SMARTER CYBER INSURANCE

emergence

personal cyber insurance

AN EMERGENCE INSURANCE WHITEPAPER

technology is playing a bigger role in families lives. This exposes them to inherent cyber risks that they haven't faced before

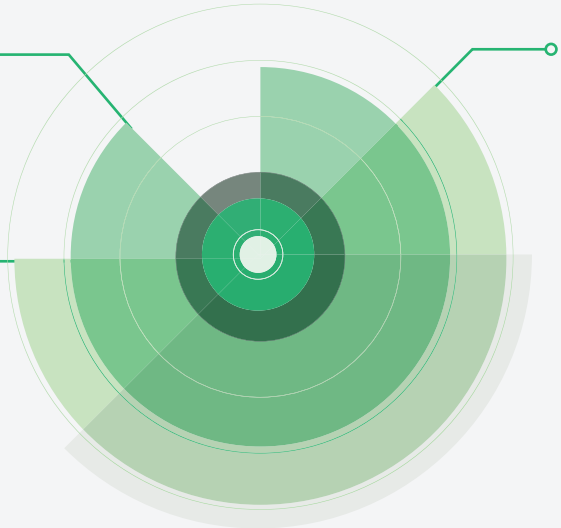
In this whitepaper, we explore the main risks for which cyber insurance provides cover. We also examine some scenarios that can help you understand what personal cyber insurance is, what it covers and the protection it provides families and individuals.

88%

of the Australian population, [22.3m people], use the internet.

71%

of the population use social media.



328 million

Is the estimated annual loss to individuals and small to medium businesses who self-reported to ACSC's cybercrime reporting tool, ReportCyber.

navigating cyberspace

Technology touches everything we do. It improves the way we communicate, collaborate and transact.

As a result, our lives have shifted online, especially since the advent of smart phones. Many of the daily tasks we used to do offline – banking, shopping and even socialising – we now do online. Data shows just how integral the online environment is to us. According to statistics1, 88 per cent of the Australian population, or 22.3 million people, use the internet.

Our dependence on the internet, and the exponential growth of web-enabled devices and social media, has had the effect of making us so much more interconnected. In fact, a whopping 18 million of us[2], or 71 per cent of the population, use social media. But technology also creates new risks. It provides fertile ground for criminal activity and antisocial behaviour.

Research backs this up. From 1 July 2019 to September 2019 this year the ACSC's cybercrime reporting tool, ReportCyber, received almost 14,000 reports[3]. That's an average of around 148 reports a day, or one cybercrime report every 10 minutes. Over this time, individuals and small to medium businesses self-reported financial losses to ReportCyber of more than $890,000 each day, representing an estimated annual loss of approximately $328 million[4].

SO, WHAT IS CYBERCRIME?

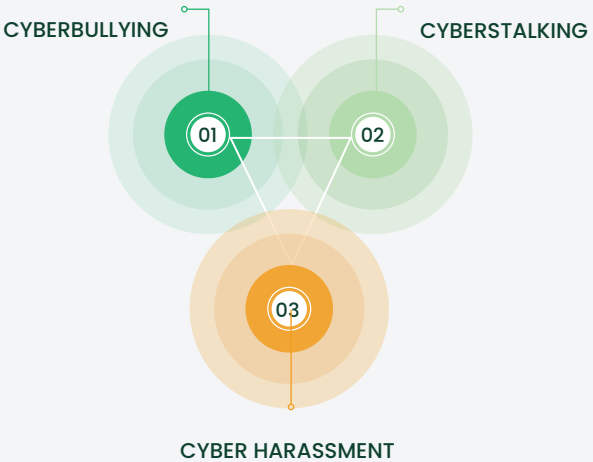
Cybercrime involves the use of computers or other digital devices to perpetrate an offence. It includes:

+ Identity theft
+ Online scams
+ Cyberbullying
+ Financial fraud

We rely on insurance protection for everyday risks we face such as fires or floods, and it was likely truthful that for some, can be susceptible to falling victim to cybercrime. This highlights the need for families and individuals to have personal cyber insurance protection in place, such as the Emergence Personal Cyber Protection insurance offering, which would respond if a cyber event were to occur.

Key features of the Emergence Personal Cyber Insurance product includes cover for the impacts of cyber events and cybercrimes such as:

+ Hacking
+ Malware
+ Viruses
+ Cyber espionage
+ Denial of service attacks
+ Cyber theft
+ Identity theft, and more



Looking beyond the technical side of cyber threats, social media can become a platform for anti-social behaviour. That's why the policy also responds to cyberbullying, cyberstalking and cyber harassment.

Dealing with cyberbullying or cybercrimes like identity theft or sim-jacking can be disruptive and time consuming, so the policy provides a wage replacement benefit if responding to the situation requires unpaid time off work.

1 Australian Internet Statistics, 2020, Prosperity Media. 2 Ibid. Cybercrime in Australia July to September 2019, 2019, Australia Cyber. 4 Ibid.

identity theft is more common than you might think

According to research by the Australian Institute of Criminology (AIC) identity theft affects more people than any other crime, with almost 22 per cent[5] Australian's having been a victim of identity crime at some point in their lives.

Moreover, identity theft can cause real and damaging effects, with the AIC's research indicating ID theft costs each victim $3,696 on average, with identity crimes costing $2.65 billion a year in Australia[6]. In the worst cases, the costs can be much higher, and victims can lose tens or even hundreds of thousands of dollars.

SO, WHAT IS IDENTITY THEFT?

Identity theft involves unauthorised use of someone's personal data such as their name, address, and date of birth and using this information to create a false identity or pose as the victim. The criminal can then use this information to steal money from the person's bank account, take out credit cards in their name or shop online pretending to be the victim.

Criminals use a variety of means to steal people's identity:

Phishing scams: thieves send people emails that look like they come from a reputable source such as a bank and ask people for details such as passwords or any information they can then use to unlawfully access their bank accounts.

Social media data scraping: criminals look for personal information on social media profiles such as their names and addresses and use this information to steal their identity or pretend to be them.

Online scams: criminals can set up fake websites that look like big name retailers. When people 'shop' there the criminals can collect details such as their credit card information and then spend up to the card's limit.

The fallout for the victim can be devastating. It can destroy their credit score; they can be locked out of their bank account and large debts can be incurred in their name. Not to mention the psychological and reputational damage that can happen, with identity theft causing substantial pain and suffering. It can take years and thousands of dollars to re-establish the person's identity.

THE COST OF IDENTITY THEFT

22%

of the population has been a victim of identity crime

ID theft costs each victim

$3,696

on average

5 Trends & Issues in crime and criminal justice: The identity theft response system, 2020, Australian Institute of Criminology. 6 Ibid

WHAT YOU CAN DO TO PREVENT IDENTITY THEFT:

+ Avoid publishing personal information such as your date of birth and address on social media platforms.
+ Educate yourself and your family about what phishing emails look like.
+ Keep a close eye on your bank account.
+ Regularly check your credit file.
+ Avoid using passwords that can be guessed easily such as your birth date.
+ Better yet, use a password manager.
+ Take care when giving out your personal information.

SCENARIO ONE

THE POWER OF INSURANCE WHEN CRIMINALS STEAL AN IDENTITY

Fred was an avid user of social media platforms. In fact, he had a few that were constantly kept up-to-date with everything that was happening in his life. Unfortunately, he shared too much information and had poor security for protection.

Thieves accessed his social media accounts and collected enough information to be able to steal Fred's identity.

The thieves illegally accessed Fred's bank account and transferred $25,000 out of his account.

When Fred next checked his bank account, he was devastated to find it had been drained of funds. Fred was also worried about what other damage could arise from having his identity stolen.

Personal cyber insurance could provide a solution. If Fred had an Emergence policy, we would first collect all the evidence, conduct forensics, and work with his bank to reinstate Fred's accounts.

We would also support Fred to make statements to police and work with credit reporting bureaus to repair Fred's credit report and score.

We would also cover wages that were lost as a result of Fred needing to take time off work to repair his identity.

While this situation is extremely stressful and shocking, we could assist the victim to recover and move forward.

the rising risks of fraud and online scams

The latest data[7] from the Australian Competition and Consumer Commission (ACCC) indicates Australians lost $634 million in 2019 from online scams and reported 353,000 scam incidents throughout the year. This huge volume of losses shows how important it is for households to protect themselves from scams.

As the large volume of online scams indicates, most involve criminals pretending to be something or someone they are not. They often use the internet to collect personal information and use this to harm the victim.

THERE ARE MANY DIFFERENT TYPES OF ONLINE SCAMS:

Phishing scams, which involve criminals sending an email from a trusted organisation like a bank and coercing the account holder to give them personal information by clicking on link to a web site that looks like it's a reputable bank's site.

Ransomware, which involves criminals installing malware on a computer, locking the machine down and demanding a ransom payment to give the information back. These scammers may also threaten to release personal information on the internet unless a ransom is paid.

HOW TO AVOID BEING DEFRAUDED ONLINE:

+ Never click on pop-up windows.
+ Keep household virus software up-to-date.
+ Be educated about common and new scams by going to the ACCC's Scamwatch site.
+ Look for suspicious phishing emails.

WHAT TO DO IF YOU'RE THE VICTIM OF A SCAM:

It's easy to feel embarrassed if fraudsters have successfully attacked you. Don't be. These are sophisticated criminals with devious methods. So it's important to act and inform the right sources if you have been duped or tricked into doing something you wouldn't normally have done:

+ Tell your bank and other relevant organisations such as any social media or dating apps.
+ Report the scam to the ACCC's Scamwatch site.
+ Change all your passwords.
+ Tell your family or friends and ask for their support.
+ If you have a cyber policy, contact Emergence.

IN 2023 AUSTRALIAN'S LOST

$3.1 billion

lost in 2022 from online scams in Australia.

239,237

scam reports were received during the year.

[7] Targeting scams 2019, 2020, The Australian Competition and Consumer Commission

DON'T BE FOOLED BY POP-UP WINDOWS

Pop-up scams are some of the most common types of online fraud. These involve a notice, often from a trusted, reputable company, popping up when you are on a web site.

These windows may encourage you to click on a link and, once you have done that, lock down your computer. They frequently include a number to call. Once victims call the number they are asked to provide their bank account and other details.

Don't be fooled. These fraudsters want victims to hand over their information so they can raid their bank accounts and steal their identity.

COVID-19 SCAMS THE LATEST FRAUD FRONTIER

Scamwatch has identified more than 3,500 coronavirus scams since the start of the pandemic, which have resulted in $2.2 million[8] in losses so far. So be very wary of any emails or text messages from government agencies, banks, travel agents, insurers and telcos about COVID-19.

Many of the scams involve messages that look like they are from the federal government requesting personal information to help you get financial support or give you early access to your superannuation.

The government is not offering this service. These are messages from scammers who want access to your personal information so they can take advantage of you.

The best way to find information from the government is to log-in to your myGov account. Don't ever give your login information to anyone who calls and asks for it or emails you.

[8] Current COVID-19 scams, 2020, Scamwatch, Australian Competition & Consumer Commission

SCENARIO TWO

RANSOMWARE

Paul opened his email one day to find a message that looked like it was from a friend. It informed him his friend had exciting news to share and invited him to click on a link to view a few pictures and a special announcement. Curious to know the news, he clicked. But the message wasn't from his friend. It was from thieves, who downloaded malware that encrypted Paul's entire hard drive, preventing access to any files whatsoever. The hackers then demanded a ransom of .1 Bitcoins ($1,500) to provide the decryption key, with the price doubling if he didn't pay within 48 hours. Paul had heard of Bitcoin but he had never acquired any and didn't really know how to. The ransom note very helpfully included instructions on just what to do. Seemed straightforward enough. It was a lot of money, and he detested the idea of paying the ransom, but what option did he have? He certainly didn't want to lose his data, and the price would soon double.

If Paul had cyber insurance, he would have contacted us as soon as he discovered he was a victim of ransomware. Our responders would establish whether data could safely be restored from any existing backups. They would check his system to assure malware was removed, reinstall software including replacement licenses as necessary, and restore his data. They would also provide Paul with advice on measures he could take to make his data more secure and to reduce the likelihood of ransomware, including learning to recognise common social engineering ploys.

If Paul's data could not be restored from backups, experts could be engaged to determine the type of ransomware, whether decryption was possible, the reputation and of the hackers, whether the decryption key was likely to work, etc. If paying the ransom became the last and only resort, our ransomware specialists would manage communications with the crooks, test the decryption keys on sample data, and would handle the Bitcoin negotiations and any payment.

supporting families

Cyberbullying is increasingly commonplace, especially among young people who may not have enough awareness about the harm their actions cause when they bully and harass their peers online. A study conducted in 2019 by McCrindle shows 24 per cent of all bullying involves social media and text messages. Worryingly, cyber threats start at a very young age and continue throughout our lives.

Cyberbullying involves the misuse of power with technology. Examples include threatening to publish explicit photos online without your authorisation, encouraging others to bully or ignoring, vilifying and spreading rumours on social media.

This is a serious issue and in many cases a crime. So, if you or someone in your family is experiencing cyber bulling:

+ Do not bully the other person back.
+ Tell them to stop.
+ Tell your friends or family what is happening.
+ Report serious incidences, such as threats to publish intimate photos without your approval, to the authorities.
+ Look at important government websites such as the Australian eSafety commissioner – www.esafety.gov.au.
+ Kidshelpline.com.au also is a great resource to get support.

[9] Make bullying history, 2019, McCrindle Research

SCENARIO THREE

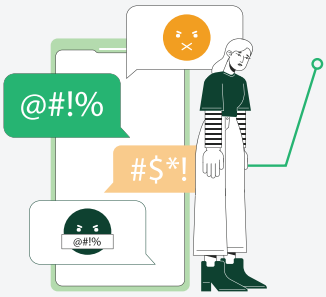
WHEN CYBERBULLYING STRIKES

Lucy, a 12-year-old girl, was bullied at school because of a disability. When she got home, the bullies continued their tirade against her in the online world. They taunted her on social media sites and sent vile direct messages to her. Worse, the bullies posted photos of Lucy and mocked her disability on popular social media forums.

This instance of cyberbullying would be covered by Lucy's parents' personal cyber insurance policy. After lodging a cyberbullying report with the Australian eSafety Commissioner, they would contact Emergence and we could provide a range of different support services.

A cyber security coach would provide guidance to Lucy and her family to reduce the risk of her being bullied online or in person again. Additionally, the family would be referred to specialist counsellors who could support them in a holistic manner.

KEYBOARD WARRIORS



24%

of all bullying involves social media and texts

CYBERSTALKING

cyberstalking a silent threat

Cyberstalking, like cyberbullying, is another form of targeted antisocial behaviour that has become all too frequent. Like cyberbullying, various methods can be used. It is most common to think of it as stalking that takes place online on social media platforms, forums, blogs, and email. Cyberstalking can also take the form of the individuals' location being tracked by using technology.

Sally has had repeated advances by an old boyfriend to get back together. Sally politely continued to decline the chance to get back together. However, the old boyfriend didn't stop. When he knew there was no chance to get back together, his actions turned from cyberstalking to an invasive and deliberate attempt to undermine her reputation.

The ex-boyfriend paid a cybercriminal to hack into Sally's computer and find some explicit photos of her. He then posts them on an adult website, tracks Sally down on a popular social media site and contacts her, sending her the photos he has uploaded to the internet. At the same time, he sends Sally's employer, friends and family the same photos. This is a heinous example of harmful publication, and unfortunately an all-too-frequent occurrence.

Sally begs for the removal of the photos from the site to which he's posted them. The ex-boyfriend responds by telling Sally she will need to pay him to take the photos down or resume their previous relationship. Sally is terrified of the ramifications that his actions might have on her career and put it in jeopardy – not to mention the affect it may have on her personal life.

During this distressing time, personal cyber insurance could provide Sally with legal advice about her options to mount a case against Jake in relation to the harassment she experienced and in response to harmful publication of the photos.

Emergence could also help to arrange for the removal of information online to protect Sally's reputation and assist her to document the details of the site through which Jake released the information, as well as all the people to which he sent photos. We could assist Sally to block Jake online and report him to social media providers.

GROWING NUMBER OF VICTIMS

According to the Australian Bureau of Statistics[10], around...

1.6 million

women and 587,00, men have experienced an episode of stalking since the age of 15 in Australia.

[10] Personal Safety Survey, 2016, Australian Bureau of Statistics

SCENARIO FIVE

FINANCIAL SCAMMERS

everyone's fair game

Amanda opened her superannuation account to check it, fully expecting to find the healthy balance she was used to seeing. But she did a double take, so shocked was she to find it had been drained. She had been the victim of a keylogging scam through which the fraudsters had hacked into her computer to record the keystrokes she used when she had previously opened her account. They used this information to log into her account and steal her funds.

If Amanda had personal cyber insurance, the first thing to do is to alert her superannuation fund and report the incident to the Australian Cyber Security Centre or the police. She would document all the necessary information and preserve any evidence that will help in dealing with the issue. Emergence would then assist Amanda in the necessary steps to resolve the situation and provide necessary support. Her financial institution would attempt to recover the stolen funds, sadly often with little success as the thieves will typically have immediately transferred the money out of the fund's network. Nevertheless, the fund is likely to undertake its own investigation and apply a higher level of security to Amanda's account and any other accounts the criminals have targeted.

We advise victims such as Amanda to reset all passwords and apply two-factor authentication to online accounts. We would also pay for a forensic specialist to check Amanda's internet-enabled devices to ensure the thieves have not compromised them and used her information to gain access to any of her other accounts.

We would assist Amanda in her efforts to recover the funds. If they prove to be unrecoverable, Amanda could submit a claim for her personal financial loss. Additionally, would be able to use surveillance across the dark web to check if her personal details have been shared with other fraudsters. For peace of mind and early warning, the policy provides for credit and identity monitoring for up to 12 months.

THESE SCENARIOS HIGHLIGHT THAT CYBER CRIMINALS CAN CAUSE UNTOLD DAMAGE TO ALMOST EVERY AREA OF OUR LIVES.

This paper has discussed some of the steps you can take to help keep you and your family safe, but even the best of efforts is no guarantee. Criminals keep advancing and refining their techniques. One of the best ways to mitigate this ongoing risk is by taking out personal cyber insurance cover.

The Emergence Personal Cyber Protection Insurance offering, provides wide-ranging protection in response to threats such as online scammers, cyber criminals and fraudsters. In an increasingly connected world, it's a sound way to give you and your family peace of mind knowing your insurance policy will respond if an event were to occur.

WHY INSURANCE MATTERS

The ACCC's research[11] shows investment scams cost Australians $126 million in 2019 alone, a 59 per cent increase compared to the previous year. Many of these scams involve technology and the criminals behind them are becoming very sophisticated.

For instance, be very wary if you receive an email from a celebrity selling a financial product. Chances are this is a hoax. More recently, scammers have used popular online games and messaging services to entice people into get-rich-quick cryptocurrency scams.

[11] Targeting scams 2019, 2020, Australian Competition and Consumer Commission

REDUCING THE RISK

TAKE STEPS TO REDUCE THE RISK OF SCAMMERS FINANCIALLY DEFRAUDING YOU ONLINE:

SAFE INVESTING

When you're investing, make sure the business and its advisers are licensed by regulators such as the Australian Securities and Investments Commission and the Australian Prudential Regulation Authority.

PIN SECURITY

Never give your PIN Number to anyone.

STRICTLY GIVE KNOWINGLY

Only donate to registered charities.

NEXT STEPS

WHAT TO DO IF YOU ARE A VICTIM OF ONLINE FINANCIAL FRAUD:

REPORT IMMEDIATELY

Report the incident to the Australian Cyber Security Centre (ACSC) or the police.

CONTACT YOUR BANK

Inform your bank.

EMERGENCE HOTLINE

Call Emergence if you have a cyber policy with us.

1300 799 562

ABOUT EMERGENCE

Australia's award-winning cyber insurance

Emergence is your award-winning underwriting agency, focused exclusively on providing flexible, innovative insurance solutions to help protect Australian businesses and families as cyber risks become increasingly prevalent.

As a pioneer of cyber cover, Emergence are experts in global cyber risk protection. We specialise in identifying and quantifying new and emerging cyber security risks and creating tailored insurance products to respond effectively to them.

Our Personal Cyber Insurance product is designed to combat the devastating harm and loss that cyber-crime can cause. Policies respond to a range of events including identity theft, personal financial loss, invasion of privacy, denial of service attacks and much more.

Cyber crime does not discriminate and is more rife than ever. The impacts of cyber crime can be devastating and difficult to recover from.

At Emergence, we believe the case for protecting you and your family is clear. Personal cyber insurance is a valuable investment. Thinking proactively about the safeguards you have in place should be a key component of everyone's cyber risk mitigation strategy, and arranging insurance will provide security and peace of mind that no one living in the digital world should underestimate.

AUSTRALIA'S AWARD-WINNING CYBER INSURANCE

be at your best with emergence

To find out how a personal cyber policy can protect you and your family visit our website. If you've experienced a cyber incident, please call our emergency hotline 24/7, 365 days a year.

emergence

cyber emergency 1300 799 562

emergenceinsurance.com.au