ourcommunity.com.au
Where not-for-profits go for help

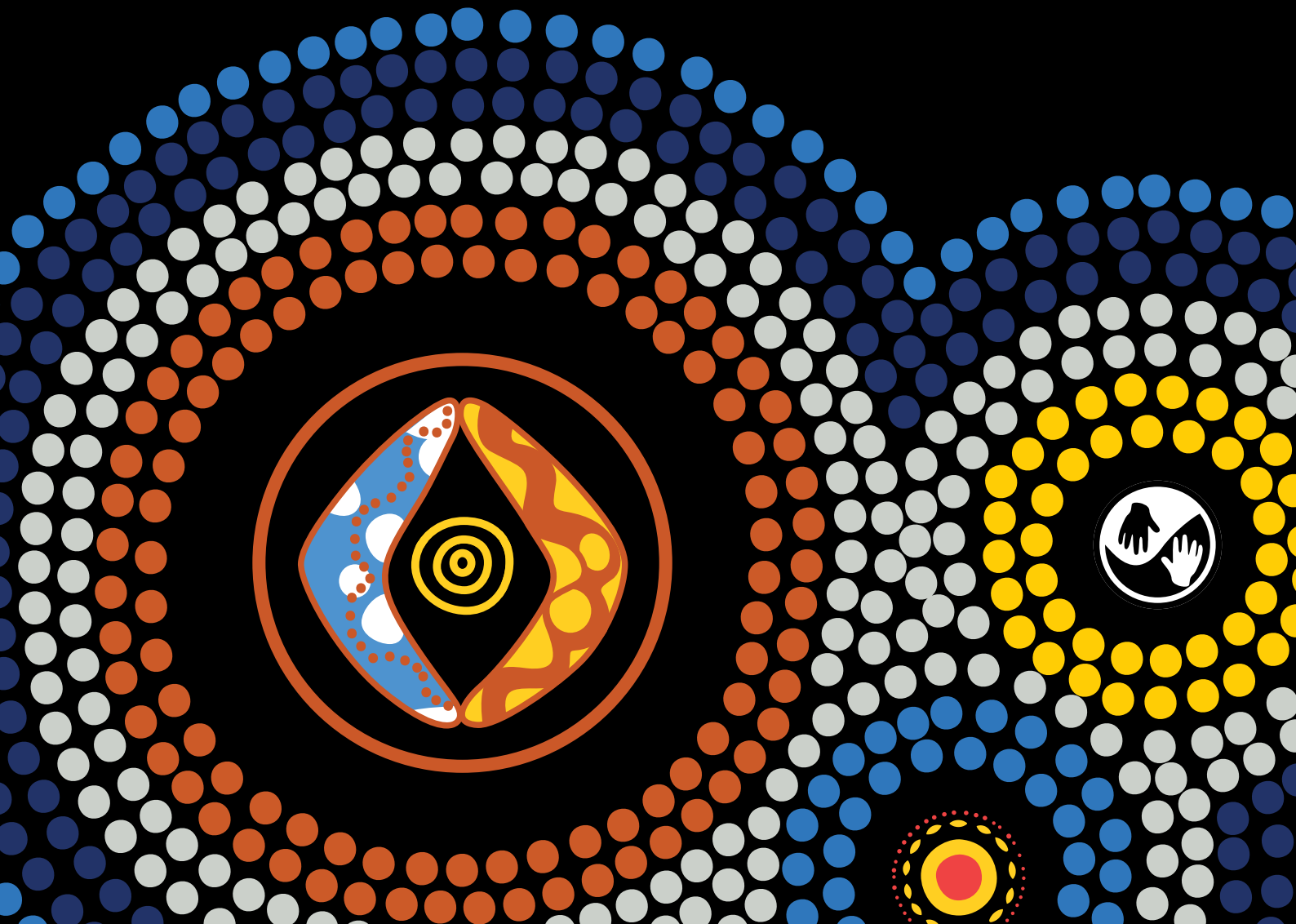
INSTITUTE OF COMMUNITY DIRECTORS AUSTRALIA
Knowledge Connections Credentials

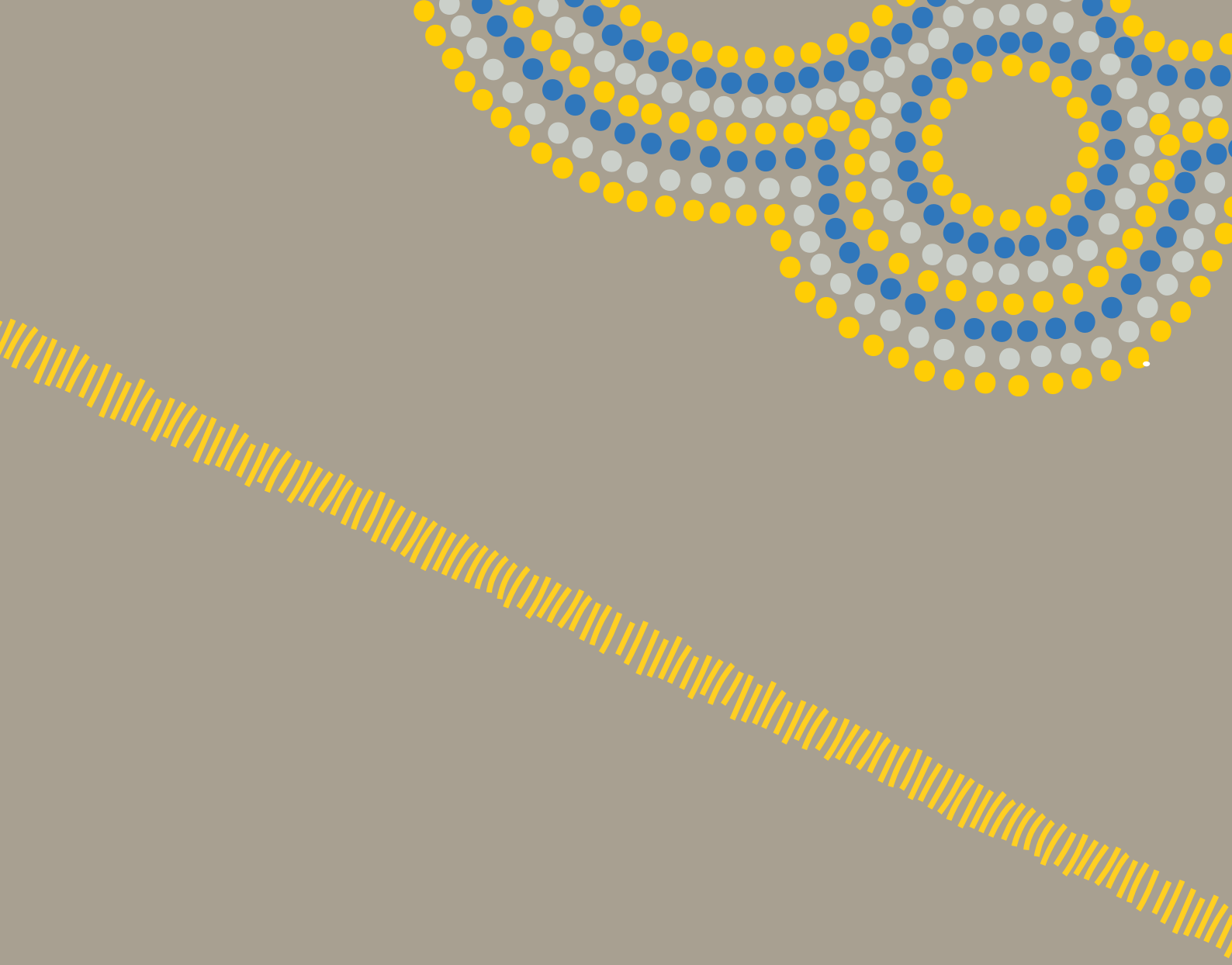
Commonwealth Bank

Indigenous Business Banking

Cyber Safety and Fraud Prevention

A practical guide for Indigenous businesses, organisations and enterprises





Cyber Safety and Fraud Prevention: A practical guide for Indigenous businesses, organisations and enterprises

Published by Our Community Pty Ltd and Commonwealth Bank of Australia.

Our Community Pty Ltd
PO Box 354
North Melbourne VIC 3051
Australia

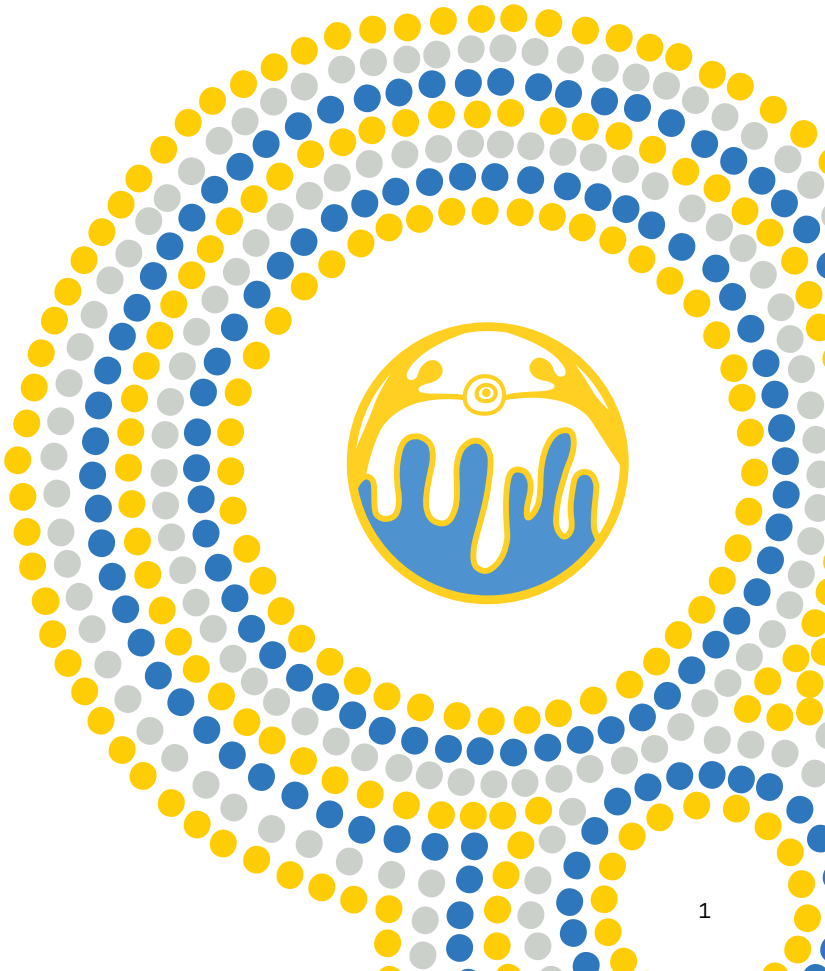
Please note:

First published in February 2021.

Indigenous Business Banking

Cyber Safety and Fraud Prevention

A practical guide for Indigenous businesses, organisations and enterprises



COMMUNITY SMART

This guide is part of the CommunitySmart program, a national financial literacy program developed by the Commonwealth Bank and the Institute of Community Directors Australia (part of the Our Community group).

Good governance and strong financial management are essential to the strength and sustainability of all businesses* and organisations.**

Through CommunitySmart, we are working to help strengthen governance and financial management for Indigenous Australians, Indigenous organisations, their staff and their board members.

* Business in this guide refers to businesses, enterprises, Unincorporated associations, Incorporated associations, Company Limited by Guarantee, Cooperative, Charitable, Parliament, Indigenous, Native Title Representative Bodies and Land Councils.

** Organisation in this guide refers to businesses, enterprises, associations, Incorporated, Company, Cooperative, Charitable trusts, Organisations formed by Royal Charter or by a Special Act of Parliament, Indigenous Corporations, Native Title Representative Bodies and Land Councils.

A practical guide to staying safe online

It is wonderful to see the steady increase in Indigenous-owned and run corporations, with almost 3,198 corporations registered under the CATSI Act as at 30 June 2019 (an increase of around 5% on the previous year).

This is a much-welcomed indicator of how Aboriginal and Torres Strait Islander peoples are continuing to make inroads towards greater economic participation and financial independence.

Today businesses rely on the internet and digital engagement, which continues to rapidly transform our world. It is an integral part of how we do business, how we communicate and how we interact with each other.

It is easy to forget that the internet is not a risk-free environment. Cyber-crime continues to rise at a rapid rate each year. Online criminals are getting better and smarter at stealing or making use of your business or your customer's data, accessing your financial systems and disrupting your business activities. If the worst happens, the losses can be significant. Your business or organisation's reputation could be tarnished, your day-to-day operations interrupted or even stopped.

Fortunately, you can stay safe online without a large outlay of money and resources. Some measures are easy, requiring little more than a regular review of your business operations. Other measures involve investing in computer software, hardware, computer programs and specialist expertise. And many risks can be reduced with a small investment in educating people within your business or organisation.

The challenge is understanding what you are trying to protect your business from and taking a risk-based approach. This means assessing how your business and your staff members (if you have any) operate or transact online, and understanding the associated risks.

And that is where this Guide comes in. It has been designed as part of the Community Smart program, produced jointly by Commonwealth Bank and the Institute of Community Directors Australia.

We have created this Guide as a starting point to help you, your business and your employees stay safe in today's online world.

As always, we extend an acknowledgment of thanks to the Elders, Indigenous business leaders and community members who continue to give so generously of their time, their knowledge and their insights into the complexities Indigenous businesses and organisations face, and for their support in the development of this Guide.

A special note of thanks to Commonwealth Bank's Cyber Security team for their support and assistance in producing this Guide as we help our customers combat the rapidly evolving and sophisticated world of cyber crime.

And, as always, to CommBank's Indigenous Advisory Council, our thanks for your guidance and support as we continue to challenge ourselves to be a better, simpler bank that supports all Australians.

We hope you find the information in this Guide useful and that it provides you with an outline of the steps you and your teams can take to keep your business – whether large or small – safe in today's online world.

We continue to look forward to working alongside our First Nation Peoples as we develop additional guides and resources to support the growing needs of this valuable sector.

Regards

Noel Prakash
Head of Indigenous Business Banking
Commonwealth Bank

Denis Moriarty
Group Managing Director
Our Community

Contents

1. Cyber security: why should we be concerned?

No matter how large or small your business, organisation or enterprise, everyone needs to be aware of fraud.

Today, the internet reaches into almost every device or computer on every desk in every office and in every home. It is possible to reach nearly every person on earth instantly via the internet. And, if we can reach them, they can reach us.

While the online world presents opportunities for cyber criminals, there are steps you can take to help keep you, your business, your organisation and your enterprise safe online.

Awareness is the key. If everyone in your organisation is alert to the dangers of online fraud, you are in a much stronger position to control and manage it.

In this Guide, we explore how you can help prevent fraud attempts that come from outside of your organisation. In particular, how you can reduce the opportunities for cyber criminals to access your organisation using your computers and your internet connections. The aim is to give you an overview of what cyber problems you might face, and some of the solutions you might be able to put in place to address them.

2. How big is the risk?

Cyber security is a real problem for businesses, organisations and enterprises of all types and of all sizes.

There are international cyber criminal gangs with the expertise and the networks to try to exploit large multi-national companies, and there are small backyard operators who will try to attack smaller businesses and enterprises.

Large organisations often spend millions on their cyber security - some even hire their own hackers to test their IT security.

If Government departments can be breached (Australian Bureau of Meteorology's http://tinyurl.com/z7v5twb, and the Australian Bureau of Statistics in 2016) your business or organisation can be too.

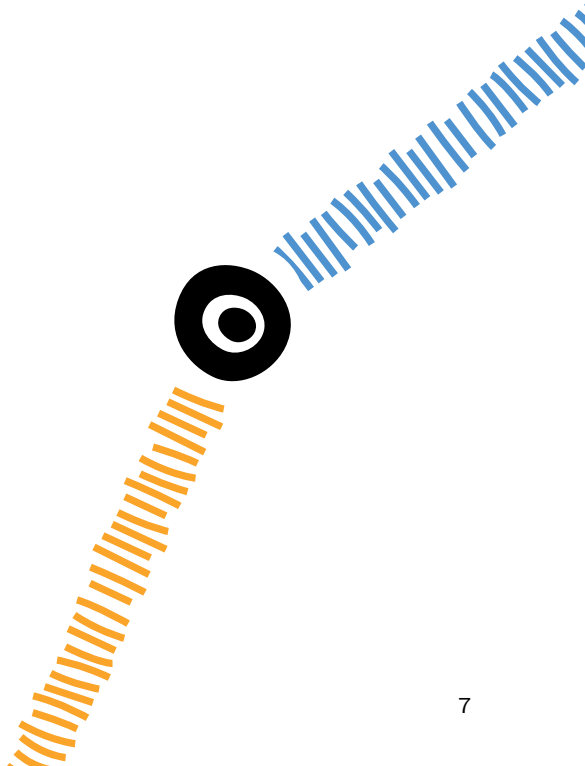
Cyber criminals often look for the weakest link to exploit and may then move on to more highly valued targets.

The cyber attacker may not even be interested in you or your business, but that does not mean they cannot hurt your business or you. A computer compromised or attacked by malicious software (malware) has the potential to be invisibly inserted into networks of other compromised internet-connected computers, known as botnets. Botnets are used to send spam, steal information, distribute malware and conduct large-scale attacks which can bring down networks simply by swamping or overloading them with traffic or messages.

Your computers may be pulled into a botnet network without you even knowing it - you may simply notice your computer is running a little slower than usual, but it can cause big problems for your business.

One botnet called Rustock, busted in 2011, consisted of approximately one million infected computers networked together to send 30 billion spam emails a day. When it was taken down, global spam volumes instantly dropped by 30%. You do not want your business or organisation to enable that kind of abuse.

And it is not just money you can lose to cyber crime. Even if you take all possible precautions, your organisation's reputation can still be affected by criminal elements. The better your reputation, the more likely it is that someone will start sending emails out in your name with your logo pretending to be you and trying to get access to other networks. There is nothing much you can do about this except to keep an eye out for frauds and send out alerts to all your contacts as soon as you detect an imposter.



Never too big or too small to be a target

Being a small business or organisation is no protection from online threats. In April 2017, Edmodo, an educational technology company had 77 million user accounts hacked. (see https://www.the74million.org/article/77-million-edmodo-users-are-hacked-as-widespread-cyber-attacks-hit-the-ed-tech-world/).

In these cases and most others, authorities are powerless to act. The lesson? Be prepared.

Cyber crimes by the numbers

$29 billion Estimated cost of cyber crimes to Australian businesses

$15.8 million Losses due to cyber threats that steal personal information

$9.2 million Malware detections recorded by Australian businesses

$276,323 Average cost of cyber crime to a business

23 to 51 Days to resolve an attack

1 of 3 Aussie adults affected by cyber crime

Sources: Department of Home Affairs, Stay Smart Online Australia, ACCC Scamwatch 2019, and CIO Magazine 2019

3. Cyber risks at a glance

Computer hijacking

A computer hijacking occurs when an attacker takes control of your device, a computer, or a component of a computer, and exploits it in some way – by using it to host illegal material such as terrorist messages, for example, or by stealing the information stored on it. Cyber criminals launch their attack by remote control, and you will not necessarily even know it is happening.

Cyber impersonation

A criminal who sends emails pretending to come from your organisation can do a lot of damage to your reputation. Cyber impersonation also covers people who post on social media, for example on Twitter, Facebook, LinkedIn, and so on, under a false name, or the name of your organisation, or your CEO.

Data or intellectual property theft

Data theft involves someone walking away with the contents of your files. This can happen via website hacking, email hacking, online account hacking, computer hijacking or phishing (see page 10).

Email hacking

If your email account is hacked, it means somebody gains unauthorised access to your email account. They can then impersonate you (by sending out emails in your name) or get access to all the information stored in any of your emails. This could even lead to blackmail attempts for example, using sensitive information contained in emails to extort money from you in exchange for keeping quiet about it.

Hacktivism

A hacktivist is a person who gains unauthorised access to computer files or networks in order to further social or political ends, rather than to extort money.

Online account hacking

If your business uses Facebook, Twitter, Instagram, SurveyMonkey, Formstack, Mailchimp, online banking, or any online services – then you are vulnerable to having your account hacked if you ignore the usual precautions such as using strong, secure passwords. A hacker can steal your information, your money or your identity, and could destroy your good reputation.

Privacy breach

Privacy breaches occur when someone walks away with personal data about you or your clients. This can easily occur if data isn't well stored or looked after, for example leaving a USB or a portable device on a train. It can also happen via website hacking, email hacking, online account hacking, computer hijacking or phishing, outlined above.

Website hacking

This is when an unauthorised party takes control of your website. The cyber attacker could be anyone from a bored teenager who replaces the text on your homepage, to a disgruntled former employee who posts defamatory comments, to a criminal gang that gets into your online system and steals your financial information so that they can transfer all your funds.

Ransomware

Ransomware refers to malicious computer programs that deny you access to your business or organisation's own data until you pay money, or a ransom, to the attackers. They do this by encrypting or locking files. Upon payment, they provide a decryption key to unlock the files.

Stealing your money

If a cyber attacker finds their way into your important accounts or systems, they can cause significant financial damage - through targeted scams or banking trojans (see below for more details) designed to steal your credit card or banking details.

Trojan horse

A Trojan horse is any malicious computer program that misleads a user about its true purpose in order to hack into their computer. The term comes from the Ancient Greek story of the wooden horse that was used to smuggle Greek troops into the city of Troy.

Virus/malware

A computer virus/malware is a malicious program that loads itself onto your computer without you knowing about it (via the internet or an infected USB drive, for example). The virus/malware then starts to replicate itself and do damage. Different computer viruses/malware have different symptoms and spread at different speeds – some make themselves known immediately (for example, by damaging all your files or using up all your computer's memory), while others are programmed to remain dormant/hidden for a period and then start replicating and doing damage.

Phishing

Phishing is a type of email fraud in which the offender sends out emails that appear to come from a legitimate service or reputable company, such as a bank or an email service provider. These emails aim to get recipients into revealing confidential information that the offender can then use for their financial advantage – for example, your organisation's online banking log-in details and passwords.

An example of a fraudulent phishing email sent by a cyber attacker:

From: Customer Service - <PWIURNFLKEUCNFGOC@wi29d8ckdsogs82ons.es>
Sent: Thursday, August 20, 2020 11:17:19 AM
Subject: COMMBANK : Your account has been locked!

Commonwealth Bank

Dear Customer,

We noticed an attempt to sign in to your account from an unregistered device in australia.

For your security, we have disabled access to your account to prevent unauthorised use. We require you to complete our account verification process in order to restore access please click the link below.

Restore Access

Best regards,

CommBank

To ensure that CommBank emails reach your inbox, please add **no-reply@commbank.wi29d8ckdsogs82ons.es** to your email safe list.

4. Who is responsible for cyber security?

Cyber security is an organisation-wide requirement.

It is natural to want to hand over responsibility for all elements of a cyber security program – risk management and mitigation, resource allocation decisions, policy enforcement and so on – to a senior manager who has the knowledge and authority to understand it all. However, whether you are a small business or a large land council that is not going to be enough.

If your organisation is large enough to have an IT department, they are going to be an important part of the solution. An effective IT person or department will help ensure your systems are robust and can translate complex technical information about cyber security risks into clear advice.

However, a wider and more inclusive hands-on approach to staying safe and secure online is much more effective than dropping all the responsibility onto one person.

Every employee needs to understand how to protect data, how to use the internet securely and how to use email safely. Little things can make a big difference when it comes to helping control cyber security.

The following is a real life example of cyber crime in action involving an Indigenous business:

We were warned, especially during Covid, that cyber criminals had become more sophisticated, were attacking more and were using different methods including using text messages.

Our business became the victim of a $140,000 redirection fraud in 2020. The cyber criminals hacked a supplier's email and changed their bank account details. We thought we were paying our supplier when we were actually sending money to the cyber criminals.

Thankfully our insurance covered the $140,000 we had lost in the scam, but our team was left gutted by the experience.

We also had a malware attack a few years ago that locked our server and we had to pay bitcoins to have it unlocked.

The lesson we learnt is that criminal activity is everywhere including online and you need to make sure you've protected your business and keep your staff trained on what to look out for.

5. Who is out to get you?

Cyber criminals can be anyone. It might be disgruntled former employees, your competitors, bored teenagers to overseas governments. The threats may even come from within your organisation.

What they all have in common is that they are opportunistic, looking to harm you or your business, and some of them have had a lot of practice at doing so.

Employees

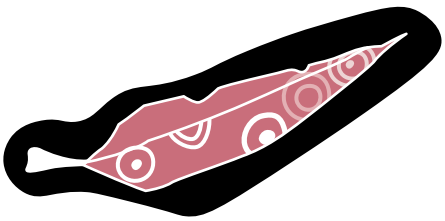
Employees can be involved in almost any security threat, whether through ignorance, negligence or carelessness. Very occasionally, they may be the criminals themselves, taking advantage of their local knowledge and their access privileges to steal money and data from you. Your security systems have to be able to deal with or compensate for employees or trusted volunteers, as well as outside elements.

Amateur hackers and vandals

Amateur hackers and vandals account for a large proportion of internet attacks. Their attacks are usually crimes of opportunity.

Amateur hackers continually scan the internet looking for well-known security holes that have not been properly plugged. Web servers and electronic mail are their favourite targets. Some hackers access systems by exploiting security flaws in software, others by stealing or guessing log-in credentials or by fooling people into sharing them. Once they find a weakness they will exploit it to plant viruses and Trojan horses (see page 10) or to use the resources of your systems for their own purposes. If they do not find an obvious weakness they will probably move on to an easier target.

Some hackers just want to see things break. Some may have a grudge against your business or organisation. You may be the target of people who are willing to put considerable time and effort into bringing down your operations by taking over your website, corrupting your data, or exposing your secrets. This is known as hacktivism. If you have any reason to expect anything like this, increase your threat rating to “elevated” and review your system defences more regularly.



Criminal hackers and saboteurs

The skill of these types of attackers is medium to high as they are likely to be trained in the use of the latest hacker techniques. The attacks are well planned and are based on any weaknesses discovered that will allow control or foothold into an organisation's computers.

Criminals also have their own infrastructure. If they do find personal information in your data systems, they know who and where to sell it to get some gain.

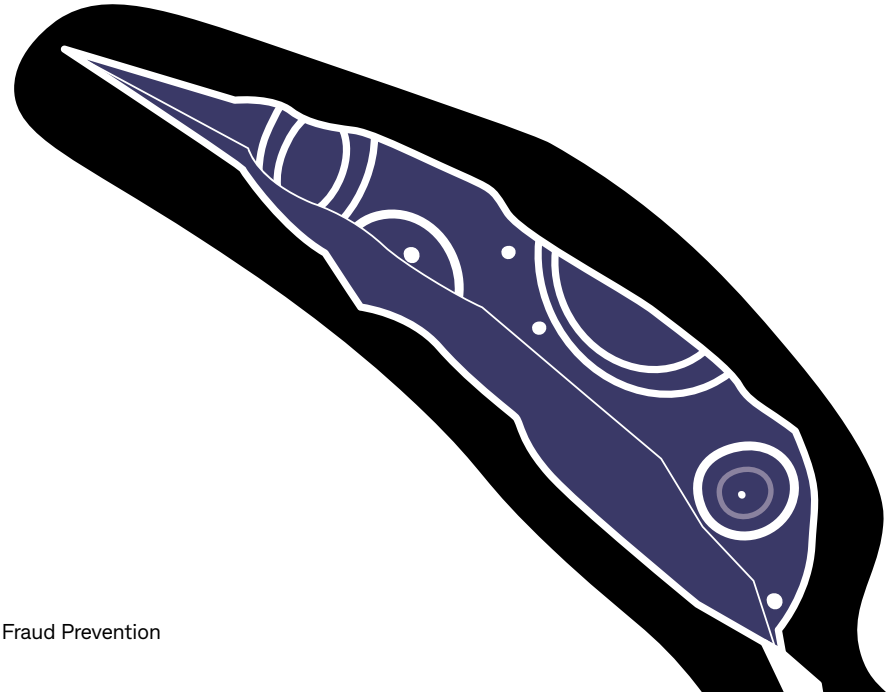
There have been instances of attackers accessing data on internal networks, encrypting it, and demanding a ransom in untraceable bitcoins (a really complex way of demanding untraceable payment) in return for the decryption key. In early 2016, a US hospital paid hackers 40 bitcoins, then worth around AU$20,000, for a decryption key to unlock its hijacked medical records system. (You can read the full story here: http://tinyurl.com/j8wdly5.)

Given the complexity and interconnectedness of our computer systems, it is simply impossible to make any system water tight or 100% secure. Even if your systems themselves are perfect, there is still a human element involved – people can and will make mistakes.

You might have heard the joke about the two men whose camp is attacked by a bear. One man pauses to do up his shoelaces. The second shouts out, "What are you doing! You know you can't outrun a bear!" The second camper replies, "I don't have to outrun the bear. I just have to outrun you."

The aim of cyber security measures is to make your systems secure enough that hackers will not bother with you because the effort is too great. The cyber hacker will almost always go for the easiest target.

Attacks by amateur hackers and vandals are usually crimes of opportunity.



6. What is vulnerable to a cyber attack?

Physical equipment is fairly easy to protect. The data on devices is often far more valuable than the actual equipment. The technology and information systems of a business or an organisation are typically made up of the following components:

Computer hardware

Including email, file, web and application servers, desktop computers, laptops, smartphones and tablets.

System software

Including operating systems (such as iOS and Windows), database management systems (like Microsoft Access, FileMaker Pro, MySQL and Oracle), communications protocols (your email and internet settings), and back-up and restore software.

Application software

Including commercial off-the-shelf software packages (Word, Excel and MYOB, Xero for example) and custom software applications you have commissioned specifically for your business or organisation.

Communications network hardware and software

Including routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

Digital assets

Including administrative data, identity data, client credit card/bank account data and intellectual property.

Digital assets audit

Putting a cyber security plan in place starts by understanding what it is you are trying to protect. You need to identify what assets you have and what level of protection they might need.

For example, personal and credit card details from your client database need to be strongly protected. Your corporate logo, while an important asset, is probably already widely available in the public domain. You do not need to put the same extremely strong protection around access to your brand or logo as you do around confidential personal client data.

Once you explore what data needs to be protected you will find that not all data is equally important and not all staff members have the same access needs. For example, everyone may need to have access to company logos, but only a select number of people will need to edit them.

Consider

How valuable are your assets, and how well are they protected? You can use this tool to conduct a digital asset audit.

Data	Value	Vulnerability	Protection method	Responsibility of
Administrative data				
Payroll records	High	Medium	Password protected; bank details encrypted; access limited to Director/CEO and relevant staff	Treasurer/finance manager or finance department.
Transaction records	High	Medium		
Program records	High	Medium		
Identity data				
Staff records	High	Medium	Password protected; data encrypted; access limited to Director/CEO and relevant staff	HR section
Volunteer/employee records	Medium	High		CEO/Director
Supplier details / Fundraising database	High	Medium	Password protected; credit card numbers encrypted; access limited to CEO and relevant staff	CEO/Director
Member database	Medium	Medium		
Client database	High	High	Password protected; data encrypted; access limited to authorised persons	
Customer database	High	High	Password protected; credit card numbers encrypted; access limited to CEO and relevant staff	Sales officer
Social media data	Low	High	Password protected; policy made clear	Staff
Intellectual property				
Images (photos, product, infographics)	Medium	High	Infringement monitored and challenged	CEO/Director
Logos and other artwork	High	Medium		
Audio and visual media	Medium to high	Medium to high		
Media releases	Low	Low	All staff have read access. Information officer has write access (password protected)	Information officer
Proprietary software	High	High	Password protected; data encrypted; access limited to CEO and relevant staff: infringement monitored and challenged	IT officer

Value: Rankings (high, medium, low) reflect the value of the data to somebody else and also the cost of fixing the system if someone else interferes with it.

Vulnerability: Rankings (high, medium, low) reflect the difficulty of restricting access to the system, the need for circulating the data outside your business or organisation, and the general complexity of the system.

7. Getting everyone involved

There are computer programs that can detect phishing emails and suspicious websites, but in the end, robust security depends on people doing the right thing.

Everybody in your business or organisation needs to take cyber security seriously.

You have to show you take cyber security seriously by putting in the resources and doing the training. You have to pick up small breaches before they become massive outbreaks. You also need to identify who is responsible for the breaches and then take steps to ensure the breach does not happen again.

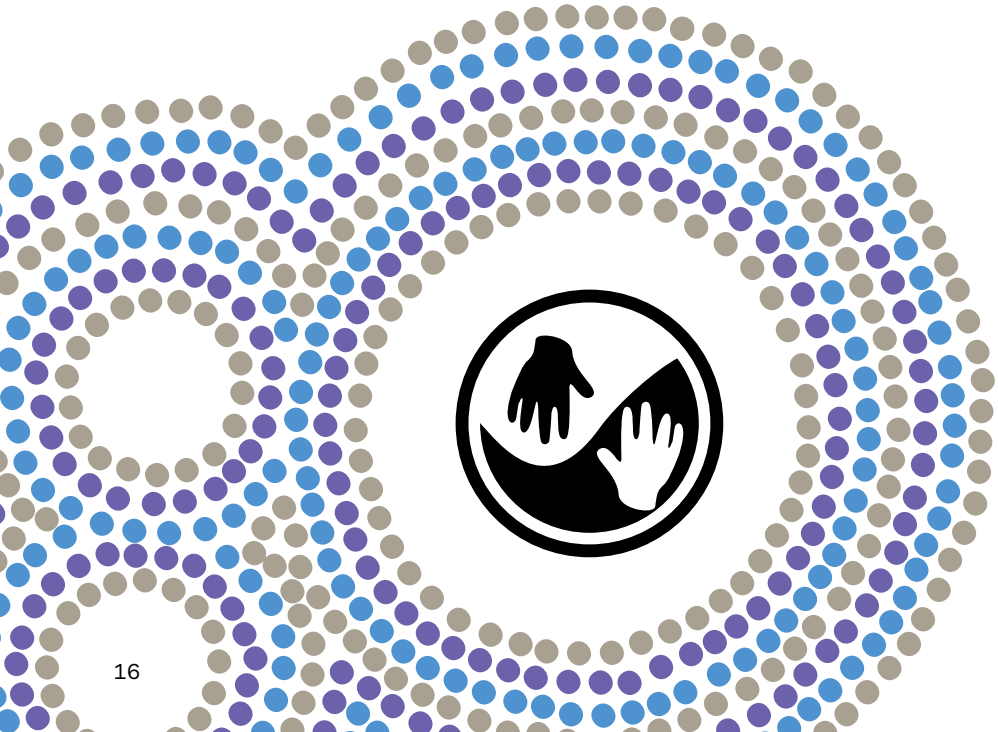
You also want to encourage people to report breaches using positive incentives and make sure they feel part of helping keep your business /organisation safe from outside criminals.

It is hard to get other people to follow the rules if you as a director or manager are not following the rules yourself. This means, for example that you should not be using unlicensed software, even if it is much cheaper than the legitimate version. If you are a not-for-profit or community enterprise, you might be eligible for a discounted software through Connecting Up (www.connectingup.org). Remember, legitimate software is a lot safer and more reliable, and is generally packaged with support/ helplines.

Make sure you are not using intellectual property – online text or graphics, for example – unless it is clear that it is not under copyright.

Do not spam people with unsolicited email, even if you think it will help grow your business/organisation.

Do not, under any circumstances, sell your clients or people's data to anyone else – that is not only unethical, it is also illegal.



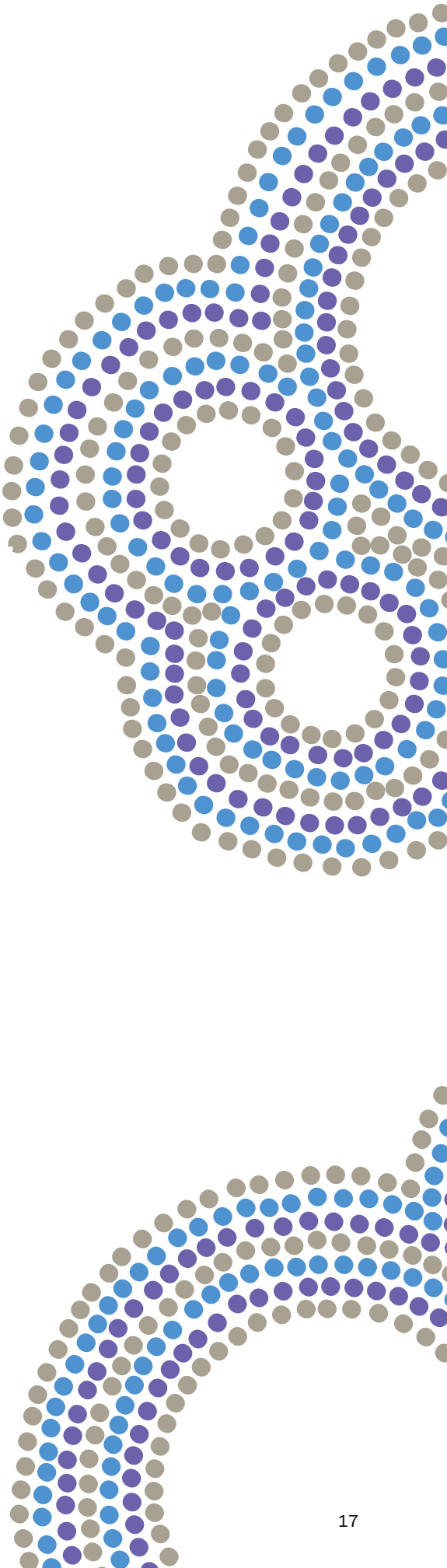
8. Put someone in charge

If you have an IT department, you will probably have people with the skills needed for the role of a cyber security officer.

If you are a smaller business or organisation, your technical person is also going to be your cyber security person. If your business is too small to have an IT person, you should nominate someone to be the go-to person in relation to your organisation's cyber security and privacy. This person may not be an expert, at least to begin with, but they should have an interest in and some knowledge of the topic and be prepared to put time into educating themselves. They will be your first port of call for security issues and will have responsibility for ensuring software is updated, information is appropriately secured, data is backed up, procedures are documented, and your staff are educated. They can also keep a keen eye on the latest cyber threats and keep everybody informed in appropriate non-technical terms.

You will have to give your cyber security person the authority needed to override any internal opposition, but make sure they consult widely on what they are doing and why. They will need good people skills, particularly in training areas, with the ability to cope calmly with questions, mistakes, and unnecessary disasters.

You may find it difficult to get someone exactly like that, and you will have to make allowances for someone learning on the job, making mistakes, and doing the best they can.



9. Embed cyber security in policies and procedures

Trust the process, not the person.

You can reduce cyber security risks posed by staff and volunteers by:

- Allowing access to IT systems, computers, laptops and so on, only to people who really need it
- Promptly removing or limiting the access of anyone who leaves, is dismissed or disciplined
- Keeping detailed system logs of all computer activity
- Physically securing computers and other IT equipment, so that only people with permission can access them.

Cyber security is part of your overall risk management policy, and you have to address it at a systems level. This means you need to document your cyber security procedures. Create a working manual aimed at beginner users, and go through it with your board members, staff and volunteers as part of their induction.

If you are a small business, you might be wondering how this applies to you. But if you have a Facebook page, or maintain a list of client email addresses, or if you use internet banking, you face the same risks as a larger business or organisation. The consequences of a cyber security breach might be smaller, and your manual might be thinner, but you still need to manage the risks.

Establishing and following robust standard operating procedures allows you to identify abnormal or suspicious activities that may signal fraud, whether that consists of a staff member showing an unusually high level of interest in the online banking records, or someone who unwittingly records all the passwords on their desktop because they cannot remember them.

Finance departments have long recognised the importance of separation of duties. For example, keeping your payables and receivables (invoicing team) in separate teams to reduce the potential for fraud.

Likewise, very few people need to have complete access to every single one of your IT systems. Put processes in place to ensure that people can access only what they need to do their job.

Security considerations sometimes conflict with flexibility and efficiency needs. For example, systems that do not allow access outside business hours are more secure, but make it more difficult for employees to work from home. (For more on this, see page 22).

See pages 42 - 49 for examples of policies and procedures, which you can adapt to suit the needs of your business.

Cyber security policy (p42)

Cyber security procedures (p43)

Acceptable use of electronic media policy (p47)

Acceptable use of electronic media procedures (p48)

Whether you are a large or small organisation, you face many of the the same cyber security risks.

10. Passwords

Wetware is IT's name for people - and it is people who make mistakes.

There are a number of ways to break into a business or an organisation's IT systems. One way is to tap into its internet connections and use sophisticated software algorithms to break its encryption and uncover its passwords. These days many organisations have strong firewalls in place to repel these threats, which means that criminals have to go to the second and less technologically driven way: telephone staff and ask them.

An example:

"Hi, Stanley. I'm Mitch from Telecom. Our meters say there's an intermittent fault on your line. Have you been having trouble? No? Well, that's what 'intermittent' means. Anyway, I'll need to have remote access to your computer for ten minutes while you go off and get yourself a coffee. If you can just tell me your username and password I'll get this fixed as quickly as possible and I won't have to bother you again."

It is surprising how often that works.

Hackers have also been known to break into secure systems simply by dropping USB drives loaded with malicious software in car parks and waiting for people to pick them up and plug them into their computer.

Amateurs hack systems; professionals hack people.

– Bruce Schneier US cyber security expert

People take short cuts all the time. They will use passwords like the following - the 25 most common (and, therefore, the worst) passwords on the internet in 2018: https://www.businessinsider.com.au/worst-passwords-of-2018-2018-12

1. 123456
2. password
3. 12345678
4. 123456789
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou
11. princess
12. admin
13. welcome
14. 666666
15. abc123
16. football
17. 123123
18. monkey
19. 654321
20. !@#$%^&*
21. charlie
22. aa123456
23. donald
24. password1
25. qwerty123

Often people who typed in 123456789 felt that their passwords were much safer than someone who was using 1234.

IT staff have a well-deserved reputation for wanting you to have a 12-character password involving four numbers, no English words, and several uppercase special characters. In addition, they will tell you:

1. You should not write it down, in case criminals find the piece of paper.
2. You should change it monthly, which requires you to memorise another random 12-digit string.
3. You should use it for only one account, which requires you to memorise another random 12-digit string for each separate purpose.

The thing is, they are right.

Many people when faced with these requirements will simply go back to using something much easier to remember, such as "password".

Your business or organisation can try to find ways to encourage or force people to follow good password practices – through training them into understanding, or you can implement a technological fix.

Specialised password management software (such as 1password. com) takes some of the difficulty out of remembering multiple complicated passwords. However, these software options bring their own risks and you need to consider these, before implementing them in your organisation.

In recent years we have seen advice around passwords change. It is now generally accepted that long and complex pass-phrases are more effective than a password. This is because they are more memorable than a long complex series of letters and numbers. It has also been shown that pass-phrases take longer for cyber criminals to crack.

If your business or organisation uses online services that are shared by multiple users, consider paying per user instead of taking the cheaper option and having different users share one account. It will cost a little more, but it means passwords are not shared. It also means you have more information about who is using the service and when, which may be important from an audit point of view.

Many online services also prohibit shared accounts, so having individual accounts means you won't be breaking their terms and conditions.

Passwords: strong, safe and secret

Implementing a secure password policy is one of the simple steps you can take to protect yourself and your business/ organisation online. Tell your people:

- Make your password long – at least eight characters, or three or four random words as part of a 'pass-phrase.'
- Use a combination of upper and lower case letters, numbers and symbols. For example, My-k1D5-ru73 is memorable (it's a play on "My kids rule"), it won't be found in a dictionary and it contains a mix of different character types.
- Do not use words from a dictionary (including foreign words) – hackers will use dictionary-based tools to crack your code. Short phrases are better than words.
- Do not make it easy. Avoid using easily discovered information such as your name, birthday or address as your password.
- Change your password frequently – try setting up a calendar reminder every month.
- Your password is just for you – do not share it and do not write it down.

11. Training your people in cyber security

Develop a layered training system – one that comes into effect at different points during an employee's time with your business or organisation.

1. Include cyber security training in your induction program for board members, staff and volunteers.
2. Provide training that is more detailed for people once they have settled into their job and know the systems they are working with.
3. Provide all your employees with a refresher course at least once a year.

Training session do not have to be long and boring. You might hold a series of lunchtime discussions on issues such as how to secure your Facebook account or how to recognise online scams. A personal story can then be related to the work environment. If you really want your staff to engage in security, make it personal for them.

A long-term program of cyber security training might look something like the following:

Cyber security induction

In the case of a small business, this might consist of a one-to-one session on cyber-security practices.

In a business/ organisation that has an IT department, the induction would probably be run by the cyber security person.

- Set up program access and passwords
- Instruct on incident response procedures
- Provide an overview of relevant policies and procedures

Three months after induction, then annually

- Review program access and password security
- Refresher on relevant policies and procedures
- Check for or install up-to-date security software

Refresher courses

- How to recognise online scams and scammers
- Safe use of social media
- Password security
- Up-to-date cyber risks

If you want your staff to engage in security, make it personal for them.

12. The weak points: hardware

Desktop computers are easily stolen in a break-in. If your data is stored on your computers, and if the robbers can get through the password security, they can steal your data.

Many offices still do not take proper precautions when it comes to protecting desktop computers. It is surprising how many businesses sell off old computers without first wiping the memory or encrypting them.

With laptops, theft is even easier. Criminals just wait until you are distracted and then simply walk off with your laptop. Or the laptop may be accidently left behind on a train or in a taxi.

In America, a data analyst from a US Government department had his laptop stolen with 26 million personal records on it. While one American study found that 600,000 laptops were lost or stolen at US airports every year[1].

1. Ponemon Institute, Airport Insecurity: The Case of Missing & Lost Laptops , June 2008.

Bring Your Own Device (BYOD)

Some businesses/organisations allow employees to use their own smartphones, tablets and laptops for work purposes. This practice, known as BYOD, or bring your own device, offers advantages such as allowing people to use equipment they are comfortable and familiar with to access work-related emails, documents and programs. It also has the potential to save business/organisations money too.

But what does BYOD mean for the security of your business/organisation's data? What does it mean for your network's risk of attack by malicious software? What if a director leaves their iPad /laptop in an uber/taxi, or an employee resigns from the organisation, taking with them a hard drive full of confidential documents? What if a director's kids have access to the laptop and post the minutes of the latest board meeting to Instagram/Facebook?

There are policy and technical solutions to these problems. Policy solutions usually involve making sure that users secure their devices with passwords and passcodes. Technical solutions involve a secure range of apps and data that enable data to be remotely erased if the device is lost or an employee leaves, potentially without removing any of the user's personal data.

When you are identifying digital assets and creating a customised security plan, it is very important that you take into account all the implications of BYOD.

The Australian Government's Department of Defence has a brief guide (http://tinyurl. com/gloyd6z) of the issues you need to consider.

Protecting your hardware

There are a number of steps you can take to make your systems reasonably secure.

- In public access areas, physically secure your desktop computers with cables and padlocks
- Monitor and control access to areas where there are computers
- If sensitive data is involved, check the sightlines to computer screens and make sure they are not visible from public areas
- Lock up rooms with computers in them at night.

The above list obviously does not work for off-site laptops, where the risk is that they can be lost or stolen. For mobile devices you might consider:

1. Stopping staff from taking data out of the office. While this is the safest course, this may be difficult to implement in practice as many people now work remotely or from home.
2. You can mandate that any data taken out of the office be encrypted. This requires more work from employees and there is a chance that some staff may not do it.
3. You can stop people from taking data out of the office and make it possible for them to securely access information from the office remotely. This will mean that you may have to punch holes in your IT defences to allow employee access. You can place strong password requirements on entry, and if there is a breach, you will be able to identify to some degree who came in from their network credentials along with network logs.
4. You can request staff to install Remote Laptop Security (RLS). This means the owner of a laptop can remotely shut down access to it, via the internet, if the device is lost or stolen. It may even be possible to locate and retrieve it.

And before you travel:

- Back up your data and leave a copy of your files in a safe and secure location
- Make sure your operating system is protected by a strong password
- Password-protect, encrypt, or remove all personal and proprietary information stored on your laptop
- Turn off file sharing and print-sharing in Settings
- Apply all software patches and updates
- Check that anti-virus, anti-spyware, and personal firewall software is installed and up-to-date on your laptop
- Set up a tracking service (so that you can locate your machine if it stolen) or install tracking software on your laptop.

Make sure you understand how to remotely access your fileserver, mail server, or desktop securely – if you are not sure, consult with IT. If you do not have an IT department, you probably will not be able to use remote access.

As we continue to erase the distinctions between computers and other devices like mobile phones and tablets, the cyber attacks discussed in this guide can now take place in your pocket.

While this is a fast-developing field, you can take the same precautions on your phone as you would on your computer. Watch out for phishing texts, turn off your phone when you are not using it, notice if your phone starts behaving oddly, do not leave it in a café and do not use it for anything that is really sensitive.

You might want to consider using an encryption app such as Signal, Wikr me or ProtonMail.

13. The weak points: software

Malicious software, or malware, is software used to gather private information, disrupt computer operations or gain unauthorised access to systems/computers.

Spyware, adware, Trojans, worms and viruses are all types of malware. Banking malware, for example, can kick into action during an online banking session – it can alter a payment you have made so that it goes to someone other than the intended recipient, or capture your log-in credentials and send them to a third party.

It is important to remember that malware is often disguised as legitimate software. Once installed it can be difficult to detect and remove.

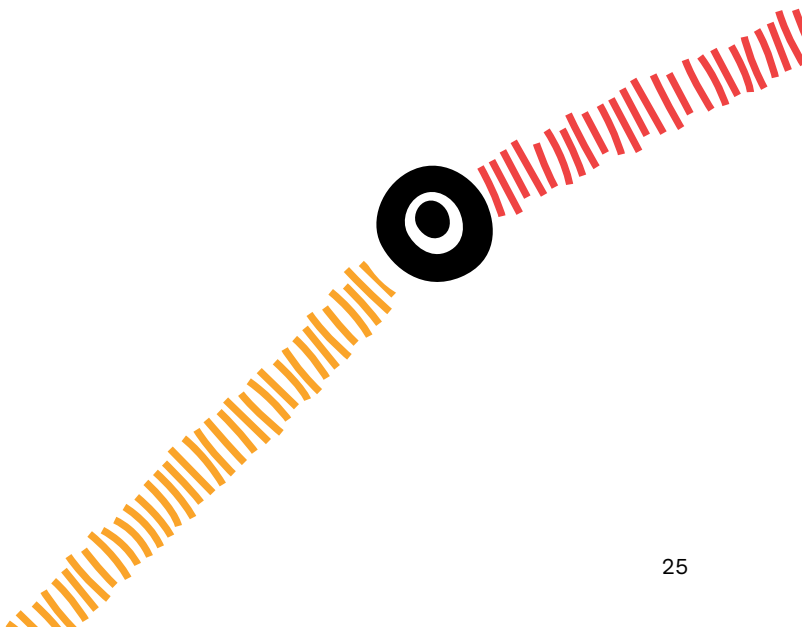
The Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) in 2017 published The Essential Eight, which can help mitigate cyber security incidents:

- Application allowlist of approved/ trusted programs to prevent execution of unapproved or malicious programs.
- Patch applications: patch or update computer software with vulnerabilities within 48 hours.
- Configure Microsoft Office macro settings: only allow vetted macros with limited write access.
- User application hardening: configure web browsers to block Flash (ideally uninstall altogether) as well as tightening configuration options on all software running in the organisation's environment.
- Restrict admin access based on user duties.
- Multi-factor authentication: implement for all users when accessing an important data repository.
- Daily backups: make backups of important data.

No software or hardware solution will be 100% effective 100% of the time. The larger and more complex a system, the higher the likelihood of bugs in the code and flaws in the design, which opens up avenues of attack.

There is also the compromise between ease of use, functionality and security. If you design a large system for ease of access it is more likely to be insecure, and if you make it watertight, ease of use suffers. People who write code have to make sure there are zero bugs in thousands and sometimes millions of lines of code, while a hacker only has to find one bug.

Increasingly, all our systems – work computers, home computers, mobile phones, online storage, the internet – flow into each other, which means that a breach in any one of them can potentially jump across to all of them. Visit the wrong website or open the wrong email attachment and you could find yourself in a world of pain, watching on as your systems facilitate cyber crime.



Protecting your software

There are many things your business/organisation can and should do to minimise the risk of exposure to malicious software:

Installing internet security software on all your computers is a good place to start. It is important to understand the full cost of security software. While you can walk into your local office supply shop or electronics retailer and buy software off the shelf, it is a better idea to buy the software directly from the software companies or their distributors. That way, you can get access to volume discounts and help with establishing processes and systems for keeping the software up-to-date. Then you are always protected from the latest threats.

There are many reputable security software companies including McAfee, ESet, Symantec and Bitdefender. Most companies release a new version of their software each year, so it can seem hard to keep up with what is the best choice. Independent comparisons are available from companies such as www.av-test.org, www.av-comparatives.org and www.virusbtn.com. They can be a great place to start your research to help identify what is best for you and your business.

Free software might seem like a bargain, but its functionality is often restricted. A modest investment now could save you big dollars in the future.

Keep your software – especially your operating systems and browsers – up-to-date. Most modern applications automatically check for the latest updates, but it is wise to make sure that application settings are correct and updates are being installed. This applies to security software as well as operating systems, browsers and productivity applications.

Use WPA2 (WiFi protected access, a security protocol) to secure your wireless network. For more advice on security wireless networks visit http://cyber.gov.au.

A firewall is a piece of computer hardware or software that protects the borders of a computer network. If there is no firewall then the borders of your network are left with holes and anyone can enter. A firewall limits the entry points. Use a firewall.

Encourage everyone to use strong passwords. Using weak passwords is like hiding the keys to your house under the front doormat – convenient, yes, but putting you at a higher risk of a break-in. For more on passwords, see page 19.

Ask IT whether you need to encrypt part or all of your data and communications. While encryption is not unbreakable, it does make life much tougher for hackers and may be enough to drive them away to look for easier targets.

Consider using a system that provides one-time passwords. Some online services have the option of using a one-time code sent via SMS when they want to log-in. This relies on the user having the phone and having the code. In security terms, this is called “something you have” and “something you know”, or two-factor authentication.

Try to restrict who can install software on your IT systems by limiting “administrator accounts”. Administrator accounts have full access to install software and alter a computer’s settings. Many types of malware work only if the logged-in user has administrative access to the computer. When you add a staff member to your network, give them access only to what they need to do their job, and no more. It might be tempting to give them elevated access “just in case”, but that may open you up to unnecessary risks. Keeping control on what is installed on your business/organisation’s computers significantly reduces the risk of malware.

14. Protecting against phishing

Have you ever received an email that looks as though it is from a bank, online store or government department but is in fact a fake? That is a phishing attack.

Phishing attacks involve what looks like a legitimate email containing links that either trick you into installing malware or direct you to a website that steals your data. In some cases, phishing attacks target specific people by using personal information from sources such as Facebook or LinkedIn to add an air of legitimacy to the message. These highly targeted attacks are also called spear-phishing. Spear-phishing is commonly used to access the administrative accounts of IT staff or confidential information from senior managers and board members.

For example

One common phishing attack looks like an email from your bank, asking you to log-in to your account and check some information. However, the link actually takes you to a fake copy of the bank's website.

Once you enter your username and password, the attacker knows you are a customer of the bank and has your login credentials.

To help ensure your organisation does not become a victim of phishing, make sure that all staff follow these tips:

- Think twice before you click on links in website pop-ups or emails – especially if the email is from someone you do not know or arrives unexpectedly or seems out of place. If you are not 100% sure, go to a web browser and check the website manually, rather than clicking on the link. If you suspect an email from your bank is a phishing scam, go to the bank's website without using the email link.
- Do not share confidential information, account numbers or passwords.
- Let your colleagues know if you do receive a suspicious email – chances are you will not be the only one.
- If you receive an unsolicited or suspicious email, do not click on any links in the email, and do not open any attachments.
- Remember the old saying– if it seems too good to be true, it usually is.
- If you are being asked to make a payment to a supplier or customer and their payment details have changed, always independently validate the request.

The doppelgänger

Phishing emails rely on looking like the real thing and are also becoming more sophisticated. These emails may contain corporate logos, branding, and information about you to make them look and sound genuine.

They will often ask you to confirm sensitive and personal information, such as bank account details and passwords. Legitimate organisations such as banks will never send you emails asking you to confirm, update or reveal your personal information.

Never click on a link in an email or open an attachment unless you are 100% certain it is legitimate. Most email programs will allow you to place the mouse pointer over a link. A small pop-up will then appear telling you where the link is actually going, so what may look like a link to a bargain on eBay or your web banking service will show up as a link to some other address.

Deceptive emails may also appear to come from within the organisation. A 2015 threat assessment (see http:// tinyurl.com/oers7ar) by the European Union law enforcement agency Europol reported an increase in "CEO fraud", whereby cyber criminals pose as CEOs or CFOs of large companies and trick lower-ranking staff into transferring large sums of money to them.

Europol said such criminals were emailing, or even phoning, employees with access to company funds and instructing them to carry out their urgent demands.

Regional subsidiaries are often targeted because staff in regional offices tend not to know senior management personally "and may be fearful of losing their job if they do not obey", the report warned.

How to spot email payment fraud

- The request claims to be urgent and/or confidential.
- You are requested to ignore standard payment authorisation processes.
- The request may include grammatical and spelling errors.
- The type of request and the language and formatting are unusual for the supposed sender.
- The 'reply to' email address is different to the sender's address.

Recommended actions

Raise awareness.

Empower your staff to always question and escalate anything suspicious. Consider phishing simulation exercises to test staff susceptibility to social engineering attacks.

Review payment processes.

Enforce strict processes for authorising payments. Implement multiple approvals for new or large payments or for requests to change the payment details of existing suppliers.

Use multiple channels to verify.

Validate suspicious requests on an alternative communication channel, using contact details listed in your internal records.

Be social savvy.

Think twice about publishing company employee information on the public internet or social channels. This applies especially to information about staff hierarchies, payment processes, new supplier relationships or executive travel plans.

Act immediately.

Notify your bank immediately if your staff have made a payment by mistake.

Define your email perimeter.

Consider measures that ensure emails from your company domain can only be sent from an allowlist of approved IP addresses (see the SPF, DKIM and DMARC standards).

15. Protecting your website

Spammers

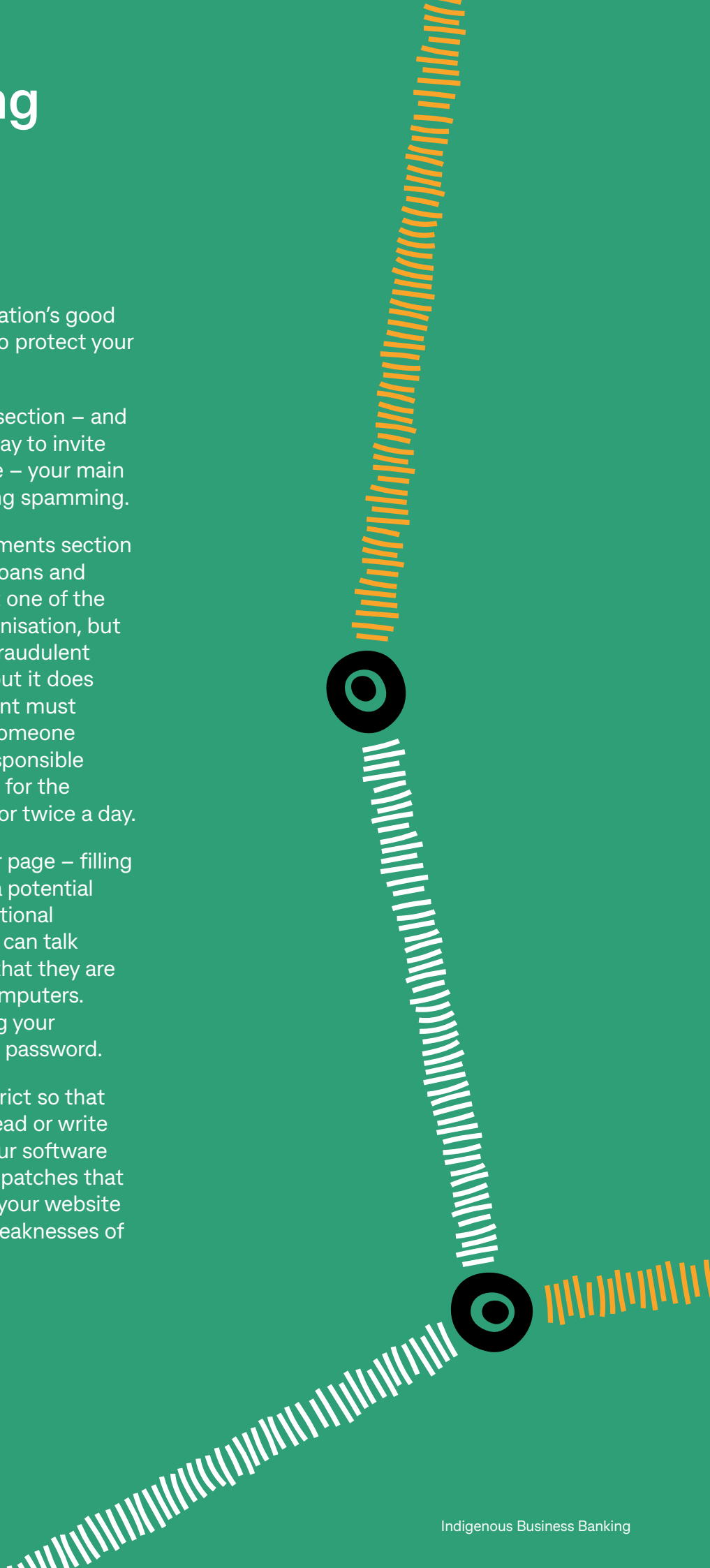
To protect your business/organisation's good name and reputation, you need to protect your website from unauthorised use.

If your website has a comments section – and it really should, that is the best way to invite the involvement of your audience – your main challenge is going to be managing spamming.

People are going to fill your comments section with advertisements for payday loans and counterfeit handbags. This is not one of the major risks to your business/organisation, but those links could lead others to fraudulent websites. It is simple to fix this, but it does involve more work. Every comment must be approved before it goes up. Someone in your organisation has to be responsible for checking incoming messages for the comments section at least once or twice a day.

Every interactive element on your page – filling out forms or uploading files – is a potential security breach and requires additional technical protection. If the public can talk back to you, you have to be sure that they are not giving instructions to your computers. To combat this, consider requiring your customers/users to sign in with a password.

Keep your default permissions strict so that unauthorised outsiders cannot read or write anything they shouldn't. Keep your software up-to-date and use any security patches that come out. Check out plugins for your website software that may address the weaknesses of your platform.



DDoS attacks

DDoS attacks, or distributed denial-of-service attacks, work by overwhelming a website or online service with massive volumes of unexpected traffic. (Remember the 2016 census? See http://tinyurl.com/gm39svu.)

DDoS attacks are tools that can be used by hactivists – activists trying to make a political point – or ransom demands. There have been many cases of perpetrators demanding payment in exchange for breaking off an attack on a website brought down by a DDoS. Some DDoS attacks have been linked to corporate espionage, with rival firms using DDoS to drive competitors out of business.

Criminals can launch a DDoS attack against anybody, big or small. There is even a market around hiring networks of compromised computers to flood a website or online service with traffic.

According to Australia's national Computer Emergency Response Team (CERT), there are a number of steps you can take to help protect your business/organisation from a DDoS attack:

If somebody claiming to be responsible for a DDoS attack against you sends you an email demanding money, do not reply – not even to say "no".

- *Do not run corporate web servers on the same computers you use for key business functions. That way, if your website suffers a DDoS attack you can still access your finance system.*
- *If your website is critical to your organisation, have a back-up plan in case your website goes down. This can include having multiple web servers or using external service providers to host your website. They are more likely to have the resources to withstand or thwart a DDoS attack.*

For practical advice on DDoS attacks and tools to help prevent them, visit the website of Australian Cyber Security Centre (ACSC) (https://www.cyber.gov.au/acsc/view-all-content/publications/preparing-and-responding-denial-service-attacks).

16. Cloud computing: benefits and risks

Cloud computing, or the storage of files and programs on the internet rather than on your computer's hard drive, presents new opportunities for backing up your businesses/organisation's data quickly and cheaply. But there are some important considerations you should be mindful of before you start backing up to the cloud:

If the cloud provider is compromised, what recourse do you have?

The cloud providers all have massive security systems, but remember: there is no such thing as an unbreakable system. If someone breaks into the cloud provider's systems or simply gets access to your account, your data could be accessed – and while you can certainly point out to your members and clients that it is not your fault, they may still hold you responsible.

Where is my data being sent to and stored?

You need to know that your data is being held by someone you trust. And if you do need to retrieve it, how long it will take. Will retrieval involve shipping physical tapes or disks? Find out before you commit.

Does the nature of my data mean it needs to be kept onshore?

In other words, does my organisation store personal information and is it subject to the Australian Privacy Principles? This is a tricky legal area, but it is important to understand your legal obligations when it comes to storing data offshore.

Data stored offshore is subject to the laws of the country where the data storage company is based and also the laws of the country where the data is physically stored. Imagine a scenario where an Australian business uses a US-based company to store its data offsite, and that company's servers are in Singapore. In theory, the organisation could find itself in a situation where it is required to protect personal information to comply with the Australian Privacy Principles and, at the same time, to provide that information to a law enforcement agency overseas.

If your organisation deals with personal information – and almost every business does – then you should seek legal advice before storing your data overseas.

Is my data going to be encrypted?

When you are thinking about cloud services for back-up, replace the word "cloud" with the phrase "someone else's computer". Would you allow someone else – anyone – to access your data?

A reputable cloud storage and back-up service will allow you to encrypt your data. In many cases they will not be able to read the data themselves because they will not have access to the decryption key – that stays with you.

17. Preventing data loss: the importance of back-ups

A major loss of your organisation's data could have a serious impact on your ability to operate and cause great damage to your reputation. You might also face legal, regulatory or other serious consequences.

To avoid losing data, backing up is critically important. The generally accepted best practice for back-ups is the three-two-one-zero approach. Here is how it works.

3 Three

The number of copies of your critical data you need to have at all times.

This is quite easy to achieve.

- First there is the master copy of your data on your computers and servers.
- Second, you can set up a back-up system where critical data is automatically copied to another computer, or, depending on your needs and budget, to other back-up drives or media.
- Third, you can use a cloud storage system to replicate your data. For a charge, the service provider will store an offsite copy of your data.

2 Two

The number of different storage media you should use. By using a cloud-based back-up service or sending back-up hard drives offsite, you are already using two different media – the original data and the back-up copy or copies.

1 One

The minimum number of copies of your data you should keep offsite, away from your main work area.

If you decide to use external hard drives for back-ups, you should ensure they are taken offsite at the end of the back-up process. If the worst should happen and there is a theft or your offices are damaged by a fire or flood, then the back-up of your data will be safe.

If you are sending data offsite, make sure you know where the data is going and who has access to it. Some businesses/organisations have sent back-ups offsite only to find that their data has leaked. If you are using a cloud service, make sure the data is encrypted. That way, even if the data is stolen, the thieves will not be able to access it without the decryption key. It is like stealing a safe but not knowing the combination.

0 Zero

The number of errors your back-ups should contain. All the back-ups in the world are worthless if they are broken.

One of the often-missed steps in back-up processes is testing the recovery process. Many people think they have robust back-up and recovery processes only to find out too late that something is not working. Unfortunately, they usually find this out the hard way.

Back-up technology is becoming cheaper and easier to use, so backing up data does not have to be a time consuming chore. Most back-up programs can be "set and forget". Just do not forget to test your system.

18. Your cyber security manual

The Australian government's Information Security Manual (see http://tinyurl.com/zxxxpf9) runs to 396 pages and still cannot fit in all the detail it needs.

Whether your business/ organisation is large or small, your cyber security manual should cover:

- Who the cyber security officer is
- Roles and responsibilities in relation to cyber security: who does what (who does back-ups, who updates software) and who has which privileges (who has access to what, who can alter what)
- What hardware you have, and who you ring if there's a breakdown
- What software you have, and who you ring if there's a problem
- What cyber security precautions are in place, and what you do if there is a breach (disaster recovery plans).

If you are a small business, the manual might run to one or two A4 pages.

If you are a large organisation with lots of staff, then you will probably need department-by-department manuals covering the particular needs of each area.

Whatever your size, you will also need an asset register and a faults log book.

The asset register will document the organisation's hardware and software, and where it is used or stored. The cyber security officer should update the register after every new purchase, noting down:

- Hardware and operating system
- Network configuration
- Software versions, licence keys and configuration details
- Software and database locations on the network
- Email and internet details
- Location of manuals, discs and back-up media.

The faults log book gives you the basic data you need for monitoring. It should record for each incident:

- The date
- The fault
- The outcomes
- The remedial actions taken
- Who took them.

19. Staying up-to-date on cyber threats

Security is a process, not a product.

Staying up-to-date on the latest cyber trends and threats is never ending.

There are many sources of information to help you. In addition to following mainstream news, have a look at the following resources:

Large providers of cyber security products

Companies like McAfee, Symantec, AVG and Sophos have newsletter services so you can sign up to email alert lists to stay on top of the latest information.

Relevant websites such as Apple, Google and Microsoft

For news and updates specific to the operating system you use.

Australian news sites with an IT security focus include www.cso.com.au and www.itnews.com.au.

Your bank or financial institution

For example, the Commonwealth Bank's security site (see http://tinyurl.com/zdaywk5). You can also subscribe to the Commonwealth Bank's free quarterly cyber security update, 'Signals' https://www.commbank.com.au/business/support/security/signals.html.

Cyber security advisory and alert services

These include the alert service offered at Stay Smart Online (see http://cyber.gov.au).

Scamwatch

Scamwatch.gov.au contains up-to-date information and tips on how to avoid the latest scams. Get in the habit of checking Scamwatch when you come across a questionable email or contact.

Australian Securities and Investments Commission

ASIC's consumer information website, Moneysmart (see http://tinyurl.com/jldgveh), is designed to raise awareness of fraud and protect you from becoming a victim.

20. What about social media?

Social media such as Facebook, Twitter and LinkedIn, make up a large part of human interaction, and your business organisation cannot really opt out. You should have a social media presence, despite the risks involved.

This requires careful handling, and you will need to have approval processes in place so that nobody tweets casual thoughts in your name that conflict with your policies or principles.

You will need to decide what you will do if the commentators on your posts criticise you (it is probably best to leave it up there but post a reasoned response) but you must not let people put up anything that is obscene, or prejudiced.

Most business/organisations need a social media presence. Your staff will probably have their own personal social media accounts. Make sure they are aware of the risks.

As the Australian Cyber Security Centre* (ACSC) says:

Users posting information about their personal life, their official duties, project details or government policy could unknowingly provide people with information that could be used to elicit government information from them or to tailor social engineering campaigns to compromise an agency's networks. Users should assume everything posted on social networking sites is permanent.

Build this kind of caution into your staff cyber security training. Tell your staff, if you have staff, to report anything suspicious to the cyber security officer.

* https://www.cyber.gov.au/acsc/view-all-content/publications/security-tips-social-media-and-social-networking-apps

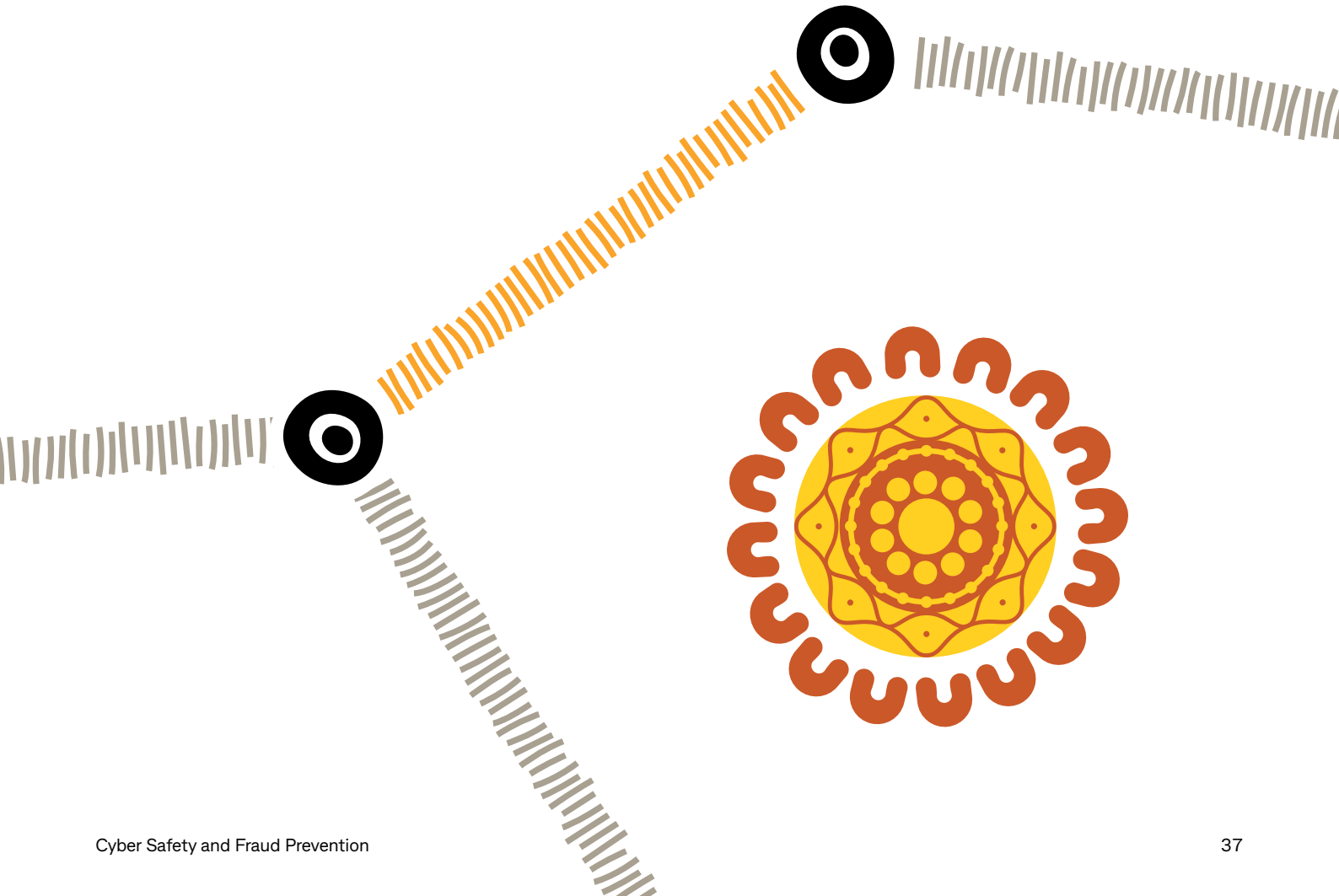
21. Online banking: is it safe?

It is important that you protect your business/ organisation's bank accounts by having more than one person to authorise withdrawals.

You will need to set things up so that every online transaction is authorised by more than one person. It is slightly more involved than counter-signing a paper cheque, but it is every bit as necessary.

Online banking services are protected by stringent security measures. For example, Commonwealth Bank's CommBiz services are protected at a hardware level and a software level (see http://tinyurl.com/gou7uae).

Each user is authenticated using a login ID and password before being granted access to CommBiz. All sessions are encrypted, and security tokens and NetLock USB devices are provided to all authorised users. The security token generates a one-time password to provide a second factor of authentication. The NetLock USB device is designed to be used along with CommBiz security tokens to give extra protection against even the most sophisticated security threats. Other banks have similar systems.



22. How much will all this cost?

Every organisation is different when it comes to cyber security risks. Your investment in cyber security will depend on how much you depend on IT.

Some organisations have a small digital footprint, while others have IT and computers at their core. The more dependent you are on IT, the more effort you should give to cyber security.

A-grade security is expensive. One estimate puts the average Australian government department expenditure on cyber security at 2% of the IT budget, while Singapore government agencies spend 10% and banks and financial institutions can spend as high as 15%.

Developing good procedures and policies for security, investing in security software and keeping your software up-to-date helps to make your business/organisation as small a target as possible. Cyber security does not need to cost a fortune, but being alert is important. To put it another way, there is no way you can afford not to be protected.

23. Can I insure against cyber security risks?

Many insurance policies, including many directors and officers' liability policies, public liability policies, public indemnity policies and fraud policies, do not cover cyber attacks or other cyber threats.

This means that if your organisation is attacked and your data falls into the wrong hands, or you are unable to carry on your work as usual, you are on your own financially.

An expensive cyber security incident does not have to involve hackers. If someone from your business/organisation accidentally leaves their laptop in an Uber or a taxi, or drops their smartphone in the street, the information on those devices is vulnerable and could be misused by opportunists.

At risk information includes credit card numbers, client lists and employee profiles.

Potential costs of investigating and fixing the breach can quickly add up to thousands or even millions of dollars. Costs can include: notifying 'affected parties', fines imposed by government agencies, third-party claims, and interruptions to your business/organisation's work.

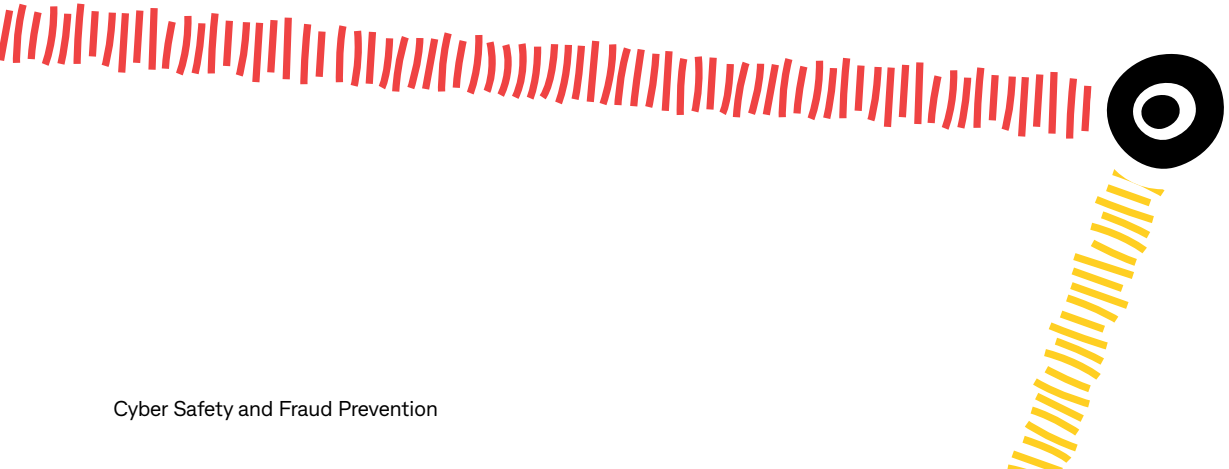
Insurance coverage for cyber incidents is still the exception, not the norm although its occurrence is increasing, so it is important check your policy.

You may find it is worthwhile taking out an additional cyber security insurance policy.

Even the process of applying for a quote for cyber coverage can be helpful to an organisation/business. It requires documenting existing systems, policies and procedures. This can help identify security flaws and vulnerabilities.

If your business/organisation elects to self-insure in the face of high premiums for cyber insurance coverage, it is critical that you take all steps to protect yourself against an attack or other losses.

If your business/ organisation is attacked and your data falls into the wrong hands, or you cannot carry on your work as usual, more than likely you are on your own financially.



24. Be prepared: plan and practice

What if, despite your best efforts, your business/ organisation has become the victim of a cyber security incident? Preparation is the key to riding out the cyber storm.

We suggest practicing what you plan to do in the event of a cyber incident. Get the right people together in a room and run some scenarios: pretend an incident has occurred and then work through what each of you would do. If you do this a couple of times each year, everyone will be able to assume their roles with less panic and greater confidence if a real incident occurs.

When it happens, it might be tempting to jump straight into reactive mode. Our advice is to stop and think first. If you have had first aid training, you will remember that the first step in giving first aid is to assess the environment. The same applies if your IT systems are under attack. Reacting in haste can increase the problem or reduce your chances of understanding the cause of the incident, mitigating the risk of a recurrence and catching the bad guys.

Start by looking at what has gone wrong. This includes understanding how the attack occurred, what systems were affected and the extent of the incident. If you have already carried out an audit of your systems and data, then it will be easier to understand what has already been affected and what might be affected if the attack continues.

Put someone in charge of managing the incident. This is not necessarily a senior manager. It should be the best person to deal with a cyber security incident – most likely your cyber security officer. Ideally, this is someone who can understand both the technical and practical impacts of the incident and translate between the two.

Next, take action quickly either to fix the problem or to stop any further leakage of information and data. If you need help make sure you reach out to a trusted IT partner.

In 2018 it became mandatory to notify affected individuals or the Office of the Australian Information Commissioner (OAIC) of a data or privacy breach. The OAIC's Data Breach Notification Guide says it is generally good practice to notify impacted individuals when a breach occurs if there is a real risk of serious harm to the individuals, although the particular circumstances and potential consequences of each breach should be taken into account. If you need help, you can contact the OAIC (https://www.oaic.gov.au/).

While admitting to a breach might be embarrassing, it is better that you let your staff, customers and other stakeholders know before they find out through word of mouth or through the media.

Lastly, and perhaps most importantly, after the cyber incident, get your key people together and examine what went wrong. Draw up a plan, implement the changes and protect yourself.

Appendix 1: Template policies and procedures

The following template policies are for guidance only and should be tailored to suit your own business or organisation.

Cyber security policy

Policy number	<<insert number>>	**Version**	<<insert number>>
Drafted by	<<insert name>>	**Approved by board on**	<<insert date>>
Responsible person	<<insert name>>	**Scheduled review date**	<<insert date>>

Introduction

While [Name of organisation] wishes to foster a culture of openness, trust, and integrity, this can only be achieved if external threats to the integrity of the business/organisation's systems are controlled and the organisation is protected against the damaging actions of others.

Purpose

This policy sets out guidelines for generating, implementing and maintaining practices that protect the business/organisation's cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

Scope

This policy applies to employees, contractors, consultants, and volunteers at [Name of Organisation], including all personnel affiliated with third parties, to all equipment owned or leased by [Name of Organisation], and to all equipment authorised by [Name of Organisation] for the conduct of the organisation's business.

Policy

While [Name of business/Organisation] wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the business/organisation's systems remains the property of [Name of Organisation].

Because of the need to protect [Name of Organisation]'s network, the confidentiality of information stored on any network device belonging to [Name of Organisation] cannot be guaranteed, and [Name of Organisation] reserves the right to audit networks and systems periodically to ensure compliance with this policy.

Information in the possession of the organisation shall be classified into different grades depending on its degree of confidentiality. Particularly sensitive information will receive special protection.

Employees and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

Breach of this policy by any employee may result in disciplinary action, up to and including dismissal.

Authorisation

[Signature of director/ board secretary]

[Date of approval by the Owner/CEO/board]

[Name of business/organisation]

Cyber security procedures

Procedure number	<<insert number>>	**Version**	<<insert number>>
Drafted by	<<insert name>>	**Approved by CEO on**	<<insert date>>
Responsible person	<<insert name>>	**Scheduled review date**	<<insert date>>

Responsibilities

It is the responsibility of the Director/CEO to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately;
- a cyber security officer is appointed.

It is the responsibility of the cyber security officer to ensure that:

- the Director/CEO is kept aware of any changes to the businesses/ organisation's cyber security requirements;
- a report on the business/organisation's cyber security is submitted annually to the board/owners

It is the responsibility of all employees and volunteers to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures in any particular instance, employees and volunteers should consult their supervisor.

Processes

Monitoring

The Director/CEO may authorise individuals with responsibility for cyber security issues in the business/organisation, including the cyber security officer, to monitor the organisation's equipment, systems and network traffic at any time for security and network maintenance purposes.

Confidentiality

Following consultation with the cyber security officer, the Director/CEO shall from time to time issue cyber security procedures appropriate to different levels of confidentiality.

The business/organisation shall classify the information it controls in the organisation's computer system files and databases as either non-confidential (open to public access) or confidential (in one or many categories). The cyber security officer is required to review and approve the classification of the information and determine the appropriate level of security that will best protect it.

System Taxonomy

Security level	Description	Example
Red	This system contains confidential information – information that cannot be revealed to personnel outside the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life-threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information.
Green	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access server and application(s). Management workstations used by systems and network administrators.
White	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
Black	This system is externally accessible. It is isolated from RED and GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.

Data Taxonomy

Security level	Description	Example
Red	• Client data allowing financial exploitation or identity theft • Business/Organisation data allowing banking or financial exploitation	• Client credit card and banking data • Business/Organisational credit card and banking data • Client details that would facilitate phishing
Green	• Client data allowing address or email exploitation • Business/Organisational intellectual property that has financial or reputational consequences	• Addresses that would facilitate spamming • Information that the business/ organisation sells • Internal emails
Black	Publicly accessible data	Non-sensitive information

Access control

Individuals shall be assigned clearance to particular levels of access to the business/organisation's information resources, and shall access only those recourses that they have clearance for. Access control shall be exercised through username and password controls.

Computer security

All PCs, laptops and workstations should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

Users must keep passwords secure. Accounts must not be shared, and no other people may be permitted to use the account. Passwords should not be readily accessible in the area of the computer concerned.

Authorised users are responsible for the security of their passwords and accounts.

System level passwords should be changed quarterly; user level passwords should be changed every six months. User accounts will be frozen after three failed log-on attempts. Log-on IDs and passwords shall be suspended after 30 days without use.

Users who forget their password must call [the IT department] to get a new password assigned to their account. The user must identify themselves by [e.g. employee number] to [the IT department].

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorised users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to log-on as system administrators. Users who need this level of access to production systems must request a special access account as outlined elsewhere in this document.

Employee log-on IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the business /organisation. Supervisors/ managers shall immediately and directly contact the IT manager to report change in employee status that require terminating or modifying employee log-on access privileges.

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the business/ organisation's cyber security officer. Monitoring of the special access accounts shall be undertaken via the periodic generating of reports to the cyber security officer showing who currently has a special access account, for what reason, and when it will expire.

Special accounts will expire in 30 days and will not be automatically renewed without written permission.

All computers and devices used by the user that are connected to the [Name of business Organisation] internet/ intranet/extranet, whether owned by the user or [Name of business/Organisation], shall be continually executing virus- scanning software with a current virus database approved by the cyber security officer.

Malware protection software must not be disabled or bypassed, nor the settings adjusted to reduce their effectiveness.

Automatic daily updating of the malware protection software and its data files must be enabled.

All email attachments must be scanned. All documents imported into the computer system must be scanned. Weekly scanning of all computers should be enabled.

A record of the antivirus and anti-malware software should be kept.

Desktop computers in areas of public access should be physically secured by cables and padlocks.

Where possible, sensitive data should not be removed from the business organisation's premises without specific authorisation.

Where this is not feasible, data on laptops that may leave the organisation's premises should be protected by full disk encryption.

Alternatively, staff who need access to sensitive data offsite should be given remote access privileges subject to adequate safeguards.

Computers being deaccessioned (whether for sale, reuse or disposal) shall not be released until all data has been securely deleted.

Users shall not download unauthorised software from the internet onto their PCs or workstations.

Users must use extreme caution when opening email attachments received from unknown senders; these may contain viruses, malware or Trojan horse code.

Users who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their [business organisation designee] immediately. The user shall not turn off the computer or delete suspicious files.

Users must not themselves breach security or disrupt network communication on the business/organisation's systems or elsewhere. Security breaches include accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties. "Disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Users shall not attach unauthorised devices to their computers unless they have received specific authorisation from their manager or the company IT designee.

Optional

Only authorised devices may be connected to the business/organisation's network(s). Authorised devices include PCs and workstations owned by company and compliant with the configuration guidelines of the company. Authorised devices also include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network non-company computers that are not authorised, owned or controlled by company.

Users shall not attach to the network any unauthorised storage devices; e.g. thumb drives, writable CDs.

Related Documents

- Confidentiality policy
- Acceptable use of Electronic Media Policy
- Technology Procedures Manual

Authorisation

[Signature of Director CEO]

[Name of Director/CEO]

[Date]

Acceptable use of electronic media policy

Procedure number	<<insert number>>	**Version**	<<insert number>>
Drafted by	<<insert name>>	**Approved by board on**	<<insert date>>
Responsible person	<<insert name>>	**Scheduled review date**	<<insert date>>

Introduction

[Name of business organisation] recognises that staff need access to email systems and the internet to assist in the efficient and professional delivery of services. [Name of organisation] supports the right of staff to have workplace access to the internet and email communications for reasonable personal use.

Purpose

This policy sets out guidelines for acceptable use of the computer network, including internet and email, by employees and volunteers of [name of organisation]. Access to internet and email is provided to [name of organisation] staff and volunteers for the primary purpose of assisting them in carrying out the duties of their employment.

Policy

Staff may use the internet and email access provided by [name of organisation] for:

- Any work and work-related purposes;
- Limited personal use (for details see Procedures, below);
- More extended personal use under specific circumstances (for details see Procedures, below).

Where staff use computer equipment or computer software at the premises of [name of business/organisation] or use computer equipment or software belonging to [name of business/organisation], properly authorised staff of [name of organisation] may access any data on that equipment to ensure that the business/organisation's policies are being adhered to. Such data should not be regarded as under all circumstances private in nature.

Authorisation

[Date of approval by the owner/ board]

[Name of business/organisation]

[Signature of owner/board Secretary]

Acceptable use of electronic media procedures

Procedure number	<<insert number>>	**Version**	<<insert number>>
Drafted by	<<insert name>>	**Approved by CEO on**	<<insert date>>
Responsible person	<<insert name>>	**Scheduled review date**	<<insert date>>

Definition

Electronic media includes all electronic devices and software provided or supported by [name of business/ organisation], including, but not limited to, computers, electronic tablets, printers, modems, fax machines, copiers, computer software applications (including software that grants access to the internet or email) and telephones, including mobile phones, smartphones and voicemail systems.

Responsibilities

It is the responsibility of the Director/CEO to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately.

It is the responsibility of all employees and volunteers to ensure that their use of electronic media conforms to this policy.

Processes

Limited personal use

Limited personal use of computer, internet and email facilities provided by the business/organisation is permitted where it:

- is infrequent and brief
- does not interfere with the duties of the employee or his/her colleagues
- does not interfere with the operation of [name of business/organisation]
- does not compromise the security of [name of business/organisation] or of its systems
- does not compromise the reputation or public image of [name of business/organisation]
- does not impact on the electronic storage capacity of [name of business/organisation]
- does not decrease network performance (e.g. large email attachments can decrease system performance and even cause system outages)
- corresponds to the procedures outlined in the Email Maintenance and Archiving Procedures document
- conforms to the practices for file management and storage outlined in the Technology Procedures Manual
- incurs no additional expense for [name of business/ organisation]
- violates no laws
- does not compromise any of the confidentiality requirements of [name of business/organisation]
- does not fall under any of the “unacceptable use” clauses outlined below.

Examples of what would be considered reasonable personal use include:

- conducting a brief online banking transaction, or paying a bill
- sending a brief personal email, similar to making a brief personal phone call.

Permitted extended personal use

It is recognised that there may be times when staff need to use the internet or email for extended personal use. An example of this could be when a staff member needs to use the internet to access a considerable amount of material related to study they are undertaking.

In these situations it is expected that:

- the staff member will advise and negotiate this use with their manager beforehand in order to obtain the manager's approval
- the time spent on the internet replaces all or part of a staff member's break/s for that day, or they adjust their timesheet accordingly for that day.

Access to electronic data

[Name of organisation] may need to access any and all information, including computer files, email messages, text messages and voicemail messages. The organisation may, in its sole discretion, authorise its staff to inspect any files or messages recorded on its electronic media at any time for any reason.

Where use of the organisation's equipment or software requires the use of a password, this should not be taken to imply any right of privacy in the user. The organisation may also recover information that a user has attempted to delete, and staff should not assume that such data will be treated as confidential.

Unacceptable use

Staff may not use internet or email access (including internal email access) provided by [name of businesss organisation] to:

- create or exchange messages that are offensive, harassing, obscene or threatening
- visit websites containing objectionable (including pornographic) or criminal material
- exchange any confidential or sensitive information held by [name of business/organisation] (unless in the authorised course of their duties)
- create, store or exchange information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies)
- conduct online gambling or online gaming
- conducting a business
- conduct illegal activities
- create or exchange advertisements, solicitations, chain letters or other unsolicited or bulk email.

Staff may not use [name of business/organisation]'s computers to play games at any time.

Related Documents

- Email Retention and Archiving Policy
- Technology Procedures Manual
- Cyber security policy

Appendix 2: Explaining the terms

A handy explanation of the technical terms.

Adobe Acrobat Reader	Software that allows you to view a PDF document (a document that can be seen but not easily changed). It can be downloaded free of charge from Adobe.
Asymmetric digital subscriber line (ADSL)	A type of digital subscriber line (DSL) broadband technology that is used to connect to the internet. It uses standard telephone lines to deliver high-speed data communications (up to 24 megabytes per second).
Analogue	This is a conventional method of transmitting data. Standard landline telephones use analogue technology. It is distinct from digital technology, which provides for greater quality and speed of data transmission.
Application, app	Software designed for a particular task, such as Word, Excel, Pandora or ABC iview. Originally the term "application" was used for computer software and "app" for mobile phone software, but today the two terms are often used interchangeably.
Assistive technology	Refers to any software or hardware that acts to assist and improve the functional capabilities of people with disabilities. Examples include wheelchairs, prosthetics, voice-to-text technology and text-to-speech technology.
Attachment	A document sent with an email message. Many types of files can be sent this way for example, Word documents, PDFs, Excel files, JPEGs. Be wary of attaching large files because these can take a lot of time for the recipient to download. If you have a large file, it is considered good practice to compress the file using software such as Winzip before attaching it to an email. Criminals will sometimes send malicious attachments containing malware.
Back-end	The part of an application that performs an essential task not apparent to the user.
Backward compatible	If software is backward compatible, it is compatible with earlier (superseded) versions of the same software. For example, the Microsoft word-processing program Word 2010 can read files created in the 2003 version of the same program, so it is backward compatible.
Bandwidth	Refers to the maximum amount of data per second that can travel a communications path in a given time.
Bit	This is short for binary digit. A Bit is the smallest unit of measurement in computing. Eight bits make up one byte.
Bitcoin	One of several kinds of digital currency which exists online and outside the domain of traditional banks. You can buy bitcoins with ordinary money. The value of the bitcoin fluctuates from time to time. It is in theory anonymous and untraceable - making it a popular form of exchange for criminals, including professional hackers. If you get a ransomware demand, the criminals will probably want to be paid in bitcoins.
Bluetooth	A wireless communications technology intended to replace cables. It allows short-range connections between two or more Bluetooth compatible devices such as mobile phones, tablets, headsets or medical equipment.
Bookmark	A saved link to a particular Web page. Microsoft Internet Explorer denotes bookmarks as "favourites."
Boolean operators	Most search engines, such as Google, allow you to limit your search or make it more specific by using words such as "and", "or" and "not". These words are known as boolean operators because of their origin as terms in logic.

Boot (re-boot)	To boot (or re-boot) means to load and initialise the operating system on a computer. Think of it as starting up your computer. In Windows you can use the key combination CTRL and ALT and DEL as a "soft" boot. This means restarting the computer rather than turning it completely off and on again, which could cause damage to your computer's hard disk under some circumstances.
Bounce back	When an email message cannot be delivered and returns an error notification to the sender it is said to "bounce back". If you receive this error notification, check that you have typed the address correctly.
Broadband	A type of communications technology where a single wire can carry more than one type of signal at once; for example, audio and video. Cable TV is one technology that uses broadband data transmission.
Browser	A software program that allows you to use the World Wide Web on your computer, tablet or mobile phone. Popular web browsers include Google Chrome, Safari, Mozilla Firefox, Microsoft Edge and Internet Explorer.
Cache	When you download (read) a web page, the data is "cached," meaning it is temporarily stored on your computer. The next time you want that page, instead of requesting the file from the web server, your web browser will access it from the cache, so the page loads quickly. The downside to this is that if the cached web page is often updated, you may miss the latest version. If you suspect that the web page you are seeing is not the latest version, go to Settings > clear history > empty cache to refresh the cache.
Computer-aided design (CAD)	Software that allows users to create 2D and 3D design and modelling. CAD is used by architects, engineers, artists and other professionals to create precise technical drawings.
Chip	A microprocessor that performs many functions and calculations that make your computer run. Your computer's chip is also referred to as the CPU (Central Processing Unit) or the processor.
Cloud computing	Refers to the storing and accessing of data and programs over the internet instead of on another type of hard drive. Examples of Cloud services include iCloud, Google Cloud and Dropbox.
Compression	Refers to the reduction of the size of a file. Compressed files take up less memory and can be downloaded or sent over the internet more quickly.
Content	Refers to a website's text and information, as opposed to its design and structure.
Cookie	A piece of code or data created by a web server and stored on a user's computer. It is used to keep track of the user's usage patterns and preferences.
Central Processing Unit (CPU)	The brains behind your computer. The CPU is responsible for performing calculations and tasks that make programs work. The higher the speed of a CPU, the faster the CPU undertakes the calculations and tasks.
Cyber crime	Any type of illegal activity that is undertaken (or relies heavily) on a computer. There are thousands of types of cyber crime, including network intrusions, identity theft and the spreading of computer viruses.
Cyber security	Refers to measures designed to protect your computer, device or network from cyber crime. This involves preventing unintended and unauthorised access, change and damage.
Device driver	A small program that allows a peripheral device such as a printer or scanner to connect to your PC.

Domain	A set of computers on a network that are managed as a unit.
Download	This is how users access and save or "pull down" software or other files to their own computers from a remote computer via the internet.
DV	Stands for digital video.
Email / electronic mail	A way of sending messages over the internet. Popular email programs include Outlook, Mozilla Thunderbird, Gmail and Yahoo Mail.
Encryption	The process of converting electronic data into an unrecognisable or encrypted form - one that cannot be easily understood by unauthorised parties.
Ethernet	The most common way of connecting computers on a network with a wired connection. It is a type of local area network (LAN) technology, providing a simple interface for connecting multiple devices.
Firewall	A barrier that acts as a security system to protect trusted computer systems and networks from outside connections and untrusted networks, such as the internet.
File transfer protocol (FTP)	A common method of transferring files via the internet from one host to another host.
Gateway	A point within a network that interconnects with other networks.
Information Technology (IT)	The use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
Graphics Interchange Format (GIF)	A graphics file format. As GIF files are compressed, they can be quickly and easily transmitted over a network. GIF is one of the main graphics formats on the internet.
Hard disk	The physical place where a computer stores information (applications and files) is known as its hard disk drive (HDD). The bigger the HDD, the more data it can store.
Hyper-text markup language (HTML)	A set of symbols inserted into files intended for display on the World Wide Web. The symbols tell web browsers how to display words and images, for example which colour, font and type size to use. The symbols are also used to direct web browsers to link to other pages on the World Wide Web via hyperlinks.
Internet	A set of interconnected networks that allow computers in different locations to exchange information. The internet includes services such as the World Wide Web, electronic mail, file transfer protocol (FTP), chat and remote access to networks and computers.
Internet Service Provider (ISP)	A company that provides access to the internet. In Australia, widely used ISPs include Bigpond, iinet and Dodo.
Intranet	This is a private, internal internet specific to an organisation or group.
Java	A programming language commonly used in the development of client-server web applications.
Joint Photographic Experts Group (JPEG)	This is the format commonly used for photos displayed on the World Wide Web. The initials JPEG comes from the name of the committee that created the file format.
Local Area Network (LAN)	This is a system that connects computers and other devices that share a common communications line and wireless link, generally within a limited geographical area such as a home or office building.

Malware	Short for malicious software. It refers to a software program that has been developed to do harm to other computers. Types of malware include viruses, worms and spyware.
Megabyte	A measure of a computer processor's storage and real and virtual memory. A megabyte (Mb) is 2 to the 20th power bytes, or 1,048,576 bytes in decimal notation.
Megahertz	The unit used to measure the speed of a computer's processor, for example 2800Mhz or 2.8Ghz.
Modem	This is a hardware and software package that allows computers to transmit information to each other via telephone lines, cable and WiFi.
Online	If a computer (or computer user) is online, it means it is connected to a network or to the internet. "Online" also refers to resources and services available on the internet, for example online banking.
Operating system (OS)	This is the software that manages all of a computer's processes and allows programs and applications to run. The most common operating system is Microsoft Windows. Others include Mac OS X and Linux.
Portable Document Format (PDF)	A file type created by Adobe Systems Inc. PDFs can be read using free software called Adobe Acrobat Reader or another PDF reader.
Phishing	This is a type of email fraud where the criminal sends out emails that appear to come from a legitimate service or reputable company, such as a bank or an email service provider. The aim of these emails is to get recipients to reveal confidential information that the criminal can use for their financial advantage – for example, online banking login details and password – or to download malicious software.
Plug-in	A software plug-in is a component that adds to a software program's functionality.
Post Office Protocol (POP)	Is an internet protocol used by your Internet service provider (ISP) to handle email. A POP account is an email account.
Pages per minute (PPM)	Generally refers to the speed of a printer.
Processor	This is the brains of your computer. It is responsible for performing calculations and tasks that make programs work. The faster the processor, the faster the computer works.
Protocol	This is a standard or set of rules that computers and other devices use when communicating with one another.
Random Access Memory (RAM)	Is usually referred to as a computer's "memory" as it stores information used by programs. Generally, the larger your computer's RAM, the more programs it can run at once without slowing down.
Read-only	A read-only file cannot be edited, modified or deleted.
Resolution	This refers to the number of distinct pixels that make up the display on a computer monitor. It is referred to as DPI (dots per inch). The higher the resolution, the finer and smoother the images appear when displayed at a given size.
Read Only Memory (ROM)	This is the part of a computer's memory that cannot be changed by a user. The contents of ROM remain even when the computer is turned off.
Software-as-a-Service (SaaS)	This is a software distribution model where software applications are centrally hosted and licensed on a subscription basis.

Search engine	Enables a computer user to search information on the internet. It is a type of software that creates indexes of databases or internet sites based on the titles of files, keywords, or the full text of files. The most popular search engines are Google, Yahoo and Bing.
Secure Sockets Layer (SSL)	A computer protocol that allows internet users to send encrypted messages across the internet. A web address that begins with "https" indicates that an SSL connection is in use.
Search Engine Optimisation (SEO)	This is the practice of making adjustments to a website to try and improve its ranking on search engines.
Server	A computer that handles requests for data, email, file transfers, and other network services from other computers.
Spam	Unsolicited email messages sent for marketing purposes.
Trojan horse	Any malicious computer program that misleads a user about its true purpose in order to hack into a computer. The term is derived from the Ancient Greek story of the wooden horse that was used to smuggle Greek troops into the city of Troy.
Unzip	To unzip a zip file means you can extract and decompress compressed files from it. If you are sent a zip file via email, you will need to unzip it before you can access the files inside it.
Unique Resource Locator (URL)	A URL or web address is the string of characters you type into a browser to access a particular website or other resource on the internet. For example, www.commbank.com.au
Viral	If an online video, photo or article "goes viral", it experiences a sudden spike in popularity in a short period of time.
Virus	A piece of programming code inserted into other programming to cause damage. Viruses can be sent in many forms but are often transmitted via email messages. When the email is opened, the virus may erase data or cause damage to your hard disk. Some viruses are able to enter your email system and send themselves to other people in your list of contacts.
Web server	The package of machine and software that stores, processes and delivers your web pages. Most large organisations have their own; most small organisations have them run by the company that looks after their web hosting package.
Wired Equivalent Privacy (WEP)	A security protocol used in WiFi networks. It is designed to provide a wireless local area network (LAN) with a level of security similar to that of a regular wired LAN. WEP-secured networks are usually protected by passwords. (See also WPA.)
WiFi	Technology that allows computers and other devices to communicate via a wireless signal.
WiFi Protected Access (WPA)	A security protocol used in WiFi networks. It is an improvement on WEP because it offers greater protection through more sophisticated data encryption.
Zip	To zip files is to archive and compress them into one file of a smaller size using a program such as WinZip. It is a handy way to make files smaller before sending them via email.

Commonwealth Bank

Committed to Indigenous Australians

At CommBank we strongly believe in the principle of shared values and highly value our relationships with Australia's First Nation Peoples. We acknowledge the traditional owners of this Land and show respect for Elders as the custodians of Country and Culture, and we remain firmly committed to reconciliation.

Our aim is to promote social, economic and financial inclusion, as well as the achievement of economic financial independence for Aboriginal and Torres Strait Islander peoples. Under the guidance of Elders Aunty Lilla and Aunty Mary from BlackCard, we have built a national team of culturally trained Indigenous Business Banking specialists. This training has provided us with a deeper understanding of Aboriginal culture, as well as the unique opportunities and challenges faced by Indigenous businesses and communities.

When combined with the skills and insights from across the wider Commonwealth Bank Group, this gives us the ability to deliver personalised, tailored services using Aboriginal terms of reference. It is a service which is delivered by our dedicated local bankers who have a strong focus on customer service, support, technology innovation, operational excellence, trust and respect.

A partnership with a difference

By providing efficient and innovative financial services, products and solutions, we work to support and economically empower Indigenous businesses. It is this commitment to applying our values to the way we work – with foresight, sensitivity, respect and experience – that we hope you get to experience with us.

ourcommunity.com.au
Where not-for-profits go for help

Who we are

Our Community is the engine room for creating and disseminating practical, affordable training, leadership and technological solutions that allow not-for-profit and grantmaking organisations to get on with the crucial work of building stronger communities.

Our partners in that work are not-for-profit organisations and social enterprises; government, philanthropic and corporate grantmakers; donors and volunteers; enlightened businesses; and other community builders.

We were one of the first companies in Australia to be accredited as a B Corporation, a process that provided external validation of our social credentials. In 2020 we ceased our B Corp accreditation in favour of legally mandating our social mission, becoming one of the first companies in Australia to enshrine our values in our constitution, which states: "commercial imperatives are afforded equal priority to our social mission, our commitment to employees, and our responsibility to the environment in which we work".

Our Community's offerings include:

- Institute of Community Directors Australia
  The best-practice governance network for the members of Australian not-for-profit and government boards and committees, and the senior staff who work alongside them - providing ideas and advice for community leaders.
- FundingCentre.com.au
  The best place to go to get and store information on grants and fundraising in Australia
- GiveNow
  Australia's most innovative giving platform - increasing donations to community causes, helping people become better givers, and providing a payment solutions hub for all not-for-profits.
- Good Jobs
  Connecting good people with social sector jobs, and providing HR support for not-for-profits.
- Communities in Control
  Australia's most inspiring annual community sector gathering: thought leadership for the not-for-profit sector
- SmartyGrants
  Software, data science and intelligence for revolutionary grantmakers - accelerating outcomes and impact.
- The Innovation Lab
  The engine room for sharing ideas and mobilising data science to drive social change
- Our Community House
  A co-working space for the social sector, where data and creativity come together to catalyse social change

The Our Community Group is evolutionary as well as revolutionary. Our websites and our services are always changing.

Our vision centres on social inclusion and social equity. Our dream is that every Australian should be able to go out their front door and stroll or wheel to a community group that suits their interests, passions and needs - or log on and do the same.

We want to help make it easy for people to join in, learn, celebrate, worship, plant trees, play a game, entertain and be entertained, care and be cared for, support others and be supported, advocate for rights and celebrate diversity. To get involved. To be valued.

This guide features elements of CommBank's Indigenous Business Banking design. It's our way of acknowledging cultural respect and understanding of Australia's First Peoples' sixty thousand plus year old culture and its history.

The work is based on an original design by a young artist Daikota Nelson, a proud Dja Wurrung woman who grew up and still lives on her traditional country in Castlemaine, Central Victoria.

The visual tells the story of caring for this great Land, and of the power of positive and lasting relationships. When viewed as a whole, the design represents all nations, tribes and individuals who inhabit and travel this great island nation. The underlying theme behind the work is that of the power and mutual benefits that can be achieved by Indigenous and mainstream Australians working together, supporting one another – based on a foundation of mutual respect and trust.

The design features a stylised map of Australia, overlaid with CommBank's logo. The outer path and footprints connecting the five larger circular elements symbolise the continuum of Indigenous Australians caring for the Land and the joining of mainstream Australians on this journey.

The scattered gum leaves around the outer edge of the work represent a welcoming to the Land; a cleansing and blessing for all – as we continue on our journey learning from one another, enriching our lives and growing from the experiences we share and the relationships that we form.

ourcommunity.com.au
Where not-for-profits go for help

INSTITUTE OF COMMUNITY DIRECTORS AUSTRALIA
Knowledge Connections Credentials

Commonwealth Bank