



# Damn Good Advice on Cyber-safety and Fraud Prevention



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

Proudly supported by: **CommonwealthBank**



## **Damn Good Advice on Cyber-safety and Fraud Prevention**

Published by Our Community Pty Ltd,  
Melbourne Victoria Australia

© Our Community Pty Ltd

This publication is copyright. Apart from any fair use as permitted under the Copyright Act 1968, no part may be produced by any process without permission from the publisher.

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

# **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.





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.

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

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 your staff.

There's an overlap, too, between Internet-based security risks and old-fashioned fraud. This handbook looks at both sets of issues.

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 operate online, and understanding the associated risks.

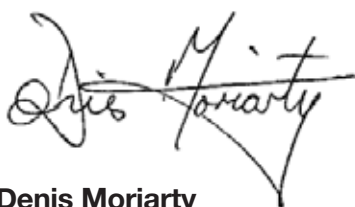
A good risk management framework has four components; this handbook encourages you to consider each component and act accordingly:

- 1. Resourcing:** how much money will we devote to cyber-security and fraud prevention?
- 2. Planning and prevention:** what steps will we take to prevent cyber-breaches and fraud from occurring?
- 3. Detection:** what systems and processes will we implement to enable us to recognise cyber-breaches or fraud if they occur?
- 4. Response:** what will we do if we detect a cyber-security incident or fraud?

This handbook has been designed to help make your job as a CEO, a senior staff member, a board member or – in a very small organisation – “the person who looks after IT” a little bit easier. This booklet's 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. 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.



**Denis Moriarty**

Group Managing Director  
Our Community



**Vanessa Nolan-Woods**

General Manager, Education and  
Not-for-Profit Sector Banking  
Commonwealth Bank



# Contents

	page
1. Isn't cyber-security a matter for the IT department?	8
2. Identifying your assets and making a plan	10
3. Protecting your organisation against malicious software	12
4. Protecting your organisation against data loss	14
5. Protecting your organisation against hackers	16
6. Protecting your organisation against phishing	18
7. Responding to a cyber-attack	20
8. Will cyber-insurance protect us?	22
9. Staying up to date on cyber-threats	24
10. Protecting your organisation against fraud	25
11. Trust the process, not the person	26
12. Use fraud detection software	27
13. Protect whistleblowers	28
14. Prevent online fraud	29
15. Educate your staff about scammers	30
16. Educate your staff about dealing with suspected theft	32

# 1

## Isn't cyber-security a matter for the IT department?

Cyber-security is not an IT department problem – it's a company-wide issue.

However, your IT department is likely to be an important part of the solution. An effective IT department or partner will help translate complex technical information about cyber-security risks into tangible business advice.

Taking a collective, all-in, hands-on approach to staying safe and secure online is much more effective than handing the risk or blame to one person and washing your hands of it. We all need to understand how to use the Internet securely and use email safely. Little things can make a big difference.

Every organisation should consider appointing a person responsible for cyber-security and privacy. They may not be an expert but they should have an interest in the subject. This person will be your first port of call for security issues and have responsibility for ensuring software is updated, information is appropriately secured, data is backed up, and your staff members are educated. They can also keep a keen eye on the latest cyber-threats and keep the business informed in non-technical, company-appropriate terms.





## Security by obscurity, or “it can’t happen to us”

Being a small target is no protection from online threats. In November 2013 a hospital and a number of charities had their websites [attacked](#) by Indonesian hackers during a diplomatic spat between Australia and Indonesia.

Not-for-profit organisations were randomly targeted and their websites were either taken offline or defaced. They included 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.

# 2

## Identifying your assets and making a plan

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 have 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.

Today's IT systems are more widely distributed than ever before. It's likely that some of your systems are hosted by service providers that store your data in data centres overseas in multiple locations. Already, then, you've entrusted the security of some of data to third parties.

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.

An important step in any security plan, then, is a thorough audit to identify which digital assets are critical to your organisation.

A not-for-profit organisation might typically possess these assets:

- fundraising database
- member database
- images (photos, product, infographics)
- electronically stored logos and other artwork
- audio and visual media
- media releases
- social media data.

When you know what you've got, you can create a customised security plan to protect your organisation's critical assets. Online tools from organisations such as the US Federal Communications Commission's [Small Biz Cyber Planner](#) and the Australian Government's Stay Smart Online [business assessment questionnaire](#) can help with this.

Your plan needs to be dynamic. That means you need to keep up to date with potential cyber-threats, which change all the time, and change your security plan accordingly.

You can subscribe to a cyber-alert service such as the one provided by the [Stay Smart Online](#) service to help you to understand the latest threats.

While you might need to review the overall plan at least once a year, or when there is a significant change to your organisation, we'd suggest quarterly or monthly reporting on the effectiveness of the plan.

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.

We'd also suggest practising what you plan to do in the event of a cyber-incident. Get the right people together and run some scenarios in a conference room: 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.

## Bring your own device (BYOD)

Odds are that you and your organisation's employees like to bring your own smartphones, tablets and laptops to work. 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 documents, files 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 loses her smartphone, 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 her tablet and they post the minutes of the latest board meeting to Facebook?

There are technical solutions to these problems. Typically, they involve creating 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 person'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 Department of Defence has a brief guide to the issues you need to consider: [http://www.asd.gov.au/publications/protect/BYOD\\_Considerations\\_for\\_Execs.pdf](http://www.asd.gov.au/publications/protect/BYOD_Considerations_for_Execs.pdf).

# 3

## Protecting your organisation against malicious software

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

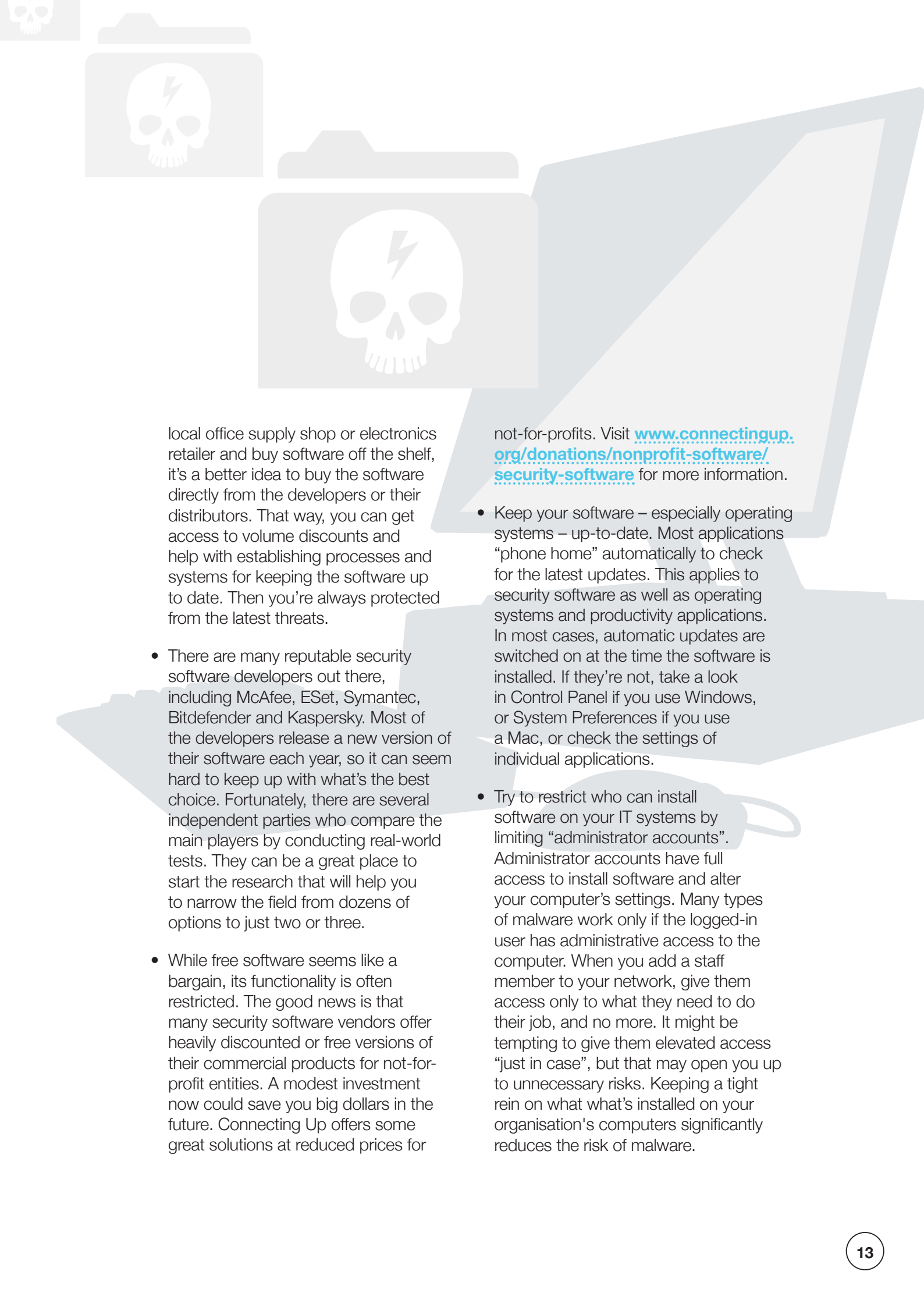
Spyware, adware, Trojans, worms and viruses are all types of malware. For example, banking malware can kick into action during an online banking session – it can alter a payment you've made so that it goes to someone other than the intended recipient, or capture your log-in credentials and send them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

Malware is often disguised as legitimate software. Once installed, it can be difficult to detect and remove. The good news is that keeping one step ahead of malware makers is not as hard as it sounds – it doesn't need to be costly, confusing or time-consuming.

It's important to realise that no software or hardware solution will be 100% effective 100% of the time. The bad guys only have to succeed once to breach your defences. So your security software needs to be able to not only block whatever threats it knows about, but also help fix any problems if something gets through your defences.

The following steps can help your organisation reduce the risk of exposure to malicious software:

- Installing Internet security software 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 developers 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 developers out there, including McAfee, ESet, Symantec, Bitdefender and Kaspersky. Most of the developers release a new version of their software each year, so it can seem hard to keep up with what's the best choice. Fortunately, there are several independent parties who compare the main players by conducting real-world tests. 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.
- While free software seems like a bargain, its functionality is often restricted. The good news is that many security software vendors offer heavily discounted or free versions of their commercial products for not-for-profit entities. A modest investment now could save you big dollars in the future. Connecting Up offers some great solutions at reduced prices for not-for-profits. Visit [www.connectingup.org/donations/nonprofit-software/security-software](http://www.connectingup.org/donations/nonprofit-software/security-software) for more information.
- Keep your software – especially operating systems – up-to-date. Most applications “phone home” automatically to check for the latest updates. This applies to security software as well as operating systems and productivity applications. In most cases, automatic updates are switched on at the time the software is installed. If they're not, take a look in Control Panel if you use Windows, or System Preferences if you use a Mac, or check the settings of individual applications.
- 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 your 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.

# 4

## Protecting your organisation against data loss

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 backups is the 3-2-1-0 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 backup regime where critical data is automatically copied to another computer, or, depending on your needs and budget, to a tape library system. Third, you can use a cloud storage system to replicate your data, or a service such as Carbonite or CrashPlan. For a charge, they will provide you with an offsite copy of your data.

### Two

Two is the number of different storage media you should use.

By using a cloud-based backup service or sending backup tapes offsite, you're already using two different media – the original data and the backup 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 backup tapes or an external hard drive for backups, you should ensure they're taken offsite at the end of the backup process. If the worst should happen and there's a theft or your offices are damaged by a fire or flood, then the backup 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 backups 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 backups should contain.

All the backups in the world aren't worth a thing if they're broken. One of the often-missed steps in backup processes is testing the recovery process. Many people think they have robust backup and recovery processes only to find out too late that something hasn't been working. Unfortunately, they usually find this out the hard way.

Backup technology is becoming cheaper and easier to use, so backing up data doesn't have to be a laborious chore. Most backup programs can be "set and forget". Just don't forget to test your system.

## Cloud computing: castles in the air?

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:

- 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 backup, 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 backup services 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.

# 5

## Protecting your organisation against hackers

A hacker is somebody who accesses your computer systems without permission or uses your computers or programs detrimentally.

Some hackers access systems by exploiting security flaws in software. Others do this by stealing or guessing log-in credentials or fooling people into sharing them.

Given the complexity and interconnectedness of our computer systems, it's simply impossible to make a system 100% secure. Even if your systems themselves are perfect, there's still a human element – people can and do make mistakes.

You might have heard the joke about the two people whose camp is attacked by a bear. When the two campers start running, one camper says to the other, "You can't out-run

a bear." The second camper replies, "I don't have to out-run the bear – I just have to out-run you."

The aim of security is to make your systems secure enough that hackers don't bother with you because the effort is too great. In other words, don't make it easy for them. Or do it better than others around you so the bear catches the others first.

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

- Use WPA (Wi-fi Protected Access, a security protocol) to secure your wireless



network. The Stay Smart Online website provides some good advice securing wireless networks: [www.staysmartonline.gov.au/computers/secure\\_your\\_internet\\_connection](http://www.staysmartonline.gov.au/computers/secure_your_internet_connection).

- 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.
- Keep your desktop and server software up to date. A significant proportion of corporate cyber-security breaches occur as a result of software flaws that would have been fixed months or years ago if the software had been kept up to date.
- Encourage everyone to use strong passwords. That means combinations of upper and lower case letters, number and symbols. Every year, security companies publish lists of the most hacked passwords, and every year combinations like "password" and "pass1234" are near the top of the list. Using weak passwords is like "hiding" the keys to your house under the front doormat.
- Consider using a system that provides one-time passwords. Yahoo! recently announced it would offer users an alternative to passwords. Instead, a user is sent a one-time code via SMS when they want to log in. This system 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.

## Passwords: strong, safe and secret

Creating a secure password is one of the simple steps you can take to protect yourself and your organisation online. This means:

- Make your password long – at least eight characters if possible
- Mix it up with 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 – don't share it and don't write it down.
- 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.

# 6

## Protecting your organisation 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 clearly a fake? That's a phishing attack.

Phishing attacks send what tries to look like a legitimate email with 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 log-in credentials.

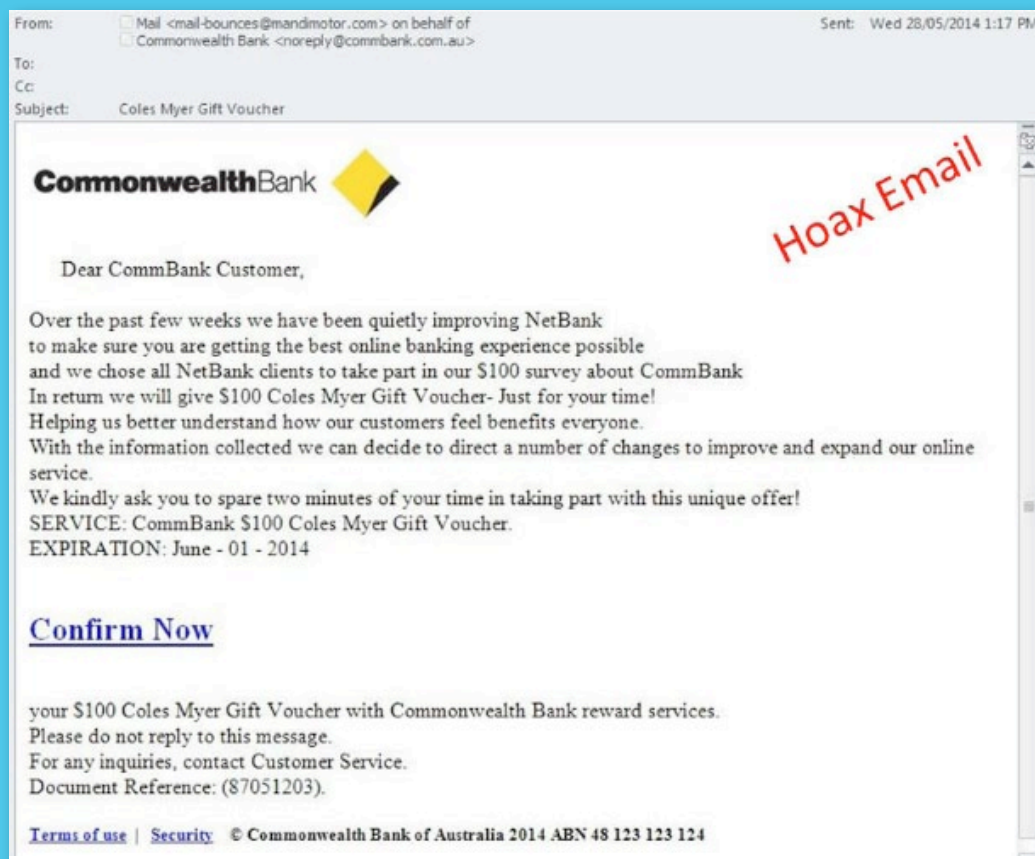
Think twice before you click on links in website pop-ups or emails – especially if the email is from someone you don't know or arrives unexpectedly or seems out of place. If you're

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.

To help ensure your organisation doesn't become a victim of phishing, follow these tips:

- If you receive an unsolicited or suspicious email, don't click on any links in the email, and don't open any attachments
- Don't share confidential information, account numbers or passwords unless you are sure you know who you are talking to
- Let your colleagues know if you do receive a suspicious email – chances are you won't have been the only one
- Remember the old adage – if it seems too good to be true, it usually is.

## 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 an email asking you to confirm, update or reveal your personal information.

Never click on a link in an email 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.



# Responding to a cyber-attack

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 cyber-storm.

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 make an assessment of 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. Often, this isn't a senior manager but the best person to deal with a cyber-security incident. Ideally, this is someone who can understand both the technical and business impacts 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](http://www.cert.gov.au)).

There is currently no requirement to notify affected individuals or 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, although the particular circumstances and potential consequences of each breach should be taken into account.

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.

## What to do if your website goes down

Websites can be subject to several different types of cyber-attack. DDoS, or distributed denial-of-service, attacks work by overwhelming a website or online service with massive volumes of unexpected traffic.

Often, DDoS attacks are linked to hacktivists – hacker-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.

If you find yourself the victim of a DDoS, attack visit CERT Australia ([www.cert.gov.au](http://www.cert.gov.au)) for practical advice and tools.

# 8

## Will cyber-insurance protect us?

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 business 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, 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 business – 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 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.

# 9

## Staying up to date on cyber-threats

Staying up to date on the latest-cyber trends and threats is easy.

There is a wealth of information to help you. In addition to mainstream news sources, consider the following resources:

- Large providers of cyber-security products are a good source of information. 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.
- Bookmark 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](http://www.cso.com.au) and [www.itnews.com.au](http://www.itnews.com.au).
- Your bank or financial institution is a key source of news and information on cyber-security. An excellent example is the [Commonwealth Bank's security site](#).
- If you don't mind a daily dose of such information, consider signing up to a cyber-security advisory and alert service such as the [Stay Smart Online alert service](#).
- The Australian Competition and Customer Commission's [Scamwatch](#) 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.
- The Australian Securities and Investments Commission ([ASIC](#)) and the Australian Prudential Regulation Authority ([APRA](#)) also offer consumer information designed to raise awareness of fraud and protect you against becoming a victim.



# Protecting your organisation against fraud

Fraud and scams can affect any organisation. Fraud can originate within your organisation, or outside it. Its likelihood and its impact will vary depending on the nature of your

organisation and the activities you undertake. It is a real and present risk for Australian not-for-profits – it's not something that should be left to trust or hope or chance.

## What is fraud?

Standards Australia defines fraud as:

“A dishonest activity causing actual or potential financial loss to any person or entity including theft of moneys or other property by employees or persons external to the entity and whether or not deception is used at the time, immediately before or immediately following the activity. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position.”

Source: Australian Standard AS 8001 (2008): *Fraud and Corruption Control*

# 11

## Trust the process, not the person

Establishing and following robust standard operating procedures allows you to identify abnormal or suspicious activities that may signal fraud.

Finance departments have long recognised the importance of segregation of duties. For example, 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.

# Use fraud detection software

Software is available to help with detecting fraud – for example, access and identity management programs can detect when someone is accessing data in an unusual way.

It might be normal for a financial controller to access the finance system between 7 am and 8 pm from the office or from home. But connecting to the system at 2 am from Russia would be odd, even if the username and password are correct. Access and identity management software can detect these sorts of anomalies and report them as they occur.



# 13

## Protect whistleblowers

Another way to protect your organisation is to establish procedures by which staff or the public can report serious fraud or unethical behaviour anonymously and safely – that is, a whistleblower policy or even a whistleblower hotline.

You can download a sample whistleblower policy as well as a fraud risk management policy from the Institute of Community Directors' Policy Bank (<http://www.communitydirectors.com.au/icda/policybank/>)

A 2014 global study of fraud by the US-based Association of Certified Fraud Examiners found that tip-offs were consistently and by far the most common fraud detection

method, with more than 40% of all cases detected this way. Employees accounted for nearly half of all tip-offs that led to the discovery of fraud.

Organisations with hotlines were much more likely to catch fraud by a tip-off than organisations without one. These organisations also experienced frauds that were 41% less costly, and they detected frauds 50% more quickly.

# Prevent online fraud

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.

- Avoid being a victim of identity fraud. Keep your personal details and passwords safe
- Keep up to date with trends in online fraud (see page 24)
- Keep your anti-virus software up to date
- Know who you are dealing with – especially online. Consider implementing identification procedures for all clients or customers to ensure you are not dealing with fraudsters pretending to be clients or customers

- Be wary of “phishing” emails (see page 19).

Your information and systems risk management framework should cover online fraud. Assess your business annually – more often if possible – to identify possible fraud risks and consider the controls you have in place to mitigate them.

Awareness is the key. If you and all the organisation’s staff are vigilant about fraud, you are in a strong position to manage it.

# Educate your staff about scammers

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.

Spend some time educating your staff in how to recognise scammers. This doesn't have to mean holding a boring two-hour seminar in a conference room. It could be a lunchtime discussion on how to secure your Facebook account and 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.

Remind everyone that the first line of defence in recognising a scammer is common sense. If it looks too good to be true, it probably is. If you receive an offer involving significant amounts of money, savings on goods or

services, time or commitment, always seek independent advice from a trusted third party. Remember:

- There are no proven get-rich-quick schemes
- Do not agree to offers or deals offered to your organisation without taking time to consider them
- If you still have questions or are uncertain about an offer you've received, contact your local [office of fair trading or consumer affairs agency](#), the Australian Securities and Investments Commission ([ASIC](#)) or the Australian Competition and Consumer Commission ([ACCC](#)) for assistance.



**Login**

admin

**Password**

● ● ● ● ● Sv43sd

# 16

## Educate your staff about dealing with suspected theft

Theft from an organisation can take many forms, including:

- Theft of cash or employee funds
- False sales or refunds and false reporting to cover up the fraud
- Stealing blank company cheques, forging signatures or altering written cheques
- Payroll fraud – making false payments to employees or making payments to “ghost” employees
- Expenses fraud – employees claiming personal expenses as business expenses
- Accounting fraud – employees hiding fraud through control of the organisation’s record- keeping books
- Conflicts of interest between an employee’s private business needs and their employer’s business needs. For example, an employee buying goods or services for the organisation at inflated prices from a supplier with whom they have a personal relationship.

If you suspect somebody is stealing from your organisation – whether it’s someone inside the organisation (a staff member or volunteer) or someone external (such as a supplier) – it is important you take timely action to help prevent further losses:

- Don’t approach the person yourself and don’t immediately investigate the matter yourself.



- Think: am I being reasonable?  
Run your suspicions by a trusted colleague or peer.
- Ask yourself: what is the basis of my belief? Are there any documents or other evidence to support my suspicions?
- Once you are satisfied your suspicion is reasonable, report the matter to the police. Let them know of any supporting documentation or evidence you have collected.

Ensure that your staff, too, are trained in what to do if they suspect someone is stealing from the organisation. Your procedure might require, for example, that they follow the first three steps above, and then report the matter:

- a. to you or to another manager or a senior person in the organisation
- b. to the human resources department, if you have one
- c. via your organisation's whistleblower policy, if you have one.

## Motivations: the occupational fraud triangle

The fraud triangle is a model for explaining the factors that cause someone to commit internal fraud, also called occupational fraud. It consists of three components that together can lead to fraudulent behaviour:

1. Motive (e.g. gambling losses)
2. Opportunity (e.g. autonomy over financial processes)
3. Rationalisation (e.g. "I will pay it back eventually").

The three elements of the fraud triangle can be seen in most, if not all, occupational frauds.



**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 grantmakers (government and philanthropic), donors, enlightened businesses, community builders, and – of course – not-for-profit organisations themselves.**

**A certified B Corporation and multi-award-winning social enterprise, Our Community offers:**

- [OurCommunity.com.au](https://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](https://instituteofcommunitydirectors.com.au) – 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](https://fundingcentre.com.au) – the best place to go to get information on grants and fundraising in Australia
- [GiveNow.com.au](https://givewith.com.au) – commission-free online donations for not-for-profits, and philanthropy education and tools for businesses, families and individuals
- [Australian Institute of Grants Management](https://australianinstituteofgrantsmanagement.com.au) – information, inspiration and education for government, philanthropic and corporate grantmakers, including Australia's most-used online grants management solution, SmartyGrants
- [Australian Institute for Corporate Responsibility](https://australianinstituteofcorporateresponsibility.com.au) – creating and facilitating authentic connections between enlightened businesses and their communities
- [The Innovation Lab](https://theinnovationlab.com.au) – the engine room for seeding ideas to drive social change by doing old things better or new things first



**Not-for-Profit  
Sector Banking**

### **Commonwealth Bank Not-for-Profit Sector Banking**

At Commonwealth Bank, communities are at the core of our vision: to excel at securing and enhancing the financial wellbeing of people, businesses and communities. For more than 100 years, Commonwealth Bank has supported Australian communities, including the not-for-profit organisations that help to sustain and strengthen them. And today we are making our banking solutions and service for our not-for-profit customers deeper and better than ever before.

In your world, it's the people who make the difference, and that's true in our world as well. At Commonwealth Bank, we have a dedicated Not-for-Profit Sector Banking Team, focused on tailoring our products and services to meet the needs of not-for-profit organisations, with smarter credit, reduced fees and the same focus on market-leading innovation we're recognised for. Our goal is to help drive efficiencies that will deliver maximum benefit to your cause.

Your banking is good hands thanks to our accredited not-for-profit sector bankers, our not-for-profit investment team, our specialist transaction bankers, our 24/7 on-shore service centre, and our dedicated switching team.





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