissioner, October 2017, *Image-Based Abuse, National Survey: Summary Report* (October 2017) https://www.esafety.gov.au/sites/default/files/2019-07/Image-based-abuse-national-survey-summary-report-2017.pdf

23 Office of the eSafety Commissioner, October 2017, *Image-Based Abuse, National Survey: Summary Report* (October 2017) https://www.esafety.gov.au/sites/default/files/2019-07/Image-based-abuse-national-survey-summary-report-2017.pdf

24 eSafety Commissioner, *Deepfake trends and challenges — position statement*, https://www.esafety.gov.au/about-us/tech-trends-and-challenges/deepfakes

VICTORIA POLICE

ACKNOWLEDGEMENT TO TRADITIONAL OWNERS

Victoria Police pays our respect to the traditional owners of lands on which we live and work. We pay our respects to Elders and all Aboriginal and Torres Strait Islander peoples who continue to care for their country, culture and people.

COPYRIGHT

AVAILABILITY STATEMENT

This publication is available in PDF and HTML formats at www.police.vic.gov.au

IMAGERY