MERIDEON
WEALTH STRATEGIES

KEEPING YOU SAFE ONLINE

10 steps to reduce cybercrime risk




STEP #1

Get educated and educate your family members

The first protection against cybercrime is to stay up to date with the ways you could be attacked so you are better prepared.

Today, many attackers target the human mind and exploit the built-in trust in human relationships. It can be incredibly easy to lure someone into clicking a link that downloads malware, or to provide the password or security info.

PHISHING

- A typical phone phishing attempt is where the attacker pretends to be someone you trust, e.g. IT Support or a customer, and will tell a reasonably plausible story, in order to trick you to give out your password or help them to get someone's account details.

- In a spear phish attack, an attacker sends an email that looks like a legitimate message from a trusted company, in hopes the victim will give up some lucre or account credentials.

Normal phishing emails are typically relatively easy to spot (they look spammy), but they are getting more and more sophisticated and believable.

RANSOMWARE

Malicious software that encrypts all your files on an infected devi ce without your permission. Cyber attackers then hold your data or systems to ransom, and demand a payment by digital currenci es, such as bitcoin to unlock your data. Ransomware is often circu lated via phishing email messages and have been known to sprea d laterally to other unpatched computers once a single computer has been infected.

Protect yourself from cybercrime!

- [ ] Never give out your password to anyone, even family members
- [ ] Handle all emails with a bit of suspicion. Remain sceptical of any email that has a strong call to action
- [ ] Ensure email tone is consistent with what you expect
- [ ] Ensure bank transfers and other sensitive processes have adequate sign off measures
- [ ] Be wary of spammy social media invites, particularly from LinkedIn.

STEP #2

Install security software on your systems

Installing a comprehensive security software solution on your computer systems is an important measure to improve your cyber security.

You should make sure that security software is installed on all computers that are connected to or capable of connecting to the internet.

Make sure your security software is setup to run automatically when your computers start, and that they automatically scan for malware daily. Most importantly, ensure that your security software is set to automatically update.

Free security antivirus products do not contain the same features as paid versions, so it's best to purchase a security product rather than using a free or limited trial product. Having said that, our IT company recommends a **combination of BitDefender and Malwarebytes Anti-malware** as the best free protection for home users.

SECURITY SOFTWARE

BitDefender
https://www.bitdefender.com.au/solutions/free.html

Trend Micro
https://www.trendmicro.com/en_au/forHome/products/free-tools.html

McAfee
https://www.mcafee.com/consumer/en-au/store/m0/index.html

Kapersky Lab
https://www.kaspersky.com.au/free-antivirus

Malwarebytes Anti Malware
https://www.malwarebytes.com

Be aware that most antivirus products do not always detect the latest threats, so it's still important to be cautious with unexpected email attachments or web links.

Good security software will:

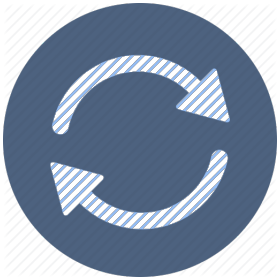
- Scan your computer(s) for known malware and remove any infections
- Scan web pages as they are being accessed to make sure there is no known malicious content that could compromise your practice's security
- Prevent connections to known malicious websites
- Prevent unauthorised connections to or from your computer or network

STEP #3

Back up your data

If there is only one take away from the recent ransomware attacks, it would be to back up your data diligently.

Make sure you have a backup plan and stick to it. This way if you are attacked by Ransomware, you can go to your backed up information rather than paying the ransom.



Ask yourself these questions:

- ☐ Do I have a plan (and have I implemented it) to keep my hardware devices and software applications up to date?
- ☐ Do I have auto-update options? Are they turned on?
- ☐ Do I have devices, such as routers/modems that need to be manually updated?
- ☐ Do I have a way to test and assure that the systems have been kept up to date?

You will need to:

- ☐ Have a backup either to a cloud service or to portable offline media
- ☐ Disconnect portable media from your device unless required, to keep it safe.
- ☐ Scan portable media before clicking on opening files.
- ☐ Do not take the risk and connect infected portable media to your computer(s)

By ensuring all your devices, operating systems and applications are kept up to date, you can minimise the possibility of being a target.

Many attacks target existing security vulnerabilities as the bad guys tend to go for the low hanging fruit. By keeping your systems and software up to date (known as patching), you will save yourself plenty of headaches.

STEP #4

Keep your systems up to date

STEP #5

Manage your passwords

Around 81% of security breaches involve the exploitation by cyber attackers of stolen or weak passwords.

It is important to that you have strong and unique passwords for your accounts and devices. A strong password , generally, has a minimum of 12 alphanumeric case sensitive characters with optional special ones, and that is not easily guessable.

TWO FACTOR AUTHENTICATION

In addition to strong unique passwords, we strongly recommend that you use two-factor authentication (2FA) to access any of your key systems and accounts (i.e. business bank accounts), where this option is available '2FA' is available for no charge.

2FA means that you also need to provide an additional factor to gain access. For example, a 2FA could be a code sent to your mobile phone via an app or SMS. This means that even if your passwords are compromised, you still have another layer of defense that can prevent cyber attackers gaining access to your accounts.

PASSWORD MANAGERS

LastPass
https://www.lastpass.com

Dashlane
https://www.dashlane.com

1Password.com
https://www.1password.com

KeePass
https://www.keepass.info

LastPass currently has a free Family version available that allows you to manage and secure your families passwords. Each person can have their own passwords or are able to share passwords with others in the family if needed.

Lastpass and other of the mentioned providers have a Security Challenge, which will go through your passwords and score you and recommend what needs changing. Once you have setup and imported all your passwords we recommend you run this and work through the list and add new Complex passwords to your websites.

Once your Password Manager is setup, clear the stored passwords from all your browsers and devices.

This is also a great way to create a Digital Estate Plan so you can provide your master password to someone who is managing your Estate.

The Password Checklist

- [ ] Don't write your passwords down or store them on your computer
- [ ] Never share your password with anyone, even family members.
- [ ] Don't EVER click 'remember this password' on your browser or mobile device, and make sure you log off when you're finished.
- [ ] Use a Password Manager

STEP #6

Be alert when browsing the web

Whether you're shopping, catching up with the news or connecting with friends, it's important to take precautions to protect your security.

- Check that the website has correct spelling, grammar and consistent design.
- Only transact online if you see a green padlock icon and https (the 's' stands for secure) in the web address bar
- Use **2FA** where you need to provide another form of ID as well as your password or PIN
- Don't log on to online banking sites or other websites that contain your personal information if you're connected to public Wi-Fi.
- Always log out of secure sites when you've finished using them, and close the browser window
- To be extra safe, it is best not to use Mobile devices to shop online or do internet banking.

Secure your banking :

- [ ] Make sure your bank has your up-to –date contact details, so they can get in touch if they see suspicious activity.
- [ ] Check the privacy and security settings in your web browser – you can disable cookies and clear your browsing history.
- [ ] Keep any financial info, such as physical bank statements or bills, in a secure place. Destroy them when they are no longer of use.
- [ ] If you notice any suspicious activity in your bank account, contact the bank right away.

Things to do right away:

- [ ] Change the default SSID: this is your network name which can be updated in your Modem Settings page.
- [ ] Turn off SSID Broadcasting: this means that your network is not discoverable to strangers and therefore less likely to become a target. You can give out the details to those you trust.
- [ ] Use WPA2: It is the security method added to WPA for wireless networks that provides stronger data protection and network access control.
- [ ] Change your default configuration password: this can be done in the Setting page and should meet the Strong Password criteria.

Manufacturers often configure routers and Wi-Fi access points with default passwords that must be changed to prevent cyber attackers from gaining easy access to your network.

STEP #7

Secure your home Wi-Fi

STEP #8

Social media and mobile security

With the coming of the digital age, access to unlimited amounts of data are at one touch of a button or one click on the screen.

You must be careful when sharing information online as you'll never know whose eyes are looking at it.

Social Network Checklist

- [ ] Never post personal and sensitive information
- [ ] Modify your privacy settings to control who sees your posts and who can tag you
- [ ] Avoid disclosing your location in posts
- [ ] Have different passwords for your social media accounts and other accounts such as for online banking
- [ ] Sign out of your social media accounts when using a public computer
- [ ] Be careful with any unusual posts or messages, especially those with links in them

Mobile Security Checklist

- [ ] Set your mobile phone to lock after a period of non-use
- [ ] Use a strong PIN, passcode, fingerprint detection or facial recognition.
- [ ] Use a device manager to help you find your phone and wipe data if lost.
- [ ] Only install apps from reputable publishers and official stores – and read the reviews first.
- [ ] Manage permissions for each app to control what data they collect, store and share.
- [ ] Don't remove hardware restrictions on your mobile phone to allow installation of unapproved apps

More and more people are connecting to the world wide web every second. Social media has become part of our daily lives. People love sharing posting personal views and achievements on different social media platforms. This is really what it's supposed to be, but we should still be aware of what to and what not to share in the virtual space as these can all be used by ill-minded cyber hackers against you or your family.

STEP #9

Use secure file sharing

When sharing files on the web, it is important that you know that only the intended persons are the people who can access the file.

As financial advisers we require a lot of information and forms to be provided and we would prefer to reduce the use of email to do this.

Please start to adopt the new technology we introduce so we can help improve your security – and save you time and money!

When sharing online:

- ☐ Sending personal info via email can be insecure. Consider putting passwords on documents or avoid sending
- ☐ Utilise our secure portals or File sharing tools to update information with us and your advisers
- ☐ Share and sign documents via secured systems (e.g. SignNow)

Help us catch any impostors!

- ☐ Provide us with a "secret word" to use if you need to authorise a transaction
- ☐ Have a chat to the team when you call so we get to know you and your voice.
- ☐ Tell us a bit about your life, travels, family and interests so we have more ways to check
- ☐ Be prepared to sign a form, or pop in to see us when you want us to make changes to your finances that raise red flags.
- ☐ In emails, communicate in your natural way. This allows us to get an idea of how you write, your vocabulary, formality etc.

The strongest defense we have to ensure we protect your money is for us to double check with you personally when high risk requests or suspicious activities take place.

The better our team knows you, the easier it is for us to identify someone impersonating you.

STEP #10

Let our team get to know you

CYBERCRIME SECURITY ACTIONS CHECKLIST

MERIDEON WEALTH STRATEGIES

Passwords

- [ ] Download a Password Manager
- [ ] Create a Complex Password for your Password Manager that you can remember
- [ ] Import all your passwords into it
- [ ] Run a Security Challenge and follow the recommended password changes
- [ ] Clear all your passwords from Browsers, spreadsheets and mobile devices
- [ ] Setup 2 factor Authentication

Hardware Security

- [ ] Change your wi-fi's default SSID
- [ ] Turn off wi-fi SSID Broadcasting
- [ ] Keep any printed financial information in a secure place.
- [ ] Set your mobile phone to lock after a period of non-use
- [ ] Make sure your bank has your up-to –date contact details
- [ ] Use a strong PIN, passcode, fingerprint detection or facial recognition.
- [ ] Setup a device manager to help you find your phone and wipe data if lost.

Software Security

- [ ] Download a good Antivirus and Malware software on all systems
- [ ] Ensure they are set to auto-update & run on startup
- [ ] Set to auto download the latest patches for all your software and delete unused software
- [ ] Check the privacy and security settings in your web browser
- [ ] Backup your important data to the cloud or portable device
- [ ] Change Social Media privacy settings to control who sees your posts and who can tag you

Dealing with Merideon

- [ ] Provide us with a "secret word" to use if you need to authorise a transaction
- [ ] Download Signnow to your Mobile device for secure document signing
- [ ] Setup your Client Portal so we can share info with you securely

MERIDEON
WEALTH STRATEGIES

LET'S WORK TOGETHER TO PROTECT YOUR WEALTH

Find out more. Contact us through the following:
T: 08 9583 5299
A: Lvl 1, 14 Marco Polo Drive, Mandurah WA 6210
W: www.merideon.com.au

This booklet is a collection of security tips that were recommended at the time of publishing.
It is meant to be a guide to improve your cyber security and not a definitive plan.
You should continue to research and educate yourself on these topics to ensure you have up to date knowledge.

Enriching tomorrow!