



The 5 C's of Cyber Security: Guidebook



ALMOST UNHACKABLE
Conscious Cyber Security

© July 2024

0404 354 524
info@almostunhackable.me
www.almostunhackable.me



"The planet does not need
more successful people.

(insert here... Tech / AI Billionaires)

The planet desperately needs
more peacemakers, healers,
restorers, storytellers and
lovers of all kinds."

Dalai Lama



ALMOST UNHACKABLE
Conscious Cyber Security



**The 5 C's of
Cyber Security:
Guidebook**

Welcome!

Hi, I am Shane and I have been in the IT industry for close to 40 years. I have covered a wide range of jobs across Windows and Apple products, and I LOVE all things Tech!

I guess many of us love our tech and like me, use devices, and the internet, every day for communication, research, work, entertainment and play. But what I don't love, is the trend of the Tech industry to become profit greedy and manipulating, by both the 'hackers' and the providers themselves, to the detriment of the consumers.

Over the last few years, I have dedicated myself to uncovering the who, what, where, why of Cyber Security and Wellbeing. My main findings: *most of us are increasing our risk of cyber-crime – without even knowing it.*

Our number of accounts, duration spent online, poor digital 'habits' and lack of awareness greatly increases the exposure to cyber threats and the probability of becoming a victim of cyber-crime.

Cyber-Crime

Most cyber-crime is launched via Phishing which is a spam message containing malicious links, designed to get you to either download malware or follow links to spoof websites. These messages were traditionally emails, but are now deployed through texts, social media and phone calls.

Most 'phishing' is aimed at accessing either your identity information, or your financial details directly whilst fundamentally aiming for the same outcome, stealing your money.

Some current cyber-crime statistics:

- i** By 2025, cybercrime will cost the world \$10.5 trillion yearly
- i** The cost of cyberattacks in 2022 was \$6 trillion
- i** 95% of data breaches result from human error
- i** Globally, 30,000 websites are hacked daily
- i** 64% of companies worldwide have experienced some form of cyber-attack.
- i** Email is responsible for around 94% of all malware.

I hear stories every week from people who have fallen victim, lost money and are undertaking the large recovery task of setting up new bank cards, new accounts, new devices, new phone numbers etc. This is inconvenient and annoying but is mostly recoverable. Their money was NOT.

The statistics, and stories, can be alarming, but we don't need to be alarmed.

We can choose to take actions which minimise our personal cyber risks.

With this in mind, we offer a layered solution of techniques in our uniquely designed model:

The 5 C's of Cyber Security.

By following the steps in this guidebook, you greatly reduce your exposure to cyber threats and the potential for severe impact caused by a cyber hacker or scammer.

Please note that this model has been developed, through extensive and independent research. All advice offered here, and on our website, are professional opinions and are not influenced by any government, or private authorities, policies or payments.

This advice offers no guarantee of preventing a cyber-crime. Cyber safety remains the responsibility of the individual user.

Who is this for ?

This model has been designed for users of all ages and for anyone wishing to dramatically reduce your risks of cyber-crime.

The Guidebook is intended for you to use as a checklist to review and implement changes to your technology environment.

We recognise that for some of you the complexities of technology may be challenging, and we offer one-on-one sessions with an experienced technician, to assist you in working through, and implementing, the 5 C's.

How to Use this Guidebook

We aim to keep it simple. You can go through the Guidebook at your own pace, and in your own way. Depending on your personal Tech usage, your greatest potential for risk reduction may be found within any of the 5 C's, or most likely, a combination of all 5.

Here's our recommendation for how you may wish to use this Guidebook:



Read through the whole guidebook and determine which points are most relevant to you, and which you may have already done.

(You may wish to use markup on the .pdf document or print out a hardcopy to keep track of your progress.)



Define the points that create the highest risk for you right now and create some uninterrupted time to start working on these items.



Take your list to your trusted technician (i.e. ME.....! 😊) and get support to work through technical / software / configuration requirements.



Continue to work through your checklist, over time, to improve your security and wellbeing.



Set a reminder to do a review of your guidebook list every 6 months and take actions. Technology continues to evolve and you need to stay attentive to remain ahead of the threats.

Glossary

Device: portable electronic equipment that can connect to the internet, such as a smartphone, tablet, or laptop computer.

Hardware: machines, wiring, and other physical components of a computer or other electronic device.

Software: the programs and other operating system information used by a device.

Router: an electronic device which connects your user devices to the internet and other devices. (creates a wi-fi network)

Operating System: (OS or iOS) the program that manages a computer's resources, allocates the memory and allows the device to interact with other devices.

Digital Footprint: an electronic footprint, of information you leave behind when using the internet. It is a traceable history of all your digital activities, actions, contributions, and communications.

Hack: a piece of code that modifies a computer program in a skilful or clever way.

Scam: a fraudulent, deceptive act, or operation to trick people into handing over money.

Malware: a program that seeks to invade, damage, or disable a device.

Cyber Security: the application of processes, and controls to protect networks, programs, devices and data from cyber threats.

Cyber Attack: malicious activity that attempts to collect, disrupt, deny, degrade, or destroy computers or networks.

MITM Attack: man in the middle attack – a scammer intercepts and changes an email.



Why the 5 C's

Yes, setting strong passwords and installing 2 Factor Authentication (2FA) is a great start towards better online security. This is like setting locks on your front door.

But at Almost Unhackable, we know that scammers are often coming in the back door, the windows, the gate- so we need to secure the whole house – your whole technology environment.

With our multi-layered approach to cyber security, we offer you:

- i** a better understanding of how scammers work so that you can detect any 'red flags' and avoid falling for their scams, (i.e. cover all your doors and windows!)
- i** more confidence in choosing secure and ethical tech providers,
- i** greater levels of security derived by configurations, of your devices and apps,
- i** habits that provide for better wellbeing around tech usage,
- i** renewed peace of mind.




The 5Cs are a conscious, preventative model against cyber-crime AND a pro-active model for your tech wellbeing.


An introduction to the 5Cs

 **Consider your digital needs.**
Review your digital footprint against your actual needs, to decide what is optimal for your daily tech needs.
Less digital activity=Lower risk

 **Choose ethical** and low-risk providers. Delete any high-risk accounts.
Ethical products=Lower risk

 **Create security** for your accounts with 14-character passwords and 2 2FA on all your banking and social accounts.
Longer passwords=Lower risk

 **Configure your accounts** and devices to increase your security and wellbeing and to decrease overwhelm.
Improved wellbeing=Lower risk

 **Click consciously** each time you are online. Stop, think and be aware of who you are connecting with, and what they are asking for.
Tech responsibility = Cyber Safe

Let's look at the 5 C's now with details of what each is about, the associated risks, and what actions you can take.



I. Consider Your Digital Needs

Have you heard of a Digital Footprint?

One definition is: an electronic footprint, of information you leave behind when using the internet. It is a traceable history of all your digital activities, actions, contributions, and communications.

Your Digital Footprint is basically how many accounts you have / applications you use AND then all the online activity you do within these accounts. (Yes, for every application or service you use, you have an account, and you leave an trail behind you.....)

Understanding your footprint is important because the more accounts you have, and the more activity, means higher digital risks for you.

Why ? Because in most of these accounts are some / or all of your personal details. Your full name, your phone number, your address, possibly your birth date.....important details that can be used by a scammer.

Would you believe that most people have between 200-500 accounts?

And of these, they may only be using 20-30 each day. Perhaps a few hundred are obsolete!

Every time you want to trial a new App, get some data, join a group, buy from a new online store, or complete an online form – you are asked to create an account. And you may never use it again, but that account, and all the personal details you enter, stay there, until either you delete the account or possibly, the organisation deletes it for you if it is inactive for a few years.

So, over time, it is easy to accumulate accounts without realising it. Your Digital Footprint grows and so does your risk!

We recommend:

- i** Create a **list of all your accounts** – this is your Digital Footprint, your full online exposure. If you are using Apple's iCloud Keychain, you can use this to get a full list of your accounts. If you don't have keychain, you may need to manually look through your devices, search history, and any places you write passwords, to find accounts you have / apps you use. Ensure you include accounts for all: socials, groups messaging, business, hobbies, sports, etc.
- i** Do a review of your Digital Footprint and **delete all accounts no longer needed**. Go through your list and if you no longer need an account, go into the account, and delete it.
- i** For accounts in your Digital Footprint that you **would like to delete but are unable** (yes, sometimes there is nowhere in an account to actually delete it!), **you can do both of the next 2 steps below** to reduce risks of these accounts.
- i** For accounts in your Digital Footprint that you **still require, change the passwords** to a strong 14-character password and add 2FA.
- i** For any general, social or community accounts in your Digital Footprint that you **still require, edit the personal details to remove full name, birth date and phone number** (or use 'dummy data' instead). Remember this doesn't apply for any business, government or legal accounts as these accounts need your correct details and should be secure accounts.
- i** When opening new accounts **consider – do I really need this account?** If YES, create it with only the personal information that is essential and with a strong 14-character password. If NO – don't create it!
- i** If you would like **assistance –contact us**. We offer a one-on-one service to do a full review, make security recommendations and assist you with the processes of deleting and changing account details.



Your Notes:

"If you think
technology can
solve your
security
problems, then
you don't
understand the
problems, and
you don't
understand the
technology."

Bruce Schneier

2. Choose Ethical

So, it's the scammers and hackers we need to protect against- right?

YES and NO. It is not just the scammers that are manipulating tech users to get money. BIG Tech companies are also doing this every day, with the structures and programming of their services .

Anytime a service, application or data is provided FREE by a BIG Tech, it means they are making money from you in other ways.

This can be from advertising on their sites, but is often by owning and selling your data, your details or your online activity.

Yes, many BIG Tech companies are blatantly providing insecure or unethical services:

- ⊗ You post a photo or message on Facebook – Facebook owns that data.
- ⊗ You post something on Twitter – Twitter owns that data.
- ⊗ Your 'googling' – your internet research history – Google own that data.
- ⊗ Your child posts a video on Tic Tok – Tic Tok own that video.
- ⊗ You post a business video on YouTube – YouTube own that video.

When you see an advert pop up about a holiday to Fiji and you think – wow, I was just looking at a holiday to Fiji yesterday – yes, they know.

They **monitor and track** your activity and use it to select advertising to be placed in front of you. They also **sell your data** to brokers – who on sell to scammers. This is targeted and intelligent marketing BUT without our explicit permission.

And this data is additionally **used to inform and develop (Artificial Intelligence) AI** models in all industries. How soon before YOUR job could be replaced by AI? It's your online activity, that is contributing to the development of AI models.

Some of these Apps also have camera and microphone access so they can monitor not only your online activity (what you are typing) but they can see, and hear, you whilst you are using their App.

In the real world, we would call that unethical, illegal / stalking / breach of privacy. In the cyber world they call it clever, profitable business.

We recommend:

NOT using any of the following unethical providers or applications:

- ⊗ **META:** Facebook, Insta, What's App
- ⊗ **Elon Musk:** Twitter (X)
- ⊗ **Open AI:** Chat GPT
- ⊗ **Alphabet:** Google, Google Docs, Gmail, Chrome, YouTube
- ⊗ **ByteDance:** Tic Tok
- ⊗ **ANY AI** within any app.

If you wish to confirm their ethics and behaviour, we encourage you to investigate these companies further yourself. There is much published evidence available online.

2. Choose Ethical continued.....

We have researched alternative providers who have high ethics and security and are human driven, not profit driven.

Many smaller businesses are now leading the way to a more human focused future for Technology. We encourage you to investigate these further yourself if you wish to understand their ethos, and values, and compare them to your own.








Yes, most of these are PAID services, instead of FREE services, but the increase in security and peace of mind are invaluable.





The main entry points for cyber-crime phishers are: email, text messages, social media, scam websites and phone calls. AND most cyber-crime occurs through unethical, insecure and often FREE, providers.

By choosing ethical providers you are reducing your risk of cyber-crime and also influencing BIG Tech to become more ethical and more security conscious.

We recommend:






Choosing the following ethical providers as alternatives for daily activities:

-  **Email:** Proton Mail
-  **Text Messaging:** iMessage, Signal
-  **Search Engine:** Ecosia
-  **Web Browser:** Brave,
-  **Cloud Storage:** Sync, Proton Drive
-  **Password Mgr:** Dashlane, Proton Pass, Bit Warden
-  **File Transfer:** Transferly

-  **Document collaboration:** CryptPad
-  **VPN:** Proton VPN
-  **Calendar:** Proton, Outlook
-  **Social Media:** Mastodon, Bluesky.social

This short, recommended list is a beginning only. We cannot attempt to cover all apps and services as there are thousands of potential digital providers that you could be using.

We know that most people choose a product based on price, and the features it offers. We recommend using some of the following tips, to determine ethics and security levels, when you are next choosing tech providers for a particular service:

-  If a service is FREE, investigate how they make their money. Their business and **profit** structure should be detailed on their website somewhere.
-  Look for the company's **Privacy Policy** and read it through. It should clearly state that your data is not sold or shared with anyone.
-  Look for the company's **security** level. It should be stated that they have E2EE = End to end encryption. The best option is when they don't have visibility of the encryption key – if they do, the key itself can be hacked.
-  Look for the company's **owner**. Who is it that owns and profits from the business? e.g. a private billionaire, public stock market company (profit driven) or a not-for-profit.
-  Research the **history** of the company. Who created it originally (were they ethical?), why was it created (what was the original purpose?), have they ever had a security breach? Has it ever been sold – why?



Your Notes:

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

Newton Lee



3. Create Security

Creating security on the accounts you have is an essential first line of defence against cyber-crime. Having a secure password, is the key to the door of your private information, data and money.

But secure passwords are no longer enough. You need **layers of security** across your passwords, devices and accounts to avoid the vast range of cyber-crime.

We recommend:

i Setup a paid **Password Manager** app and put in ALL your accounts and passwords. You can no longer just 'remember' all your passwords. It is essential that you have these documented securely. Add passwords over time, if you don't have a current list of passwords, and update it every time you change or add a new account. Ensure you have a really strong password as your Master Password and that you can remember this, and have an emergency, trusted person who also holds this password.

We Recommend: [Dashlane](#). Dashlane now have a 'Family Feature' so you can manage passwords across multiple devices, and family members, for approx. \$100 / year.

i Create **strong passwords** more than 14-characters long. (As above, when you change a password, update it in your Password Manager.) You can also use a random password generator, or memorable passphrase something like "My Blue Car has 4 Windows". Characters, spaces and length of password help to increase strength.

i Check **password strength** [here](#), before using a password, to confirm how secure it is against hackers.

i Setup **2 Factor Authentication (2FA)** or an Authenticator App on all of your bank accounts, other financial accounts and high-risk accounts such as social media. 2FA means that each time you attempt to log in with a password, it will then request a code to allow login. This code will be sent to your designated email, text or an authenticator app. This 2FA is a crucial measure to stop scammers, they may get your password but without a 2FA code, they cannot access your account. **We Recommend:** [Step Two Authenticator](#) for Apple Devices and [Authy](#) for Windows / Apple device combinations.

i Bank with a **reputable financial institution** that has a high level of cyber security. Some of the smaller, local, banks do not have the funds for sophisticated cyber security and can be higher risk.

i **Update your devices operating systems** (iOS & OS) regularly, or as prompted. These security updates are aimed at identifying, and avoiding, current hacks. When your operating systems are older (sometimes this is necessary on older devices) you are at higher risk of current scams / hacks.

i **Have a trusted technician** who knows you, how, and what you use technology for. Gaining support from different family, friends and inexperienced technicians is increasing the likelihood that some of your configurations may not be optimal and increasing your risks.

i **Cover your webcam** when not in use and only use reputable recording and downloading software. Also only allow webcam and microphone access to ethical and secure apps. (you may not realise it but Facebook uses your webcam to see you, even when you are not videoing)



3. Create Security continued.....

i Turn off **Siri & Alexa** and revert to manual instigating of a digital assistant, when needed. If Siri is turned on (on a phone, iPad or apple pod) it is constantly scanning and listening for your commands – but it is also listening for any information that it may use to feed into AI. So, your private conversations are not so private.

i When you wish to sign up to a new, unknown site / organisation, use Apple's '**hide my email**' service or an email alias creation app instead of giving them your personal email address. Never provide personal details such as full name, Date of birth, phone number – to unknowns. (Use 'fake' details instead)

i Regularly (daily or weekly) backup your desktop and laptop devices using **Time Machine** or a reputable backup application, so data can be recovered if you do have a hard drive failure or malicious hack on your computer. In a worse-case scenario, you can often get back any lost data from a backup.

i Keep your iPhone, iPad and essential files stored, or **backed up in the iCloud**. In a hack, loss or damage of a device, being able to restore your precious photos and contacts is a huge relief!

i When **sending invoices** do not use email. Emails can be intercepted and the email itself, or an attachment can be altered, then resent to the receiver. This is now a common way hackers get money – they change bank details on emailed invoices. When you need to send an invoice, or a secure financial document, to a client use an secure, end to end encrypted file transfer system such as **Transferly**. Even MYOB and Xero are no longer perfectly secure for sending invoices.

i When **connecting to your banks** or financial institutions, online, type the full bank address into the browser rather than an online search of just a few letters of their name. (If you select from a list that comes up it is probable that the first few sites listed are malicious sites aimed to look like banks.). Or do all your banking from your banking app with 2FA installed rather than via a website.

i Do not change, or cancel, your **phone number** without first gaining support to update any security configurations which have your phone number listed as 2FA. Once you list your phone number as your 'recovery' or 2FA contact number it is crucial for accessing your essential accounts. If you lose a phone, split up with a partner, or lose a spouse you may be quick to delete, or change, your phone account. But please STOP and check with a technical expert regarding any digital impacts.

i If you have a personal / business **website**, it needs to have a strong password, 2FA and be protected with regular updates. Your typical login address is "yourwebsite.com/wp-admin". Log into your WordPress account and run the updates regularly. Websites with old or non-updated platforms become vulnerable to hackers and potentially your website could be destroyed.

i When **answering your phone**, don't state your name. Just say hello and nothing else. This prevents hackers from obtaining your voice on audio to re-digitalise and use.

i If you want to go further to protect your financial environment, you can setup blocks / shields in **Credit Savvy**. This will mean that if your identity is compromised, a hacker will not be able to alter your credit history ranking.



3. Create Security continued.....

When **travelling** interstate, or overseas, there are extra risks associated with new people, crowded places, different cultures. Your Cyber Security risks may also increase when travelling as you are possibly busier, less aware of your surroundings and more likely to be distracted.

We recommend when travelling:

- i** Ensure to use **Face ID** on your iPhone / iPad instead of a PIN number which can be seen, or guessed by someone who steals your device.
- i** If you need internet (wi-fi) in a public area the first choice is to **Personal Hotspot** from your own iPhone. If you do need to use a public wi-fi service, ensure you set up a trusted VPN. We recommend: [ProtonVPN](#) or [IVPN](#)
- i** Ensure you are using a trusted messaging service such as Apple iMessage or **Signal** for all my texts, calls, and video messaging. If iMessages are coming up green (instead of blue) you are messaging someone who is not on an Apple device, so messages won't be encrypted from their end. In this case, swap to Signal.
- i** If you want extra security for crowded areas, you can use a **Faraday bag** (we keep some in stock!) for carrying your device. A Faraday Bag protects your device from various types of electronic interference, including electromagnetic pulses (EMP) and radio frequency identification (RFID) scanning / hacking.
- i** Be more **focused** and aware when travelling. It often involves interruptions to sleep, unfamiliarity with places and more Tech use. Please don't click on links, respond to emails, or similar, when you are jet-lagged, over tired or stressed.

Cyber Security strategies within **networking and administration** are another level of defence and create even greater protection against hackers. **These can be setup by your trusted technician.**

We recommend for extra security by your technician:

- i** Set your DNS (Domain Name System) on your router to 'Private Network' i.e. **Quad 9**. This will prevent your online searches from being tracked.
- i** Ensure your **router firmware** is updated to the current version. If your router is older than 5 years old, and is no longer able to update to current versions, then replace the hardware with a new one. Old router technology is more vulnerable to hackers.
- i** Set up a separate '**Guest Wi-fi**' on your router at home with a strong password. When you have guests, only allow them to access this wi-fi, not your own personal wi-fi. This will keep their devices, and their digital activity separate from your own and isolate the risks.
- i** If you have any **Smart home devices**, such as fridges, solar inverters and home automation, that connect to the internet, ensure these are attached to the Guest wi-fi, not your personal wi-fi.
- i** Set up a **separate Administrator** (Admin) account on your Mac / computer to your user account (usually your name). Ensure you know the passwords to both, because changes, uploads etc will require administrator access. (If you do get hacked when logged into your user account, hackers will not have 'permissions' to download or alter anything on your device.)



Your Notes:

"Socialising on the internet is to socialising, what reality TV is to reality."

Aaron Sorkin



4. Configure for Wellbeing

Preventing cyber threats is a key aspect of cyber security and being online. But our decreased wellbeing is a critical, and an often-overlooked symptom, of the ever-expanding online world.

Using technology has a direct, and indirect impact to your mental, physical, emotional and social wellbeing.

We can take responsibility to make better choices which can improve our wellbeing, and the wellbeing of our family, at all levels.

These recommendations are gentle suggestions. Everyone is different, so please choose whatever resonates for you – and create your own bespoke Tech environment and habits.

It is an ongoing work in progress, so have fun and adjust as you go!

We recommend:

- i** Upon **waking**, say good morning to your partner, children, plants, animals BEFORE you pick up your device and start scrolling.
- i** Use '**Do not Disturb**' on your device to limit the hours of the day that people can have direct access to you. You may also set specific times of the day, or days of the week, where you won't respond to emails / business texts. Let your clients know when they can expect to hear back from you, on other days, take a break.
- i** Keep your **desktop / screen** clear of junk files and have a clear filing system for your work and your personal data files. A busy screen / desktop adds to overwhelm and confusion.
- i** Keep your **email inbox** clear – file or delete emails once read. And empty your junk folder and deleted items folders regularly.

- i** Set times of the day aside when you need to get work done and **turn off notifications** or leave phone on silent.
- i** Have set times of the day which are **tech free** for all the family. This way you can all be present for each other.
- i** Look at your weekly **tech usage** statistics and decide on a goal to reduce this. Set up some strategies on how to achieve this goal in coming weeks. We lived without devices until just a few decades ago – it is perfectly do-able!
- i** Your **phone** does not need to be in your hand 24 / 7. Create a new 'place' for your phone to live which is near, but not obtrusive, perhaps a bag? Or a table in a central room could be a charging station and all devices reside here.
- i** Have **tech free rooms** in the house which are always designated as device free. These rooms are a relaxing, safe space for everyone.
- i** Never use a device as a **babysitter** for children and never use it as a babysitter for yourself! If you are feeling angry, depressed and need some 'downtime' feel free to watch TV or do analogue activities, but don't go online and do shopping, work, social media etc. Your mood is not likely to improve!
- i** Set a few **specific times** a day when you check your messages so that these times are when you are in an alert state and not distracted by family or work. Then you can single focus on the messages and delete / action as necessary.
- i** If you are on **Social Media** set a specific, limited, time each day that you go 'on socials'. Limit yourself to perhaps 1 hour or less, in either the morning or the evening. All that extra time you save can be spent with a partner, family or just relaxing!



4. Configure for Wellbeing continued...

- i** When doing **real life** (IRL) socialising or work meetings, give your phone, and laptop, some time off. Place them away and enjoy just BEING and CONNECTING with people. Ask colleagues to do the same and you will be amazed at how the dynamics change.
- i** Go **analogue!** Swap out using your phone as a full organiser and bring back an analogue clock, watch and hard copy diary. Then you can use these for work, or play, without any digital interferences.
- i** **Remove social** apps from your phone so you are not tempted to use them at inappropriate times. If you are feeling addicted and needing a 'social fix', try replacing social media with something else: dance to a song, phone a friend, hug a pet.
- i** **Unsubscribe** from mailing lists that you no longer need or that don't offer a positive impact to your wellbeing. Restrict your inbox to messages of Love and Light!
- i** **Download** documents to read, or work on so that you can work off-line.
- i** Have a '**digital detox**' regularly where you spend 1-2 full days, tech free, preferably in nature or doing something you love.

Children's Wellbeing

Children's bodies, and brains, are developing until age 21. For this biological and neurological development, they need to move, play, touch, be in nature and have human experiences.

Excessive screen time, social media and gaming have all now been shown to have detrimental impacts to children's wellbeing.

We recommend for children:

- i** **No devices** for children under 8. Replace electronic and electric toys with analogue toys, human singing, playing and stories.
- i** Never use a device as a **babysitter** for children. They will learn to be dependent on it.
- i** **No social media** for those under 18. Youths and young adults' brains cannot yet filter out and discern genuine, uplifting posts from predatory behaviour.
- i** Be a **role model** for your children – be human focused, not tech focused, delete your own social media accounts.
- i** If children need a **phone** to contact you, provide a 'dumb' phone. If children need a smart phone – setup parent permission for downloads, teach children cyber safety – remove socials and Whats app, discord etc. - see an expert on how to configure the phone to maximise your child's safety.
- i** Children need **sleep** for rest and development, don't allow phones or laptops in the bedroom and don't allow tech usage after dinner.
- i** Encourage in real life - **IRL** groups and playdates for all children under 16.
- i** Establish clear and firm **tech boundaries** with children from an early age. Teach them the joys of a low-tech lifestyle!



5. Click Consciously

Your own awareness, your understanding of how hackers gain access, and how scammers manipulate you, is your most powerful tool in cyber-crime prevention. Yes, it may be the last line of defence and sometimes it is the most crucial. If a scammer does get through your other lines of defence, here is where you can prevent yourself from becoming a victim.

You can create a personal, human detection system to discern, and avoid, scammers.

We recommend:

- i** Don't post photos, names, ages, locations of yourself, or particularly your children, on insecure, or public forums online e.g. social media. Scammers can quickly build a profile and use it to impersonate you, or possibly to locate you or your child.
- i** When **rushing**, stressed or tired don't use your devices. Never quickly reply, respond or react. Always allow time and space to consider what action to take. When we rush or are multi-tasking, we are less likely to be able to discern a request from a scammer, versus a real request.
- i** Don't use **public wi-fi**. If there is no private wi-fi network, you can connect to the internet via a Personal Hotspot from your own phone. Public wi-fi is insecure and a favourite 'phishing' spot for hackers.
- i** Never give **anyone else access**, or use, of your iPhone, iPad or computer. It seems easy to hand your phone to a child, spouse or friend but your devices contain your personal, identity data, passwords and security configurations. Unknowingly, another person may use, or change, this data and increase your cyber risks.

- i** Only let a **trained, trusted, technician** do software, hardware or configuration maintenance. Your devices are complex technology and powerful interfaces. If you get your child, partner or neighbour to 'fix' something on your device, they can be unknowingly weakening your cyber security.
- i** Never give out your **passwords** to anyone – neither a friend or someone requesting it online. The only people who should have access to your passwords are YOU, and one trusted emergency contact. Only give a password to a known, technician, in person.
- i** Don't use your **Apple ID email address** for general mailing lists. Use a different email, or 'hide my email' when signing up to mailing lists. It is best for the least amount of contacts to have your Apple ID address .
- i** Know who your **providers** are for email, domain names, web hosting and internet. Have their contact details available for emergencies. If you get phoned by someone regarding a service, you are more likely to detect a fraud and if you ever need assistance, you will have contact details at hand.
- i** Keep tabs on your '**digital footprint**' and regularly delete accounts, and apps, you no longer require. Be aware of which accounts may be putting you at higher risk and setup controls / configurations to secure them.
- i** Anytime you think you may have been **hacked**, stop immediately and gain advice from a reputable technician.
- i** From time to time, conduct an **online search** of your own name to see where your identity is known. Be aware of which accounts may be high risk and take actions to delete any unwanted associations, accounts, apps.

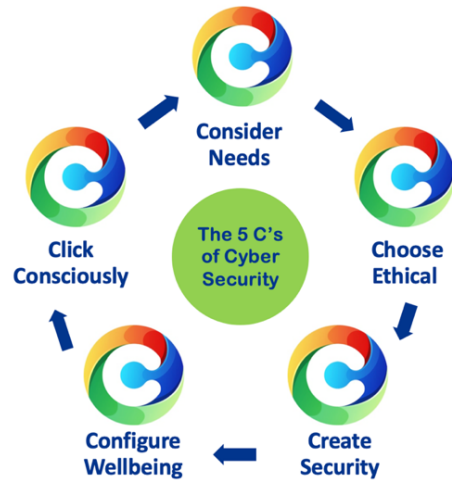


Further Support:

Please contact us if you would like further support to understand, and implement, any aspect of 'The 5 C's of Cyber Security.'

"The human spirit
must prevail over
technology."

Albert Einstein



We offer one-on-one sessions on:

- 📍 Reviewing your Digital Footprint
- 📍 Setting up Passwords and 2FA
- 📍 Swapping to Ethical Providers
- 📍 Marketing without Social Media
- 📍 Tech Wellbeing for Families
- 📍 And lots more.....!

Text / Phone:

0404 354 524

Email:

info@almostunhackable.me

You can find further resources, and information on our services, at our website:

www.almostunhackable.me