Capital Partners

LIFE CONVERSATIONS. WEALTH SOLUTIONS

Personal Cyber Security Checklist

Our lives are deeply connected online. Cyber security is no longer optional. It’s essential.

This checklist is designed to help you stay safe and confident online. It offers clear, practical advice to help you protect yourself from online threats.

We focus on the essentials: keeping your personal and financial information secure.

Whether you’re working remotely, shopping online, or managing your finances, this guide will help you safeguard your privacy and avoid digital risks.

Let’s take a closer look at how you can secure what matters most.

The Checklist

This checklist will guide you through the essential steps to secure your personal information, defend against cyber threats, and navigate the internet with assurance.

Item	Cyber Secuity Checklist	Completed?
1	Utilise a password manager to safely store passwords.	Yes / No
2	Ensure you are using long passwords/passphrases as opposed to short passwords. Use different passwords/passphrases for each login stored in the password manager.	Yes / No
3	Ensure you are using Two Factor Authentication (2FA) for logins where possible.	Yes / No
4	Ensure the software on your devices is up to date. Re-start your devices regularly to ensure the software is installed.	Yes / No
5	Ensure you have antivirus software installed on your devices and it's up to date.	Yes / No
6	Maintain a back-up of any important information being stored on a device.	Yes / No
7	Avoid using public open WIFI at airports, cafes etc.	Yes / No
8	Screen your phone calls. Do you know the number of the person calling you? If unsure, let the call go to voicemail. If someone calls you and asks you for personal information, take their name and tell them you will call them back.	Yes / No
9	Double check your emails and sms messages received before responding or taking any action. Is it from a trustworthy source?	Yes / No
10	Think twice before you click a link, open an attachment or download anything to your device. Can you trust the source?	Yes / No
11	Never allow remote access to your devices or provide sensitive details if you have been contacted unexpectedly.	Yes / No
12	Complete a factory reset before disposing of old devices.	Yes / No

Additional tips

Item	Cyber Secuity Checklist
1	**Utilise a password manager to safely store passwords.** Password managers are highly recommended for several reasons: 1. **Convenience**: You won't need to remember all of your passwords, as the password manager securely stores them for you. 2. **Security**: It generates strong, unique passwords for each of your accounts, which enhances your online security. 3. **Efficiency**: Auto-login features save you time by filling in your credentials when you visit websites or apps. 4. **Accessibility**: You can access your passwords from any platform, whether you're on your phone, tablet, or computer. 5. **Safety**: Password managers have encrypted storage, which means your passwords are protected by strong encryption methods. 6. **Password health**: They can alert you if your existing passwords are weak, reused, or have been compromised in a data breach. 7. **One master password**: You only need to remember one strong master password to unlock your vault. Remember, no system is infallible, so it's important to choose a reputable password manager and maintain good security practices, such as keeping your master password/passcode safe and enabling two-factor authentication when available.

Item	Cyber Secuity Checklist
2	**Use different passwords/passphrases for each login** stored in the password manager. Long passphrases offer several security advantages: 1. **Harder to crack:** The length of a passphrase makes it more difficult for attackers to guess or crack using brute force methods. The number of possible combinations increases exponentially with each additional character, making it significantly more secure than shorter passwords. 2. **Easier to remember:** Passphrases can be a sequence of words or a sentence, which are often easier to remember than a complex string of characters. This means you're less likely to forget it and less tempted to reuse passwords across multiple sites. 3. **More entropy:** Entropy is a measure of randomness and unpredictability. Longer passphrases generally have higher entropy than short passwords, especially if they include a mix of upper and lower case letters, numbers, and symbols. 4. **Phishing resistance:** Long passphrases that are unique and not easily guessable can help protect against phishing attacks, where someone might try to trick you into revealing your password. For example, a passphrase like "BlueSky@MorningCoffee2024!" is not only long but also includes a mix of different types of characters, which makes it stronger against various types of cyber attacks.

Item	Cyber Secuity Checklist
3	**Ensure you are using Two Factor Authentication** (2FA) for logins where possible. Here's why: 1. **Enhanced security:** With 2FA, you need more than just a password to log in. It typically involves a second form of verification, such as a code sent to your phone or a biometric scan. Even if someone steals your password, they won't be able to access your account without the additional factor. 2. **Mitigates password vulnerabilities:** Passwords can be compromised through data breaches or phishing attacks. 2FA helps safeguard against these risks by requiring an extra step for verification. 3. **Broad applicability:** Many services now offer 2FA, including online banking, social media, and email accounts; and across different devices. 4. **Various methods:** You can choose from different 2FA options, such as SMS texts, mobile apps, or physical security keys. Each method has its pros and cons, but they all enhance security.

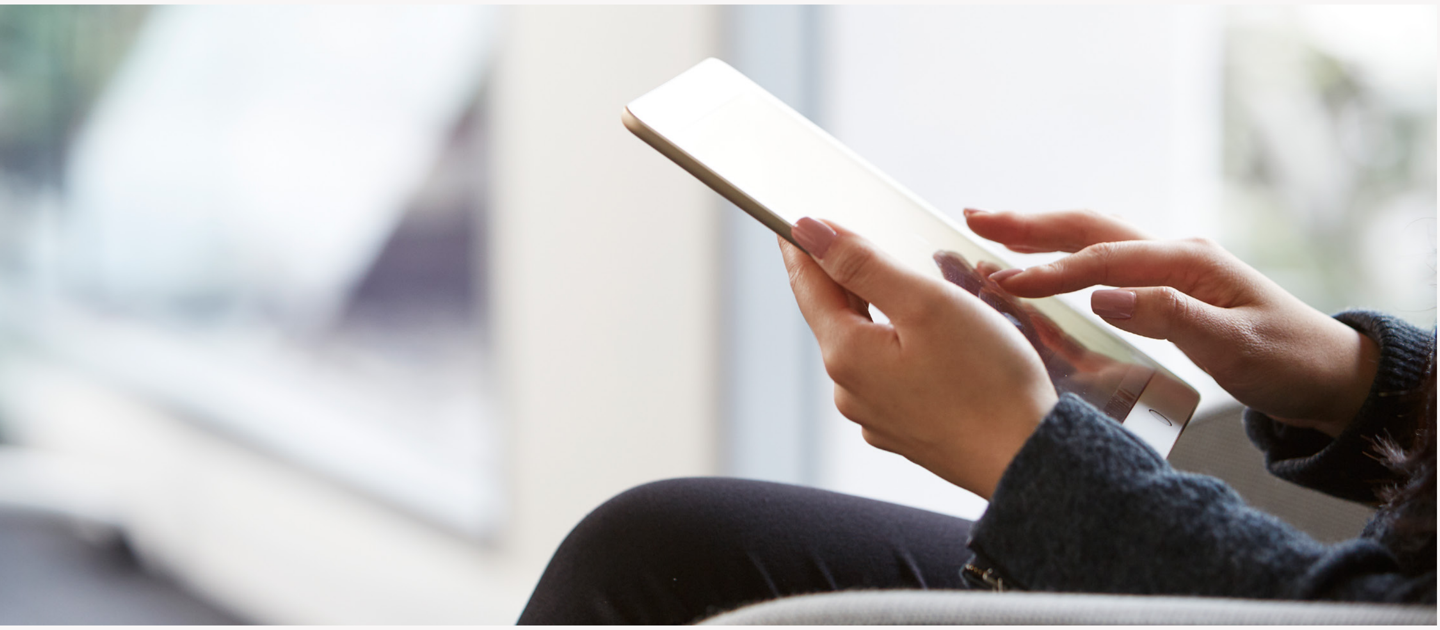
Item	Cyber Secuity Checklist
4	**Ensure the software on your devices is up to date.** Keeping software up-to-date enhances overall security, how well your systems work, and how fast they are. Regular updates help by: 1. **Reducing vulnerabilities:** Updates often include patches that fix security vulnerabilities. By staying current, you protect your systems from known exploits. 2. **Protecting sensitive information:** Outdated software can be an entry point for cyberattacks. Keeping it up-to-date ensures that sensitive data remains secure. 3. **Ensuring smooth operation**: Updates improve performance, stability, and compatibility. They help prevent crashes, glitches, and other issues.

Item	Cyber Secuity Checklist
5	**Ensure you have antivirus software installed on your devices and it's up to date.** Having antivirus software is essential for several reasons: 1. **Protection against malware**: Antivirus software assists to detect and prevent malware, including viruses, from infecting your computer. 2. **Internet security**: Good antivirus programs provide browser extensions that enhance internet security. They help block malicious websites and protect your online activities. 3. **Data protection**: Antivirus safeguards your data. If hackers breach your computer, it helps to prevent data loss, theft, or tampering. 4. **Preventing identify theft**: By keeping your system secure, antivirus helps prevent identity theft and unauthorised access to personal information. 5. **Safeguarding confidential information**: Whether it's family photos or personal documents, antivirus ensures the contents of your computer remain safe. 6. **Performance optimisation**: Malware can slow down your computer. Antivirus keeps your system running smoothly.

Item	Cyber Secuity Checklist
6	**Maintain a back-up of any important information being stored on a device.** Maintaining separate backups for your data helps by: 1. **Protecting from data loss:** Backing up your data helps safeguard against unforeseen events like hardware crashes, malware attacks, accidental deletion, or natural disasters. If your main computer fails, having a separate backup ensures you don't lose critical information. 2. **Continuity:** Separate backups will minimise downtime during disasters or cyberattacks, allowing operating to continue smoothly. 3. **Accessibility and retrieval**: Storing backups remotely (e.g., in the cloud or on external drives) ensures data accessibility even if your primary system fails. It also facilitates collaboration and file sharing.

Item	Cyber Secuity Checklist
7	**Avoid using public WIFI at airports, cafes etc.** Using open public Wi-Fi networks can expose you to multiple risks: 1. **Man-in-the-middle attacks (MITM):** These attacks allow eavesdropping on your data transmissions. Cybercriminals can intercept sensitive information, compromising your privacy. 2. **Unencrypted networks**: If a network lacks encryption, your web traffic is vulnerable. Scammers can easily access it, potentially leading to security breaches. 3. **Malware distribution**: Attackers exploit software vulnerabilities to inject malware onto your device without your knowledge. 4. **Wi-Fi snooping and sniffing**: Malicious actors can monitor your online activities, capturing sensitive data. 5. **Malicious hotspots**: Some attackers create fake hotspots to deceive users into connecting, putting their data at risk. To stay safe, consider using a virtual private network (VPN) and avoid sensitive transactions on public Wi-Fi.

A cybersecurity report was lodged every six minutes in the 23/24 financial year



Item	Cyber Secuity Checklist
8	**Screen your phone calls.** Screening your phone calls offers significant benefits from a financial protection perspective: 1. **Identifying scam calls:** Advanced call screening services use algorithms and databases to identify and flag known scam numbers, warning you of potential risks. This helps protect your financial information and privacy. 2. **Preventing phishing attacks:** By blocking or not answering suspicious calls, call screening helps prevent phishing attacks. It shields sensitive personal information, reducing the risk of financial fraud.

Item	Cyber Secuity Checklist
9	**Recognising potential cyber threats in emails or SMS messages is crucial.** Here are some common signs to watch out for: 1. **Unfamiliar sender**: Be cautious if the sender is unknown or uses an email address that doesn't match the legitimate organisation they claim to represent. 2. **Generic greetings**: Phishing emails often lack personalised greetings and use generic language. 3. **Urgency or threats**: Scammers create urgency, claiming problems with your account, suspicious activity, or billing issues. 4. **Suspicious links or attachments**: Avoid clicking on links or opening attachments unless you're sure of their legitimacy. 5. **Spelling and grammar mistakes**: Poor language quality can be a red flag. 6. **Requests for personal information**: Be wary of requests for sensitive data like passwords, payment details, or tax file numbers. If in doubt, call the supplier to confirm their bank details.

Item	Cyber Secuity Checklist
10	**Think twice before you click a link, open an attachment or download anything to your device.** Clicking on links without caution can have the following consequences: 1. **Malicious payloads:** Risky links may download viruses, malware, or spyware onto your device. These can compromise your privacy and steal sensitive information. 2. **Phishing scams:** Scammers create fake login pages to steal your credentials. Clicking a link could unwittingly hand over your username, password, or security answers. 3. **Slow down and verify**: Preview links before clicking. Check for typos, suspicious links, and unexpected redirects.

Item	Cyber Secuity Checklist
11	**Never allow remote access to your devices or provide sensitive details if you have been contacted unexpectedly.** Allowing remote access to your device for an unknown person is extremely risky: 1. **Security risks:** Granting remote access means giving control of your device to someone else. They can install malicious software, steal sensitive data, or compromise your privacy. 2. **Scams and fraud:** Scammers often pose as tech support agents, claiming they need access to fix issues. In reality, they exploit your trust to steal information or money. 3. **Loss of control:** Once remote access is granted, you lose control over your device. Unauthorised actions can occur without your knowledge. Always be cautious and never allow remote access unless you're certain of the person's legitimacy!

Item	Cyber Secuity Checklist
12	**Complete a factory reset before disposing of old devices.** This is essential for several reasons: 1. **Data privacy:** A factory reset erases all personal data, including photos, messages, and accounts. Without it, your information could be accessible to the next user or potential attackers. 2. **Security:** Resetting ensures that any malware or unauthorised apps are removed. Otherwise, they might persist and compromise the new owner's security. 3. **Identity protection**: Personal details, login credentials, and saved passwords could remain on the device. A factory reset prevents identity theft. 4. **Resale value**: If you plan to sell or donate the device, a factory reset increases its value and ensures a clean slate for the next user. Remember to back up any imporant data before performing the reset.

Resources

Thank you for reading our personal cyber security checklist.

Cyber threats are constantly evolving, so staying informed and proactive is essential. Regularly review and update your security practices and encourage others to do the same. Feel free to forward on this ebook to those you care about.

Applications & software

Password Managers allow you to store unique password strings for all your accounts.

Utilising one of these products will prevent multiple accounts from being breached at once due to unique and complex passwords. Some services include:

- Lastpass - https://www.lastpass.com/
- 1Password - https://1password.com/
- NordPass - https://nordpass.com/

Anti-virus software adds an additional layer of security by blocking viruses or malware from breaching your system after being unintentionally downloaded via a website, email or scam call. These pieces of software can be installed on Laptops, PCs and sometimes Tablets or Phones.

- Microsoft Defender - https://www.microsoft.com/en-au/microsoft-365/microsoft-defender-for-individuals
- Crowdstrike - https://www.crowdstrike.com/en-au/
- Webroot - https://www.webroot.com/au/en/home
- Bitdefender - https://www.bitdefender.com/en-au/

ACSC

Australian Cyber Security Centre (ACSC) is the central location for cyber security resources, training, guidelines, and reporting in Australia. It is backed by the Australian Signals Directorate, which also provides military support for signals intelligence, cyber warfare, and information security.

Organisations around Australia will regularly follow the Essential 8 cyber security guidelines defined and updated by the ACSC regularly to ensure companies are always ahead of the curve.

If you need further information or assistance to secure your personal information, you can contact the ACSC or the partners they recommend to help you secure yourself online.

The ACSC website contains plenty of resources to identify the next steps if you've been hacked, are looking for news on recent threats or are trying to improve your security posture. The following links will assist:

- Interactive guide for responding after you've been hacked or received a scam call. https://www.cyber.gov.au/report-and-recover/have-you-been-hacked
- Running a cyber security exercise to establish your organisation's baseline. https://www.cyber.gov.au/resources-business-and-government/exercise-in-a-box
- List of resources to assist with the response to different types of attacks and preventative actions. https://www.cyber.gov.au/report-and-recover/where-get-help
- Reporting scams to help others avoid a breach. https://www.cyber.gov.au/learn-basics/explore-basics/recognise-and-report-scams
- Gold standard set of guidelines to ensure your organisation is secure. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
- Latest cyber alerts and advisories. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories
- Learning Materials to increase your cyber security knowledge. https://www.cyber.gov.au/learn-basics

Key terms

- Adware: Software that shows you ads and tracks what you do online.
- Advanced Persistent Threat (APT): A long-term, sneaky attack where hackers stay hidden in a network for a long time.
- Antivirus: A program that finds and removes bad software from your computer.
- Authentication: Checking to make sure someone is who they say they are.
- Botnet: A group of infected computers controlled by hackers to do bad things.
- Cryptography: Turning information into a secret code so only certain people can read it.
- DDoS (Distributed Denial of Service): An attack where many computers overwhelm a website to make it stop working.
- Encryption: Changing data into a secret code to keep it safe from prying eyes.
- Firewall: A security system that controls what data can come in and out of your network.
- Malware: Any software designed to harm your computer or steal your information.
- Phishing: Tricking people into giving away personal information by pretending to be a trustworthy source.
- Ransomware: A type of malware that locks your files and demands money to unlock them.
- Social Engineering: Manipulating people into giving up confidential information.
- Spyware: Software that secretly watches what you do on your computer.
- Trojan Horse: Malware that pretends to be a useful program but actually harms your computer.
- Virus: A type of malware that spreads by attaching itself to other programs or files.
- Vulnerability: A weakness in a system that hackers can exploit.
- Worm: Malware that spreads itself to other computers without needing to attach to anything.

Interesting facts about cyber security

- Cybercrime is Big Business: By 2025, cybercrime is expected to cost the world $10.5 trillion annually . This includes everything from data breaches to ransomware attacks.
- Frequent attacks: A cyber-attack happens every 39 seconds[1]. This shows just how relentless cyber threats can be.
- Human error: About 95% of cyber security breaches are due to human error[1]. This highlights the importance of training and awareness.
- Phishing dominance: Phishing is the most common type of cyber-attack, with over 80% of reported incidents involving some form of phishing .
- Ransomware costs: Ransomware attacks are projected to cause $265 billion in damages by 2031[1]. These attacks can be devastating for businesses and individuals alike.
- Email vulnerability: Around 35% of malware attacks start with an email[1]. This makes email security a critical aspect of cyber defence.
- IoT devices: By 2030, there will be over 50 billion IoT devices connected to the internet[2]. Each of these devices can potentially be a target for cyber-attacks.
- Password reuse: Despite warnings, 65% of people reuse passwords across multiple accounts[2]. This practice significantly increases the risk of a security breach.
- Mobile malware: Approximately 1 in 50 mobile phones will be infected by malware[2]. This makes mobile security just as important as securing computers.
- Social media risks: About 43% of cyber-attacks involve social media platforms[2]. These platforms can be used to spread malware or conduct phishing attacks.

[1] 50 Surprising Cybersecurity Facts & Statistics [2024] - DigitalDefynd

[2] 30 Interesting Cyber Security Facts and Stats of 2024 (knowledgehut.com)

Capital
Partners

PRIVATE WEALTH
ADVISERS

22 Delhi Street West Perth WA 6005	T +61 8 6163 6100 capital-partners.com.au

Disclaimer: This information is of a general nature only and may not be relevant to your particular circumstances. The circumstances of each investor are different and you should seek advice from a financial adviser who can consider if the strategies and products are right for you.