Not-for-Profit
Sector Banking

Damn Good Advice On Cyber Safety and Fraud Prevention

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

INSTITUTE OF
COMMUNITY DIRECTORS
AUSTRALIA
▸Knowledge ▸Connections ▸Credentials

CommonwealthBank

Damn Good Advice on Cyber Safety and Fraud Prevention

Published by Our Community Pty Ltd,

Melbourne Victoria Australia

Requests and inquiries concerning reproduction should be addressed to:

Our Community Pty Ltd

PO Box 354

North Melbourne 3051

Victoria, Australia

Please note:

While all care has been taken in the preparation of this material, no responsibility is accepted by the author(s) or Our Community, or its staff, or its partners, for any errors, omissions or inaccuracies. The material provided in this guide has been prepared to provide general information only. It is not intended to be relied upon or be a substitute for legal or other professional advice. No responsibility can be accepted by the author(s) or Our Community or our partners for any known or unknown consequences that may result from reliance on any information provided in this publication.

ISBN: 978-1-876976-53-8

First published: May 2014. This edition published July 2019.

Not-for-Profit Sector Banking

Damn Good Advice On Cyber Safety and Fraud Prevention

CommunitySmart

This book is part of the CommunitySmart program, a national financial literacy program developed by Commonwealth Bank Not-for-Profit Sector Banking and the Institute for Community Directors Australia (part of the Our Community group of enterprises).

Good governance and strong financial management are essential to the strength and sustainability of every one of our nation's 600,000 not-for-profit groups and schools.

Through CommunitySmart, we're working to help strengthen not-for-profit sector governance and financial management by providing practical advice for not-for-profit organisations and their staff, board members and volunteers.

A plain English guide to staying safe online

Over the past 20 years, not-for-profit organisations have been transformed as the internet has become an integral element of fundraising, communicating, researching, grantmaking, philanthropy, interacting with like-minded people, and coming up with great new ideas.

That's all good – but the internet is not a risk-free environment. Fraudsters are out to steal your organisation's data, access your financial systems or disrupt your activities. If the worst happens, the losses could be significant. Your organisation's reputation could be tarnished, your normal operations interrupted or even stopped dead in their tracks.

Fortunately, staying safe online can be achieved without a massive outlay of money and resources.

Some measures are easy, requiring little more than regular housekeeping. Other measures involve investing in computer hardware and software and specialist expertise. And many risks can be mitigated with a small investment in educating the people within your organisation.

The challenge is getting your head around what you're trying to protect yourself from and taking a risk-based approach. This means assessing how your organisation and your staff members (if you have any) and your volunteers operate online, and understanding the associated risks.

This handbook has been designed to help make your job in doing all that a little bit easier. And its companion guides, *Damn Good Advice for Board Members* and *Damn Good Advice for Treasurers*, can help to improve your understanding of your organisation's finances. All these publications are part of CommunitySmart, the national financial literacy program run by the Institute of Community Directors Australia (part of the Our Community group of enterprises), in partnership with Commonwealth Bank Not-for-Profit Sector Banking.

CommunitySmart is one example of how we are working to revolutionise banking for not-for-profit organisations. CommunitySmart is about going beyond everyday banking to provide extra value for the not-for-profit organisations to whom we owe so much as a community.

Commonwealth Bank is a proud partner of Our Community. This unique relationship is a great example of how collaboration can bring real value and thought leadership to the community sector. A particular thanks goes to Commonwealth Bank's Cyber Security Team who shared their specialist knowledge and insights and were instrumental in making this guide possible.

We are proud of the legacy that has already been created. Better bank accounts, new financial literacy tools, and greater understanding of the roles that board members and CEOs play in our community organisations are among the benefits that have been produced and sustained. But there's much more to be done. We look forward to joining with you and others in your position to ensure we get it right.

Price

Julienne Price
Head of Schools and Not-for-Profit Sector Banking
Commonwealth Bank

CommonwealthBank

Moriarty

Denis Moriarty
Group Managing Director
Our Community

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

Contents

Page

1.

Cyber security: why should we be concerned?

It's a tough old world out there. Here you are doing good for humanity and making the world a better place, and there are people around who instead of patting you on the back are more interested in picking your pocket. Even not-for-profits have to beware of fraud.

The 2015 Not-for-Profit Finance & Governance Insights report, published by the Institute of Community Directors Australia (ICDA), found that 6% of community groups had experienced fraud in the past three years (and another 8% didn't know or wouldn't say). Large organisations were the most at risk, with their rate at 15%. Losses ranged from a few hundred dollars to a quarter of a million, with the average at $34,000.

Considering they're a public-spirited lot of community heroes, not-for-profits can be pretty reluctant when it comes to bringing down the hammer. Only 35% of groups said they'd reported the fraud to police, and 58% came right out and said they hadn't. This is no way to keep the sector safe, and the first item in your fraud policy should be a commitment to following it up all the way.

Most of the fraud experienced – 79% – came from inside the organisation. The most important thing you can do to guard yourself against fraud is to tighten up your financial control procedures and check regularly to see that they're being enforced.

If you want to know how exactly you should do that, get a copy of our book on not-for-profit finances, Damn Good Advice for Not-for-Profit Treasurers (see https://www.ourcommunity.com.au/files/DamnGoodAdvice.pdf, and download the relevant financial control policies from ICDA's policy bank (see http://tinyurl.com/jjao35j).

In this guide, however, we're zeroing in on preventing the 21% of fraud attempts that come from outside organisations, and more specifically on your cyber security: help make sure people can't get at you through your computers and your internet connections.

Not-for-profits are making use of the full potential of modern technology for their administration, their mission, and their fundraising, and every opportunity brings its own risks. The wide world of the internet now reaches into almost every computer on every desk in every office. We can reach almost every person on earth instantly, and if we can reach them they can reach us. The more things your organisation does on its computers, or online, the more damage that malicious people or organisations or gangs can do to you if they get access. Just like the offline world, the online world presents opportunities for fraudsters. But there are a number of things you can do to stay a step ahead of them, and we set them out in the pages that follow.

Awareness is the key. If you and your organisation's people are all vigilant about fraud, you're in a strong position to manage it.

In a well-run not-for-profit, the board knows enough about cyber security to be reasonably satisfied that matters are under control, the CEO knows enough to know what has to be done and to identify someone with the skills to do it, and the person on the pointy end – the one who actually has to set up the defensive systems – knows all about it or can get a specialist in. Of course, in some not-for-profits one person or a few people carry out all of these tasks, but the principle remains the same: the people governing and managing a not-for-profit must know enough about cyber safety to be comfortable that the organisation has the right safeguards in place.

This book isn't intended as a technical coding manual, and it would go out of date pretty quickly if it was (and every computer setup requires its own set of solutions). It's intended to give you – as a board member, or as a manager – an overview of what cyber problems your organisation might face, and the sort of solutions you might put in place to address them.

> “
> # CYBER WHAT?
>
> **Adjective: Internet-related, computerised; as in cyber security, cyber war, cyber commerce, cyberdyne.**
>
> **Boomers read it as “newfangled”.**
>
> **Gen Xers read it as “high-tech”.**
>
> **Millenials leave off the “cyber” prefix altogether – they've never known the non-cyber version of anything.**
> ”

2.

How big is the risk?

Cyber security is a real problem, and it's a problem for organisations of all types and sizes.

There are international criminal gangs with the expertise and the networks to try to rip off large multi-national companies, and there are casual backyard operators who are sufficiently hungry to try to take a bite out of smaller targets like you. Large organisations often spend millions on their cyber security, even hiring hackers of their own to test the locks, and you're going to have to loosen the purse strings a little yourself.

If the Australian Bureau of Meteorology's defences can be breached (see http://tinyurl.com/z7v5twb), or the Australian Bureau of Statistics' (remember the Census debacle of 2016?), your organisation's can be too. What did anyone want with the weather reports, you ask? Perhaps nothing. One commentator suggested, "They're looking for the weakest link and maybe there are weaknesses they can exploit which will enable them to then move into other, more highly valued targets."

The attacker may not even be interested in you, but that doesn't mean they can't hurt you. They may want you to be a part of their invisible zombie army. Any computer compromised by malicious software (malware) has the potential to be invisibly conscripted into networks of other compromised internet-connected computers, known as botnets. Botnets are used to send spam, steal information, distribute malware and conduct such larger scale attacks as bringing down networks by swamping them with traffic.

Your computers may be pulled into a botnet network without you even knowing it. It might not seem that bad for you, actually – you may simply notice your computer running a little more slowly than usual – but it stuffs up the system big time. 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 don't want to enable that kind of abuse.

Losing money to cyber crime is one thing; losing your good reputation to it is another. In 2015, the UK's Women's Resource Centre, an umbrella body for women's charities, found that its website's homepage had been replaced by a page stating "I love Isis & Jihad" and an accompanying promotional video. However unfairly, the group's reputation suffered.

Welcome to the 21st century.

Security by obscurity, or "it can't happen to us"

Being a small target 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-techworld/).

Not-for-profit organisations were randomly targeted and their websites were either taken offline or defaced. They included NSW Family Planning, the Children's Tumour Foundation of Australia, the Freedom Project, South Australia Police Legacy and the Rats of Tobruk Association of Victoria.

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

Financial loss as a result of cyber crime

In the past three years, has your organisation experienced any financial loss as a result of cyber crime?

2.5%	91.3%	6.2%
Yes	No	Don't know; won't say

How much has been lost to cyber crime?

$250	$25K	$9.3K
Lowest reported loss from cyber crime	Highest reported loss from cyber crime	Average reported loss from cyber crime

Source: 2015 Not-for-Profit Finance & Governance Insights report, published by the Institute of Community Directors Australia (ICDA).

The question that nobody can answer is, "What's the chance I'm going to get hit by a serious attack?" Even if you take all possible precautions, your organisation's reputation can still be affected by criminal elements. The better your reputation, in fact, the more likely it is that some nasty piece of work will start sending emails out in your name with your logo pretending to be you and trying to get access to other networks. There's 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.

3.

Cyber risks at a glance

Computer hijacking

A computer hijacking occurs when an attacker takes control of 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. You won't see a balaclava-clad hijacker sitting in front of your computer in your ergonomic chair. Instead, they'll launch their attack by remote control, and you won't necessarily even know it's happening.

Cyber impersonation

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

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 13).

Email hacking

If your email account is hacked, it means somebody gains unauthorised access to your email account. Then they can impersonate you (by sending out emails in your name) or get access to all the information stored in any of your email. This could even lead to blackmail attempts – i.e. 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 for money or giggles.

Online account hacking

If your group uses Facebook, Twitter, Instagram, Survey Monkey, Formstack, Mailchimp, online banking, or just about any other online service – and what organisation doesn't use at least one of these? – then you're 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 destroy your good reputation.

Phishing

Phishing is a type of email fraud in which the perpetrator 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 lure recipients into revealing confidential information that the perpetrator can use for their financial advantage – for example, your organisation's online banking log-in details and passwords.

Privacy breach

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

Ransomware

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

Stealing your money

If an attacker finds the right files, they may learn your bank or credit card details, and they can then plunder your assets. Again, this can happen in any of the ways described here.

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 is derived from the Ancient Greek story of the wooden horse that was used to smuggle Greek troops into the city of Troy.

Virus

A computer virus 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) and then starts to replicate itself and do damage. In this way, it's like a common cold virus that infects your body – the virus finds its way in and then makes you feel unwell as it multiplies. Different computer viruses have different symptoms and spread at different speeds – some make themselves known immediately (e.g. by damaging all your files or using up all your computer's memory), while others are programmed to remain dormant for a period and then start replicating and doing damage.

Website hacking

This doesn't mean your organisation's website develops a phelgmy cough. It means an unauthorised party takes control of your website. The attacker could be anyone from a bored teenager who replaces the text on your homepage with unsavoury messages, to a disgruntled former volunteer who posts defamatory comments, to a criminal gang that busts into your online donations system and steals all your financial information so that they can transfer all your funds.

4. Who's responsible for cyber security?

Cyber security is not an IT problem: it's an organisation-wide issue.

It's natural to want to be able to hand over responsibility for all the elements of a cyber security program – risk management and mitigation, resource allocation decisions, policy enforcement and so on – to a clearly defined senior manager who has the knowledge and authority to nail it all down. But whether you're a small scouting group or a large national charity, that's not going to be enough – not nearly.

Your IT people, if your organisation is large enough to have such a team, are going to be an important part of the solution, it's true. An effective IT person or section will help ensure your systems are robust and can translate complex technical information about cyber security risks into tangible advice.

However, you can't just hand it to them and walk away. A collective, all-in, hands-on approach to staying safe and secure online is much more effective than dropping all the risk – and if something goes wrong, all the blame – on one person and washing your hands of the responsibility. We all need to understand how to protect our data, how to use the internet securely and how to use email safely. Little things can make a big difference.

Cyber protection isn't like a city wall, which you can rely on without much thought. It's more like a city glasshouse, in which everybody has to avoid throwing stones.

Start up!
Plan
ea

5.

Who’s out to get us?

When it comes to cyber crime, the baddies are a varied collection, ranging from disgruntled former employees bright bored teenagers to national governments. The threats may even come from within. What they have in common is that they’re all the kinds of people who, when passing a door, will automatically try the handle, just in case. They’re unprincipled, they’re opportunistic, they’re unsleeping, and they’ve had a lot of practice.

Employees

Employees and volunteers can be involved in almost any security threat, whether through ignorance, negligence or carelessness. Very occasionally, they are the baddies themselves, taking advantage of their local knowledge and their access privileges to rip out your money or your data. Your security systems have to be able to 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 haven’t 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’ll exploit it to plant viruses and Trojan horses (see page 13) or to use the resources of your system for their own purposes. If they don’t find an obvious weakness they’ll probably move on to an easier target.

Some hackers just want to see things break, which is bad enough. Worse still, though, is a hacker who has a grudge against your organisation specifically. If you work in a contentious area (and it only takes one combative person to make any area contentious), you may attract people who are willing to put considerable time and effort into bringing you down by taking over your website, corrupting your data, or exposing your secrets. It's known as hacktivism. If you have any reason to expect anything like this, increase your threat rating to "elevated" and review your defences more regularly.

Criminal hackers and saboteurs

The probability of a criminal attack is low, but not entirely negligible given the amount of sensitive information contained in databases. 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 tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into an organisation's computers.

Criminals, furthermore, have their own infrastructure. If they do find personal information in your data systems, they know where to sell it.

There have even been instances of attackers accessing data on internal networks, encrypting it, and demanding a ransom in untraceable bitcoins 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. (Read the full story here: http://tinyurl.com/j8wdly5.)

Given the complexity and interconnectedness of our computer systems, it's simply impossible to make any system 100% secure. Even if your systems themselves are perfect, there's still a human element involved – people can and do make mistakes. But that's no reason not to try for absolute security.

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 wails, "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 won't bother with you because the effort is too great. The bear will almost always go for the easiest target.

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

6.

What's vulnerable to cyber attack?

Physical equipment is relatively easy to protect – but when you think about it, the data on devices is far more valuable than the actual equipment. The technology and information systems of 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, for example) and custom software applications you've commissioned specifically for your 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 and intellectual property.

Digital assets audit

Putting a cyber security plan in place starts by understanding what it is you're 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 donor database need to be strongly protected. On the other hand, while your corporate logo is an important asset, chances are it's already widely distributed in the public domain. It doesn't make sense to put the same extremely strong protection around access to your logo as you do around confidential personal donor data.

Once you delve into what data needs to be protected you'll quickly realise that not all data is equally important and not all staff members have the same needs. For example, it may be appropriate for everyone to have access to company logos but for only select people to be allowed to edit them.

A not-for-profit organisation will typically possess the following assets. How valuable are yours, and how well are they protected? Use this tool to conduct an audit.

Data	Value	Vulnerability	Protection method	Responsibility of
Administrative data				
Payroll records	High	Medium	Password protected; bank details encrypted; access limited to CEO and relevant staff	Treasurer/finance section
Transaction records	High	Medium		
Program records	High	Medium		
Identity data				
Staff records	High	Medium	Password protected; data encrypted; access limited to CEO and relevant staff	HR section
Volunteer records	Medium	High		CEO
Fundraising database	High	Medium	Password protected; credit card numbers encrypted; access limited to CEO and relevant staff	CEO
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
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 the organisation, and the general complexity of the system.

7.

Check your culture

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.

What counts in this context is the culture of the organisation. Everybody takes this seriously or nobody does. Top-down dictation probably won’t work, and may be counterproductive; if your staff think they’re getting their own back on the boss by going to strange websites during working hours then you’re asking for trouble.

You have to show you take cyber security seriously by putting in the resources and doing the training. If security isn’t almost instinctive it’ll be trampled in the rush. You have to pick up small breaches before they become massive breaks in the dam wall, and you have to rap the knuckles of those responsible.

Mind you, you don’t want to discourage people from reporting breaches, either. Policing by itself isn’t enough. Ideally, your lever should be positive incentives. It’s hard to get into the habit of rewarding people for doing it right, because that means you have to hand out awards for absolutely nothing happening, but it’s worth it. You have to offer your staff and volunteers incentives in line with your cyber security profile. And if you’re a tiny volunteer-run organisation you have to sell it to them one by one and day by day.

Another point to note is that it’s hard to convince other people to follow the rules if you as a board member or manager are not pretty squeaky clean yourself. This means, among other things, that you shouldn’t be using unlicensed software, even if it is much cheaper than the legitimate version. You might be eligible for a discounted version through Connecting Up (www.connectingup.org). Even if you’re not, legitimate software is a lot safer and more reliable, and comes with helplines.

Similarly, don’t use intellectual property – online text or graphics, for example – unless it’s clear that it’s not under copyright. Don’t spam people with unsolicited email, even if you think they may make a donation. Don’t, under any circumstances, sell people’s data to anyone else – that’s not just unethical, it’s illegal. Do as you would like to be done by.

8.

Put someone in charge

Wanted: One tech-savvy angel

A basic position description for a cyber security officer would list:

Essential skills

Computers

- Advising on computer purchases (hardware and software); setting up computers; maintaining networks; installing software; setting up accounts; troubleshooting problems; reviewing security
- Maintaining database systems
- Ensuring data back-ups

Internet

- Setting up internet connections; maintaining networks; reviewing security

Website

- Advising on systems; monitoring interface; reviewing security

Desirable skills

Computers

- Expertise in commercial applications (e.g. Excel, SQL); training staff in applications; administering applications; database management

Internet

- Arranging online back-ups; training staff

Website

- Handling website design; updating and managing content; training staff to update and manage content

Social media

- Expertise in using social media; training staff

If you've got a fully qualified IT section, you've probably got someone who has all these skills and can apply them to the role of cyber security officer. If you're a smaller organisation, your tech person is also going to be your cyber security person. If your group is too small to have an IT person, you should still nominate someone to be the go-to person in relation to your organisation's cyber security and privacy.

You'll have to give your cyber security person the clout necessary to override any institutional inertia, but make sure they consult widely and keep their finger on the pulse of the office.

This person may not be an expert, at least to begin with[1] but they should have an interest in and some knowledge of the topic and be prepared to put a bit of time into educating themselves (as long as they can get on to the internet, they'll find the answer somewhere). They'll 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 members (if any) and volunteers are educated. They can also keep a keen eye on the latest cyber threats and keep everybody informed in appropriate non-technical terms.

In a volunteer organisation you're looking for a jack-of-all-trades who can work out what's needed, set it up, and help people use it. They'll have to be self-educating, self-starting, and self-monitoring. They'll need good people skills, particularly in training areas, with the ability to cope calmly with silly questions, stupid mistakes, and unnecessary disasters.

You're probably going to find it difficult to get someone exactly like that, and everybody else is going to have to cope with someone learning on the job, making mistakes, and doing the best they can. To keep grumbling to a minimum, let it be known that anybody who demonstrates informed criticism will be conscripted to help.

[1] If you can find someone from the IT area to take on the cyber security role, so much the better – but don't hold off until an expert comes along.

9.

Embed cyber security in policies and procedures

Trust the process, not the person.

You can mitigate the cyber security risks posed by staff and volunteers – those who remain oblivious to the risks as well as those who want to act maliciously – by:

- Allowing access to IT systems, computers, laptops, e.t.c. only to people who really need it
- Promptly removing or limiting the access of anyone who 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 pitched at the level of the naïve user, and go through it with your board members, staff and volunteers as part of their induction.

If you're a very small volunteer-run organisation, you might be wondering how this applies to you. But so long as your group has a Facebook page, or maintains a list of members' email addresses, or uses Internet banking, you face the same risks as a larger group with paid staff and inhouse IT experts. The consequences of a cyber security breach might be smaller, and your manual might be correspondingly 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 new volunteer showing an unusually high level of interest in the online banking records, or a staff member who unwittingly records all the passwords on her desktop because she can't remember them otherwise.

Finance departments have long recognised the importance of segregation of duties. For example, you'd be mad not to keep your payables and receivables in separate teams so that there's no chance of one being used to defraud the other. Similarly, very few people need to have complete access to every single one of your 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 considerations. For example, systems that don't 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 32.)

See pages 60-68 for templated policies and procedures, and adapt them to your organisation's specific circumstances:

Cyber security policy (p61)

Cyber security procedures (p62)

Acceptable use of electronic media policy (p66)

Acceptable use of electronic media procedures (p67)

> “Whether you're a large or small organisation, you face the same cyber security risks.”

10. Passwords

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

There are a number of ways to break into 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, however, 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: ringing up the staff and asking them.

"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 in a jiffy and I won't have to bother you again."

It's 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 in.

As US cyber security expert Bruce Schneier told NetworkWorld magazine in 2003, "Amateurs hack systems; professionals hack people." The highest walls in the world won't protect your city if someone leaves the gates open or welcomes a wooden horse inside. Which, left to themselves, they tend to do. People take short cuts through minefields, eat pizza with blue mould from the back of the fridge, and text while driving. People use passwords like – well, have a look at these, 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

123456, password, 12345678, 12345678, 12345, 111111, 1234567, sunshine, qwerty, iloveyou, princess, ,admin, welcome, 666666, abc123, football, 123123, monkey, 654321, !@#$%^&*, charlie, aa123456, donald, password1, qwerty123.

The worst of it is that the people who typed in 123456789 probably felt they were being super-scrupulous compared to those who used 1234.

IT staff have a well-deserved reputation for being the kind of people who want you to have a 12-character password involving four numbers, no English words, and several uppercase special characters. And on top of all that, they'll tell you:

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

The thing is, they're right.

Many people, unfortunately, when faced with those requirements just shrug their shoulders and go back to "password".

Your organisation can try to find ways to encourage or force people to follow good password practices – through training them into understanding, or scaring them into submission, and keeping it up, year after year – or it can implement a technological fix. Specialised password management software (such as 1password.com) takes some of the hassle out of remembering multiple complicated passwords. However, these software options bring their own risks and organisations need to weigh these up, before recommending to staff.

In recent years we have seen advice around passwords change and evolve. It's 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, particularly when we need to remember hundreds at a time. It has also been proven that pass-phrases take longer to crack.

One more thing: if your organisation uses online services that are shared by multiple users, consider paying per user instead of taking the cheap option and having different users share one account. It will cost a little more, but it means passwords aren't 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.

Passwords: strong, safe and secret

Implementing a secure password policy is one of the simple steps you can take to protect yourself and your 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.
- Don't use words from a dictionary (including foreign words) – hackers will use dictionary-based tools to crack your secret. Short phrases are better than words.
- Don't 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, so don't share it and don't write it down.

11.

Training your people in cyber security

You'll need a layered training system, one that kicks in at several different points during an employee or volunteer's time with your organisation.

First, include cyber security training in your induction program for board members, volunteers and staff.

Second, provide a more detailed going-over for people once they've settled into the job and know the systems they're dealing with.

And third, and always, provide everybody with booster shots once a year or so.

None of this needs to entail boring two-hour seminars in a fluro-lit conference room. You might hold a series of lunchtime discussions on issues such as how to secure your Facebook account or how to recognise online scams. That personal touch can then be related, succinctly, 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 volunteer-run organisation, this might consist of a one-to-one session between, say, the outgoing treasurer and the incoming one, or between the coordinator of volunteers and a number of new volunteers.

In an 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 it.

If it's any consolation, most burglaries are pretty low-rent affairs and the computers often end up at the pawnbrokers still locked down. That said, many offices still don't take proper precautions – indeed, it's not at all unknown for departments to sell off old computers without wiping them, encrypting them, or protecting them with any password stronger than the name of your dog.

With laptops, the perpertrators don't even have to ramraid the office; they can just wait till your attention wanders at the coffee shop, pick up your bag, and walk out with your life. You can leave your laptop on the train, and whoever gets off the train last gets to keep it. You can leave it in a taxi, giving the driver a rather larger tip than you planned. One data analyst from a US government department had his laptop nicked with 26 million personal records on it and so far it's cost the US about $200 million to tidy up after him.

One American study found that 600,000 laptops were lost or stolen at US airports every year[1]. The really odd thing though is that 65% of the ones that were handed in remain unclaimed. That's a lot of data floating around.

[1] Ponemon Institute, Airport Insecurity: The Case of Missing & Lost Laptops (see http://tinyurl.com/6ggple), June 2008.

Bring Your Own Device (BYOD)

Odds are that you and your organisation's employees use your own smartphones, tablets and laptops for work purposes some of the time. This practice, known as BYOD, or bring your own device, offers advantages such as allowing people to use gear they're comfortable and familiar with to access work-related emails, documents, and programs. And it has the potential to save your organisation money too.

But what does BYOD mean for the security of your organisation's data? What does it mean for your network's risk of attack by malicious software? What if a board member leaves her iPad in a taxi, or an employee resigns from the organisation, taking with him a hard drive full of confidential documents on his own laptop? What if the chair's kids have access to his tablet and they post the minutes of the latest board meeting to Facebook?

There are policy and technical solutions to these problems. Typically, policy solutions involve ensuring that users secure their devices with passwords and passcodes; and technical solutions involve a secure repository of apps and data that can be remotely erased if the device is lost or an employee leaves, potentially without removing any of the user’s personal data.

When you're identifying digital assets and creating a customised security plan to match, it's imperative 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) to 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're not visible from public areas
- Lock up rooms with computers in them at night.

None of that, obviously, works for off-site laptops, where the risk is that they'll be lost or stolen because people are careless. It's very, very difficult to have policies against absent-mindedness, because by definition people are not thinking about the policy when they do the thoughtless thing. You have to take other steps to compensate.

1. You can forbid people from taking data out of the office.

   This is the safest course, if it's feasible; but these days it often isn't. The boundaries between work life and home life are thinner and more ambiguous than they used to be, and many people do work from home.

2. You can demand that any data taken out of the office is encrypted.

   This is a compromise, requiring as it does more work from the employee, making it probable that some proportion won't do it.

3. You can forbid people from carrying data out of the office but make it possible for them to access information from the office remotely.

   This is also a compromise, in that it means you have to punch holes in your defences to allow access to employees, but it may be preferable; you can place strong password requirements on entry, and after a breach you can at least identify more or less who came in from their network credentials along with network logs.

4. You can require 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
- Ensure that 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 gets taken) or install tracking software on your laptop.

Understand how to remotely access your fileserver, mail server, or desktop securely – if you're not sure, consult with IT (if you don't have an IT department, you probably won't be able to use remote access anyway and are thus pretty safe).

Increasingly, of course, we're erasing the old distinctions between computers and other devices like mobile phones and tablets, meaning that the cyber attack problems we've discussed above are now turning up in your pocket.

While this is a fast-developing field, begin by taking the same precautions on your phone as you would on your computer – watch out for phishing texts, turn it off when you're not using it, notice if it starts behaving oddly, don't leave it in the café, don't use it for anything that's really sensitive. You might want to consider using an encryption app such as Signal, Wikr me or Proton Mail (note that the person who's messaging you has to have the same app installed).

13.

The weak points: software

Malicious software, or malware, is software used to gather private information, disrupt computer operations or gain unauthorised access to 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've 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's 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 Centre Security (ACSC) in 2017 published The Essential Eight, which can help mitigate cyber security incidents:

- Application whitelisting of approved/trusted programs to prevent execution of unapproved or malicious programs.
- Patch applicaitons: 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).
- Restrict admin privileges based on user duties.
- Multi-factor authentication: implement for all users when accessing an important data repository.
- Daily backups: make backups of important data.

It's important to realise that 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. Then there's the compromise between ease of use, functionality and security. If you design a large system for ease of access it's 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, too, 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 potentially jumps 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 device zombiefies into a botnet facilitating massive cybercrime.

It's surprising it doesn't happen more often, really.

Protecting your software

There are many things your 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's 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's 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're always protected from the latest threats.

There are many reputable security software companies out there, 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's 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 the research that will help you to narrow the field from dozens of options to just two or three.

You get what you pay for. Free software might seem like a bargain, but its functionality is often restricted. The good news is that many security software vendors offer heavily discounted or free versions of their commercial products to not-for-profit organisations. A modest investment now could save you big dollars in the future. Connecting Up (www.connectingup.org) offers some great solutions at reduced prices for not-for-profits.

Keep your software – especially operating systems and browsers – up-to-date. Most modern applications automatically check for the latest updates, but it's prudent to ensure 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 WPA (WiFi protected access, a security protocol) to secure your wireless network. The Stay Smart Online website provides some good advice on securing wireless networks (see http://tinyurl.com/j4cr5r5).

Encourage everyone to use strong passwords. Using weak passwords is like hiding the keys to your house under the front doormat – convenient, yes, but with a high risk of provoking difficult conversations with your insurers. For more on passwords, see page 28.

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. Gmail users have the same option.

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

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.

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 a tight rein on what’s installed on your organisation’s computers significantly reduces the risk of malware.

14. Protecting against phishing

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

Phishing attacks send what looks like a legitimate email containing links that either fool 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 copy of the bank's website. Once you enter your username and password, that party knows you're a customer of the bank and has your login credentials.

To help ensure your organisation doesn't become a victim of phishing, ensure 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 don't know or arrives unexpectedly or seems out of place. If you're 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.
- Don't share confidential information, account numbers or passwords.
- Let your colleagues know if you do receive a suspicious email – chances are you won't have been the only one.
- If you receive an unsolicited or suspicious email, don't click on any links in the email, and don't open any attachments.
- Remember the old adage – if it seems too good to be true, it usually is.
- If you're 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 deal. And they're becoming more and more sophisticated all the time. 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 con lower-ranking staff into transferring large sums of money to them.

Europol said such fraudsters 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 includes 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 a whitelist of approved IP addresses (see the SPF, DKIM and DMARC standards).

15. Protecting your website

Spammers

To preserve your organisation's good reputation, you need to protect your website from unauthorised use.

If it has a comments section – and it really should, because that's the best way to invite the involvement of your sympathisers and stakeholders – your main problem is going to be spamming. People are going to swarm like wasps to fill your comments section with advertisements for payday loans and counterfeit handbags. This isn't one of the really major risks to you, as an organisation, but those links could lead others to fraudulent websites. It's pretty simple to fix this, but it does involve more work. Every comment must be approved before it goes up. Someone has to be responsible for checking incoming messages for the section at least once or twice a day.

Every interactive element on your page – filling out forms, for example, or uploading files – is a potential security breach and requires additional technical protection. If your public can talk back to you, you have to be sure that they're not giving instructions to your computers. Require your users to sign in with a password.

Keep your default permissions stern so that unauthorised outsiders can't 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.

Crooks can launch a DDoS attack against anybody, big or small. There's 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 organisation from a DDoS attack:

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

- Don't 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/publications/preparing-for-and-responding-to-denial-of-service-attacks).

Privacy Setting
Edit
Terms and conditions

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 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 I have?

The cloud providers all have massive security apparatuses, but remember what we told you: there's 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 go with the rest – and while you can certainly point out to your members and clients that it's not your fault, they may still hold a grudge.

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 ever you need to retrieve it, how long will this 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's 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 not-for-profit uses a US-based company to store its data offsite, and that company's servers are in Singapore. Hypothetically, the organisation could find itself in a situation where it is required to protect personal information to comply with the Australian Privacy Principles, and simultaneously to provide that information to a law enforcement agency overseas.

If your organisation deals with personal information – and almost every not-for-profit does – then you should seek legal advice before storing your data overseas.

Is my data going to be encrypted?

When you're 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 won't be able to read the data themselves because they won't 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’s how it works.

Three

Three is the number of copies of your critical data you need to have at all times.

It’s reasonably easy to achieve. For a start, there’s the master copy of your data on your computers and servers. Second, you can set up a back-up regime 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.

Two

Two is 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’re already using two different media – the original data and the back-up copy or copies.

One

One is the minimum number of copies 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’re taken offsite at the end of the back-up process. If the worst should happen and there’s a theft or your offices are damaged by a fire or flood, then the back-up of your data will be safe.

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

Zero

Zero is the number of errors your back-ups should contain. All the back-ups in the world aren’t worth a thing if they’re 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 hasn’t been working. Unfortunately, they usually find this out the hard way.

Back-up technology is becoming cheaper and easier to use, so backing up data doesn’t have to be a laborious chore. Most back-up programs can be “set and forget”. Just don’t forget to test your system.

18.

Documentation: your cyber security manual

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

Whether your organisation is large or very, very 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's a breach (disaster recovery plans).

If you're a small community group, the manual might run to one or two A4 pages – that's fine.

If you're a very large organisation with lots of staff, then besides the whole-of-organisation manual, you're probably also going to need section-by-section manuals covering the particular needs of each area.

Whatever your size, you'll 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 unending; you may feel you're doing a lot of running to stay in the same place.

There are, however, a wealth of information sources to help you. In addition to following mainstream news, hook into 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

An excellent example is the Commonwealth Bank's security site (see http://tinyurl.com/zdaywk5). You can also subscribe to the Commonwealth Bank's 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://tinyurl.com/oyrppv4), if you don't mind a daily dose of such information.

Scamwatch

Scamwatch.gov.au is a treasure trove of up-to-date information and tips on how to avoid the latest scams. Get in the habit of checking in with 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 – Facebook, Twitter, LinkedIn and the like – are making up a larger and larger part of human interaction, and your organisation can't really opt out. You should have a social media presence, despite the risks involved.

This requires careful handling, and you'll need to have approval processes in place so that nobody tweets casual thoughts in your name that conflict with your policies or principles. You'll have to decide for yourself what you'll do if the commentators on your posts criticise you (it's probably best to leave it up there but post a reasoned response) but you mustn't let them put up anything that's obscene, or bigoted.

Your organisation should have a social media presence to do its job. Your staff probably don't, but they'll have one anyway. Make sure they're aware of the risks. As the Australian Cyber Security Centre (ACSC) says (https://www.cyber.gov.au/publications/security-tips-for-social-media):

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 and volunteer cyber security training. Tell your staff, if you have staff, to report anything extra suspicious to the cyber security officer.

●●●●○ Vodafone TR 3G
3:20 PM
83%
Social
Instagram
Facebook
Twitter
3
WhatsApp
Me
YouTube
Skype
Periscope
Foursquare

21. Online banking: is it safe?

It is imperative that you protect your organisation's bank accounts by making it necessary for more than one person to authorise withdrawals from them – definitely, positively, no exceptions.

Letting one person sign cheques is equivalent to sticking a "kick me" sign on your back. Well, the same goes for online banking. You'll need to set things up so that every online transaction is authorised by more than one person. It's slightly more involved than counter-signing a paper cheque, but it's every bit as necessary.

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

Under this system 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?

Cyber security risks are like other organisational risks, and every organisation is different. Your investment in cyber security will depend on how reliant you are on IT.

Some organisations have a small digital footprint, while others have IT and computers at their core. As a rule of thumb, the more dependent you are on IT, the more effort you should devote 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 can go as high as 15%. It's unlikely that your risk profile is going to come anywhere near that, but for most Australian not-for-profits even 1% would be a huge hit.

That said, developing good procedures and policies for security, investing in security software and keeping your software up-to-date all go a long way to making your organisation as small a target as possible. Cyber security does not need to cost a fortune, but vigilance is important. To put it another way, there's 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 can't carry on your work as usual, you're on your own financially.

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

Susceptible information includes credit card numbers, list of donors, client lists and employee profiles.

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

Trent Youl from the cyber security firm FraudWatch International told a 2015 Our Community conference that class-action lawsuits relating to the theft of personal data in cyber attacks were inevitable and that Australian not-for-profits need to be prepared.

Insurance coverage specifically for cyber-incidents is still the exception, not the norm, for Australian not-for-profits and even for the business sector, although its prevalence is increasing. Check your policy.

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

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

> “If your organisation is attacked and your data falls into the wrong hands, or you can't carry on your work as usual, you're on your own financially.”

24. Be prepared: plan and practise

What if, despite your best efforts, your organisation has become the victim of a cyber security incident? Don't panic! Preparation is the key to riding out the cyberstorm.

We suggest practising 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've had first aid training, you'll 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 exacerbate 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 assessing what has gone wrong. This includes understanding how the attack occurred, what systems were affected and the extent of the incident. If you've 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.

Appoint someone to take charge of managing the incident. This isn't 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 at least to stop any further leakage of information and data. If you need help, you can contact CERT Australia (www.cert.gov.au).

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 affected 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/).

If you're a CommBank customer and you suspect fraudulent activity has taken place, you should call our dedicated CommBiz helpdesk on 13 23 99.

Keep in mind that while admitting to a breach might be embarrassing, it's much better that you let your staff, customers and other stakeholders know before they find out on the grapevine or, worse yet, through the media.

Lastly, and perhaps most importantly, when the dust has cleared, get your key people together and thoroughly examine what went wrong. History doesn't need to repeat itself. Draw up a plan, implement the changes and protect yourself.

APPENDIX 1:

Template policies and procedures

Please note that these are template policies for guidance only. Our Community has partnered with Moores who can tailor these policies to suit your organisation. Through the Our Community partnership with Moores, not-for-profit organisations are able to access training or legal advice in this area at a pre-agreed price. For more details call Moores' NFP-Assist Legal Hotline on **(03) 9843 0418** or email: **NFPassist@moores.com.au**.

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 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 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 Organisation] wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the 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 board secretary]

[Date of approval by the board]

[Name of 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 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 CEO is kept aware of any changes to the organisation's cyber security requirements;
- a report on the organisation's cyber security is submitted annually to the board.

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 CEO may authorise individuals with responsibility for cyber security issues in the 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 CEO shall from time to time issue cyber security procedures appropriate to different levels of confidentiality.

The 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 Organisation data allowing banking or financial exploitation	Client credit card and banking data Organisational credit card and banking data Client details that would facilitate phishing
Green	Client data allowing address or email exploitation Organisational intellectual property that has financial or reputational consequences	Addresses that would facilitate spamming Information that the 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 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 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 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 Organisation] internet/intranet/extranet, whether owned by the user or [Name of 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 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 [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 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 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 CEO]
[Name of 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 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 organisation] or use computer equipment or software belonging to [name of organisation], properly authorised staff of [name of organisation] may access any data on that equipment to ensure that the 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 board]

[Name of organisation]

[Signature of 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 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 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 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 organisation]
- does not compromise the security of [name of organisation] or of its systems
- does not compromise the reputation or public image of [name of organisation]
- does not impact on the electronic storage capacity of [name of 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 organisation]
- violates no laws
- does not compromise any of the confidentiality requirements of [name of 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 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 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)
- undertake 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 organisation]’s computers to play games at any time.

Related Documents

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

APPENDIX 2:

A–Z of technology terms

Don't know your bandwidth from your back-end? Here's a handy glossary of tech terms.

Adobe Acrobat Reader

Acrobat Reader is 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.

ADSL

Asymmetric digital subscriber line (ADSL) is 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

Analogue 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

An application or app is a piece of software designed for a particular task, such as Word, Excel, Pandora or ABC iview. Traditionally, the term "application" was used for computer software and "app" for mobile phone software, but the two are now often used interchangeably.

Assistive technology

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

An attachment is a document sent with an email message. Many types of files can be sent this way (e.g. 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.

Back-end

Back-end refers to 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

Bandwidth refers to the maximum amount of data that can travel a communications path in a given time, usually measured in seconds.

Bit

A bit (short for binary digit) is the smallest unit of measurement in computing. Eight bits make up one byte.

Bitcoin

Bitcoin is one of several kinds of digital currency, existing online 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 theoretically anonymous and untraceable, making it the favoured medium of exchange for criminals, including professional hackers. If you get a ransomware demand, the criminals will probably want to be paid in bitcoins.

Bluetooth

Bluetooth is 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 bookmark is a saved link to a particular Web page. Microsoft Internet Explorer denotes bookmarks as "favourites."

Boolean operators

Most search engines (e.g. 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) is 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

An email message that cannot be delivered and returns an error notification to the sender is said to "bounce back". If you receive such an error notification, check that you have typed the address correctly.

Broadband

Broadband is a type of communications technology whereby 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 just accesses 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're seeing is not the latest version, use the "refresh" button on your browser.

CAD

Computer-aided design (CAD) is a type of 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 chip is 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

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

Compression is 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

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.

CPU

The central processing unit (CPU) is 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

Cyber crime is 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

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 device driver is a small program that allows a peripheral device such as a printer or scanner to connect to your PC.

Domain

A domain is a set of computers on a network that are managed as a unit.

Download

Downloading is the method by which users access and save or "pull down" software or other files to their own computers from a remote computer via the Internet.

DV

DV stands for digital video.

Email

Email or electronic mail is a way of sending messages over the internet. Popular email programs include Outlook, Mozilla Thunderbird, Gmail and Yahoo Mail.

Encryption

Encryption is the process of converting electronic data to an unrecognisable or encrypted form, one that cannot be easily understood by unauthorised parties.

Ethernet

Ethernet is 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 firewall is 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.

FTP

File transfer protocol (FTP) is 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.

GIF

Graphics interchange format (GIF) is a graphics file format. Because 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.

HTML

Hyper-text markup language (HTML) is 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 – e.g. 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.

ISP

An internet service provider (ISP) is a company that provides access to the Internet. In Australia, widely used ISPs include Bigpond, iinet and Dodo.

Intranet

An intranet is basically a private, internal internet specific to an organisation or group.

Java

Java is a programming language commonly used in the development of client-server web applications.

JPEG

JPEG stands for Joint Photographic Experts Group, which was the committee that created the file format known as JPEG. The format is commonly used for photos displayed on the World Wide Web.

LAN

A local area network (LAN) 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

"Malware" is 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 computer processor 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

Megahertz is the unit used to measure the speed of a computer's processor (e.g. 2.8Ghz).

Modem

A modem (“modulator-demodulator”) 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 is currently connected to a network or to the Internet. “Online” also refers to resources and services available on the Internet – e.g. online banking, online dictionary.

Operating system

An operating system (OS) is the software that manages all of a computer's processes and allows programs and applications to run. The most prominent operating system is Microsoft Windows. Others include Mac OS X and Linux.

PDF

Portable document format (PDF) is a file type created by Adobe Systems Inc. PDFs can be read using free software called Adobe Acrobat Reader or another PDF reader.

Phishing

Phishing is a type of email fraud in which the perpetrator 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 lure recipients to reveal confidential information that the perpetrator can use for their financial advantage – for example, online banking log-in details and passwords.

Plug-in

A software plug-in is a component that adds to a software program's functionality.

POP

A 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.

PPM

Pages per minute (PPM) generally refers to the speed of a printer.

Processor

The processor 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

A protocol is a standard or set of rules that computers and other devices use when communicating with one another.

RAM

Random access memory (RAM) is usually referred to as a computer's "memory" – 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

Resolution refers to the number of distinct pixels that make up the display on a computer monitor. It is denoted in DPI (dots per inch). The higher the resolution, the finer and smoother the images appear when displayed at a given size.

ROM

ROM stands for read-only memory. It 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.

SAAS

SAAS stands for software as a service. It is a software distribution model whereby software applications are centrally hosted and licensed on a subscription basis.

Search engine

A 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.

SSL

SSL, or secure sockets layer, is a protocol that allows Internet users to send encrypted messages across the Internet. It is generally used when transmitting confidential information (e.g. personal data or credit card details). A web address that begins with "https" indicates that an SSL connection is in use.

SEO

SEO, or search engine optimisation, is the practice of making adjustments to certain aspects of a website in an effort to improve its ranking on search engines.

Server

A server is a computer that handles requests for data, email, file transfers, and other network services from other computers.

Spam

Spam refers to unsolicited email messages sent for marketing purposes.

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 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 is to 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.

URL

A URL (unique resource locator) or web address is the string of characters you type into a browser to access a particular website or other resource on the Internet (e.g. https://www.ourcommunity.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 virus is 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 that, when opened, 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

A web server is 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 handles their web hosting package.

WEP

Wired equivalent privacy (WEP) is 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 WAP.)

WiFi

WiFi is a technology that allows computers and other devices to communicate via a wireless signal. Essentially, it means you can browse the Internet without tripping over phone cords.

WPA

WiFi protected access (WPA) is 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 smaller size using a program such as WinZip. It's a handy way to make files smaller before sending them via email.

CommonwealthBank

About Not-for-Profit Sector Banking

Our purpose is to improve the financial wellbeing of our customers and communities. For more than 100 years, we've been supporting Australian communities including the not-for-profit organisations that help to sustain and strengthen them. Our goal is to help drive efficiencies that will deliver maximum benefit to your cause.

A partnership with a difference

We're focused on continuing to redefine the modern banking relationship with our not-for-profit clients, providing each with the ability to access and leverage resources that would often be beyond their financial reach. These resources include:

- The latest technology and products to help reduce administration, get funds into your organisation faster and stay in real-time control of funds.
- Dedicated Innovation Labs, innovation teams and not-for-profit innovation specialists to support your organisation deliver both new and existing services.
- Think tanks and masterclasses featuring the latest in design thinking methodologies.
- A range of training programs and expert consulting teams including cyber security and data analytics.

Specialist bankers

Our national team of not-for-profit sector bankers have been specifically accredited in not-for-profit sector banking, enabling us to work in close partnership with community organisations. We remain focused on deepening our bankers' knowledge and expertise through offering training in the Institute of Community Directors Australia's Diploma of Business (Governance).

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

The Our Community group provides advice, connections, training and easy-to-use tech tools for people and organisations working to build stronger communities. Our partners in that work are not-for-profit organisations and social enterprises; government, philanthropic and corporate grant makers; donors and volunteers; enlightened businesses; and other community builders.

A Certified B Corporation and multi-award-winning social enterprise, Our Community's offerings include:

- **OurCommunity.com.au** – Australia's centre for excellence for the nation's 600,000 not-for-profits and schools: where not-for-profits go for help
- **Institute of Community Directors Australia** – the best-practice governance network for the members of Australian not-for-profit boards, committees and councils, and the senior staff who work alongside them
- **FundingCentre.com.au** – the best place to go to get information on grants and fundraising in Australia
- **GiveNow.com.au** – commission-free online donations for not-for-profits, and philanthropy education and tools for businesses, families and individuals
- **Good Jobs** – Connecting good people with social sector jobs, board vacancies and internships
- **Communities in Control** – Australia's most inspiring annual community sector gathering: thought leadership for the not-for-profit sector
- **Australian Institute of Grants Management** – information, inspiration and education for government, philanthropic and corporate grant makers
- **SmartyGrants** – software and data science for revolutionary grant makers
- **Australian Institute for Corporate Responsibility** – creating and facilitating authentic connections between enlightened businesses and their communities
- **The Innovation Lab** – the engine room for sharing ideas to drive social change

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

INSTITUTE OF
COMMUNITY DIRECTORS
AUSTRALIA
▸Knowledge ▸Connections ▸Credentials

CommonwealthBank

072019