

# How to stay safe online

Last time we looked at some of the many threats to us as users of computing devices.

These range from direct attacks on personal and corporate computers to dolls that spy on young children.

Of course, all those that spy are not necessarily villains. Depends on your point of view.

You may not be aware that the Tax Office has employed a team of data mining specialists, or data doctors. Their role is to look online at social media sites such as Facebook and Instagram to determine if what people are posting matches with what they're reporting in their tax returns.

For example, some one might be posting photos of themselves relaxing in Byron Bay on a gorgeous January weekend and yet have lodged a claim for an overseas conference for that same time.

So warn your children.

## **BUT BACK TO THE REAL BADDIES**

Both criminals and government hackers are increasing their assaults, seeking money or advantage. Most of these people live in Russia, Romania, or China.

These hackers attack and steal valuable information from businesses and public authorities like hospitals, government departments and individuals like you and me.

Hackers can take advantage of all our feelings, even that of love.

For example, the Australian competition and consumer commission recently issued yet another warning about dating scams, revealing that mostly mature-age lonely Australians had lost more than \$25 million from romance scams in 2016 alone.

Research shows that our worst online habit is rarely changing our pin numbers (37% of users)

Other bad habits include accessing public Wi-Fi networks to use Internet banking (23%) and using "auto-fill" feature of many programmes to add personal information (22%)

Here's some tips on how you can fight back to protect your private data.

## **KEEP UP TO DATE**

Keep the operating system of your desktop computer, laptop, tablet or smart phone up to date. An unpatched machine is more likely to have software vulnerabilities that can be exploited

Most operating systems these days can be adjusted so that the system is updated automatically.

Microsoft and Apple have gone to great lengths to protect their OS by providing built in protection.

Both companies claim their protection is as good if not better than free or paid versions of commercial anti-virus software.

Dozens of free anti-virus programs like AVG or Avast are available. Most of them do a decent job of protecting your computer and network against common malware threats (viruses, spyware, etc.)

But the paid versions of these and other programs provide added protection, easier administration in business settings, and other benefits over their free counterparts.

And subscribe to the free Federal Government service called **Stay smart online** ([www.staysmartonline.gov.au/](http://www.staysmartonline.gov.au/)) for security alerts.

### **BE CAREFUL WHAT YOU SAY**

According to the latest Kaspersky Lab statistics, around 60 per cent of emails sent worldwide are spam. The vast majority of these spam emails are created to scam you of your hard-earned money.

So always ignore unsolicited emails, and be wary of attachments, links, and forms in emails that come from people you don't know, or which seem suspicious.

And when in doubt about anything, leave it out. IOW, don't click and don't reply

Be especially aware of unexpected emails with subject tags related to celebrities, holidays or current events.

Be on the lookout for emails from Telecommunication companies (Optus/Telstra etc), banks (Westpac, Commonwealth Bank etc), online payment services (PayPal, Western Union), mail companies (Fed EX or Australia Post) and the Australian Tax Office (ATO).

Make sure to **NEVER** give out your name, email, home address, phone number, account numbers or any other personal information about your family or your friends.

And of course never send funds or your financial details to someone you have met online, especially in a make friends chat room. Beware of what seem like loveable strangers asking you to send them for money orders or international funds transfers.

### **PROTECT SENSITIVE DATA**

Reduce the risk of identity theft. Securely remove sensitive data files from your hard drive, which is also recommended when recycling your computer.

Use the encryption tools built into your operating system to protect sensitive files.

Many programs offer the option of "remembering" your password. Don't let them - these programs have varying degrees of security protecting that information.

Close your browser after logging out to clear personal information from the browser memory. This is especially relevant if you use a public or shared computer (e.g. In Internet cafes and libraries)

### **WEB BROWSER HIJACKING**

If your browser suddenly behaves in unexpected or undesirable ways, it may have been hijacked.

Here are some other symptoms that indicate you've been hijacked, and how to fix it.

- Browser home/start page changed to an unwanted site
- New favorites, bookmarks, toolbars, or desktop shortcuts that you did not add
- Typing a URL into the address bar and being taken to some other URL instead
- Your default search engine has been changed

- Inability to access certain sites, particularly anti-malware sites that might help you
- Endless pop-up ads for things you don't want to see
- Sluggish computer response; malware often slows your whole system down.

How does hijacking happen? In many cases, the hijacking software is something you downloaded and installed, thinking it was something beneficial.

If you believe your browser has been hijacked, shut down your browser immediately.

If you cannot close the browser in the usual way, you have a choice of emergency exits which vary from browser to browser.

Here are some tips but you need to check your system ahead of time so that you know what to do in an emergency.

## HOW TO ESCAPE

**In Edge** you close active window: *ALT + F4*

**Google Chrome** you close current window: *CTRL + SHIFT + W* or *ALT + F4*

**Firefox** you Minimize all windows (this will minimize all open windows to your Windows taskbar): *Windows Key + M*

Then Quit Firefox (this will only quit the active instance of Firefox; if you have other windows open, you will need to repeat this shortcut for them): *ALT + F4*

## WHAT ABOUT YOUR MOBILE DEVICES?

Protect your portable devices such as laptop, tablet and phone when out.

- Set a password to access the user account on your computer or mobile device, and change this password regularly. Make sure the system requires this password from you whenever it boots or wakes up
- Use a screen lock for your computer or mobile device when you're not using it, requiring you to enter a password when you return.
- Use reliable firewall software to prevent unwanted access over your network connections
- If you have one installed, use your onscreen rather than actual keyboard to enter passwords
- Don't leave your laptop or tablet in an unsecured area, or unattended and logged on, especially in public places like transport terminals and cafes.

You can get locking cables and leashes to secure your machine to a pillar or table leg but they are really meant for people who frequently work in libraries or travel a lot.

## SMART PHONE RISKS

Obviously you keep your valuable smart phone close at all times. A protective cover is a good investment in case of accidents.

But also check what can appear on your smart phone's lock screen.

Just activate your phone's digital personal assistant (e.g. Siri) and ask these questions:

- What is my name?

- Where do I live?
- Directions to my home?
- Most recent phone call?

You may be surprised how much info you can get from a “locked” mobile.

So remember that while it’s understandable that you to want convenient access to a number of features without having to unlock your phone, you are laying yourself open to data theft.

On most phone’s operating systems you can control what information is available on your lock screen through **Settings**.

### **AND BE CAREFUL OF APPS**

Experts attending the Mobile World Congress, the world’s largest gathering for mobile phone professionals, in Barcelona last week, warned of the growing risks of malware.

They said the major risk on smartphones remains downloading a hostile app that tries to compromise your data or run up your phone bill.

The best advice for Android phone users to avoid such threat is to stick to the **Google Play Store** instead of downloading apps from third-party stores or off the Web.

The fact that Google screens its Play Store apps makes the risk of malware there “dramatically less than a third-party app store, by far,” said a spokesman Still, the Play Store isn’t immune from crooks.

Last month, for instance, the Slovakian security firm found a trojan app on the Play Store disguised as a world weather app. Google yanked the app after hearing the news.

The risk of downloading malware on iPhones is minute in comparison to Android, thanks in part to the strict limits Apple places on how apps interact with the operating system.

But again use Apple’s own App Store or, if you have a Windows device, use Windows own store.

But whatever operating system you use, experts advise we look past apps’ star ratings and instead check users’ comments.

Users can report ‘Don’t install this,’ ‘this is bloody malware,’ but many people install the app anyway because it sounds so appealing.

Now, of all our sins of security the worst is keeping the same PIN number.

### **ONE WAY TO REMEMBER PINs**

Most banks will issue you with a four or six digit number for use at ATMS. You can change that PIN to numbers you prefer.

Here’s how to encode your own choice of PIN number

Say your bank asks you for a four number security code. You think of a phrase about banking and decide to use “**Money is the root of all evil.**”

Count the number of letters in each word of that phrase.

The result is 5 2 3 4 2 3 4 – more numbers than you need.

Just use the first four numbers, 5 2 3 4

Then it would be safe to carry a written reminder of your Commonwealth Bank Pin number in your wallet reading “Combank evil.”

Of course, these words could be taken as a comment 😊

Another example. Your main credit card is black. So say to yourself “**My card is black.**” Count the letters in each word. Now your pin is 2 4 2 5.

The note in your wallet could be “credit card black.”

## **BUILT IN SECURITY**

Computers today offer a number of inbuilt security aids, including biometrics.

In information technology, *biometrics* means technologies that measure and analyse your bodily characteristics for authentication purposes.

So these programmes check your fingerprints, your retinas and irises, your voice pattern and the arrangement of your facial features.

Many of us already use fingerprint readers – the other methods are already used by security services at airports for example but are expected to be a feature of home computers in the future.

So what are ordinary people like us to do to keep our information secure?

## **USE STRONG PASSWORDS**

The boring answer is to use strong passwords.

You can pay other people to create passwords for you by buying a special programme that you download to your computer.

Such programs are called *Password managers*. They organise and protect passwords and can automatically log you into websites where passwords are required.

Of course, they too can be hacked.

It’s your choice.

So we are back to ourselves.

Experts advise using whole phrases (including spaces) and avoiding common phrases, song lyrics or famous quotes.

Basically keep your password a nonsensical string of letters and numbers that you can still remember. And change it often.

## **OK. So how?**

Left to their own devices, most people will choose passwords that are simple for them to remember. Like “Password1” or “123456.”

Hackers use a technique called “socialising” which involves researching people so as to better guess their passwords.

Hackers get information about their victims by reading their profiles on Facebook, postings to chat rooms, and associations with sporting and social groups such as celebrity fan clubs.

Using these methods hackers can discover facts you may use in a passwords such as your mother's maiden name, where you went to school, your star sign, car you drive, pet's name, and your partner's birthday.

Experts say passwords will not necessarily keep you safe on line. But the longer and more complicated the password the better your chances.

And because we are seniors, don't think you can't remember complex passwords or PIN numbers. You can!

Just one thing you have to be aware of - some drugs have a negative effect on memory, especially anti-depressant medications. Discuss side effects with your doctor.

Now let's look at passwords YOU create to be easy for you to remember.

### **TIPS FOR GOOD PASSWORDS**

First, a few important rules:

- Use at least eight but preferably 10 characters in your passwords.
- Each password you create should contain at least three of the following character types: upper-case letters, lower-case letters, numbers, and special characters or spaces
- In other words, your password should be long and complex.

### **WRITE IT DOWN**

But we older people have to admit we feel more secure after choosing a very complicated password to then write it down so we don't forget.

You can write your passwords on a small piece of paper, and keep it with your other valuable small pieces of paper: in your wallet. Or at home in a small notebook.

But how to protect your notes?

### **ENCODE YOUR REMINDER**

One simple trick use is simple encoding. For example, just add one or two extra random letters at the front or end of the real password

For example, Tj7e4uI@ could become:

5Tj7e4uI@ (just remove the first character to reveal the real password)

Tj7e4uI@5 (just remove the last character)

@Tj7e4uI (just put the first char in the last position)

Another method is to write down a reminder that means something to you but nothing to anyone else. We'll come to that method of note taking later.

### **HOW TO CREATE A COMPLEX PASSWORDS**

OK you say, but where do I start creating a complicated password?

**The secret is to link something new (your new password) to something old, something that you already know really, really well.**

For example, an easy-to-remember password can be based on a phrase that is significant to you for a personal reason.

This phrase should be easy for you to remember, but other people should not associate it with you saying it a lot.

### ONE EXAMPLE

You can use a phrase such as “We moved to Lismore in 2002”

To turn this phrase into a password just take the first letter of each word.

This gives **WmtLi2002**

One checker says that would take about two days for a hacker to break.

Another example is “My family lived at 18 Smith Avenue when I was 7”

This gives **Mfla18SAwIw7**

(This slightly longer password would take a hacker an estimated 400 years to break).

### NOW ADD COMPLICATIONS

- Make your password longer by adding two or three dots or exclamation marks at the end or the beginning
- Insert a space
- Substitute numbers for letters and vice versa. (7 instead of Z, E instead of 3, @ instead of a, ! instead of i)
- Substitute words for numbers (one, two, three...)
- Substitute numbers for words – 2 for “Two” or 4 for “for”
- Use special characters such as ( ! @ # \$ % ^ & to punctuate and separate words

NOTE: Don’t use a forward slash.

Let’s work on **WmtLi2002**. One result:

**Wm2L! 2000&two...**

That would take 98 centuries to break.

Using these tips, you can create memorable passwords that will be nearly impossible to guess.

### MULTIPLE USE PASSWORDS

All the experts say you should NOT to use the same password for multiple sites. If a password gets compromised on one site, it may allow hackers to log into other accounts with the same credentials.

If you are willing to take a risk you can use a **variable core** password.

You think of your password as multiple parts: a central **core** of the password and a prefix and/or suffix, which is specific to the service that is being protected.



## A SAMPLE CORE

For example, your core might be **Mgpw4** from the words "**My generic pass word 4 (for)...**"

If this password is to be a password for the ANZ bank site, you might choose to add "ANZ" to the end of the password.

This would make your ANZ password

**Mgpw4ANZ**

Or what about adding a bit of punctuation such as

**Mgpw4: ANZ**

(note the colon and the space before ANZ)

Experts say to **change your passwords regularly**, say every three months.

Taking the ANZ example we could do this by adding abbreviations for the month and the year in front of the core.

So your password for your ANZ account could be

**Jan17Mgpw4: ANZ**

Then three months later it could be

**Apr17Mgpw4: ANZ**

You get the idea.

You can have different generic passwords for different types of accounts.

For all bank accounts you could use a phrase like "A penny for your thoughts" or ...

**Ap4yt**

Then add details of the bank and date. Such as ...

**Jul17 Ap4yt: NAB**

For accounts connected with shopping you could have a generic core password like "We love to shop at weekends" which makes your core ...

**Wl2s@w**

Once you have a password, check on its strength at various sites such as

<https://password.kaspersky.com/>

## OTHER SECURITY MEASURES

Passwords alone won't keep you safe. Two-step verification, where you confirm a login with a one-time code sent to your phone, makes a stolen password worthless.

Check with sites you use frequently to see what form of two-step verification they offer you.



**A FINAL WORD**

Think what could happen if you were killed or incapacitated and no one knew your password/s?

So, as an ultimate fall back position, write a complete explanation of how you set up your passwords and leave the explanation somewhere completely safe.

You could ask your solicitor to keep the explanation in his office along with a copy of your will or alternatively you could leave the explanation with a trusted friend or in a bank safe deposit box.

C, p@\$swo4d\$ R e@si 4U

Good luck

Gr@3 me!