Cyber Security

Don't ever think "It won't happen to me". Everyone, on every device that is connected to the internet, is at risk of being hacked, succumbing to a virus, being a victim of a phishing scam, malware, ransomware and other attacks are also rife.

Your personal and financial well-being through to your professional reputation and everything in between can be at risk, so we all need to continue to take Cyber Security seriously.

At Safe on Social, we believe that learning good Cyber Security practices should underpin everything that we do online.

Password management

Use long passwords 20 characters or more are best.

Use a healthy mix of characters, preferably alphanumeric, and never use the same password for multiple sites because if a hacker can access one of your accounts, it will only be a matter of time before they have your whole online life at their fingertips.

Always use a password/passcode or biometric to lock your mobile device that way if it is lost or stolen, people won't be just a pin code away from access your bank account, your social media account and many other personal things like photos.

As hard as it may seem, please don't share your passwords and don't write them down.

Update your passwords periodically, at least once every six months (90 days is better).

If you are an an Apple user, consider using the free Keychain Access to manage passwords.
Keychain Access is a macOS app that stores your passwords and accounts information and reduces the number of passwords you have to remember and manage.

When you access a website, email account, network server or another password-protected item, you may be given the option to remember or save the password. If you choose to keep the password, it's saved in your keychain, so you don't have to remember or type your password every time.

To ensure that passwords and other data stored in your keychain are secure, make sure to set up a login password for your computer.

Alternatives to Keychain Access for Windows, Mac, Android, iPhone, Linux and more can be found in this article just released by CNet, The article outlines the best password managers should you want to invest in one. https://www.cnet.com/news/the-best-password-managers-directory/

A password manager can help you to maintain strong, unique passwords for all of your accounts. These programs can generate strong passwords for you, enter credentials automatically, and remind you to update

Keep all device software up to date

Installing software updates for your operating system, apps and programs when prompted is critical and a great habit to get into.

Always install the latest security updates for your devices as soon as possible after you are notified of them. This includes app updates on your mobile devices, Playstations, Xbox. These updates always include "Security patches" where they fix any security vulnerabilities. Particularly important when your credit card details are often stored in your account details.

On your computer always make sure you turn on Automatic Updates for your operating system.

Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.

Make sure to keep browser plug-ins (Flash, Java, etc.) up to date.

Avoid suspicious emails and phone calls

Phishing scams are a constant threat. Cybercriminals may attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information.

Phishing scams can be carried out by phone, text, or through social networking sites - but most commonly by email.

Be suspicious of any official-looking email message or phone call that asks for personal or financial information. Always hover your mouse over the email address to see if it is actually from the organisation it claims to be from if you are even slightly suspicious.

Common Phishing scams at present include people ringing up claiming to be the support division or your telecommunications provider (they never call you unless you have called them and requested a call back) saying there is a problem with your internet etc.

Be careful what you are clicking on. Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically, and often silently, compromise your device. If attachments or links in the email are unexpected or suspicious for any reason, don't click on it.

Never leave devices unattended

The physical security of your device is just as important as its technical security.

If you need to leave your laptop, phone, or tablet for any length of time password lock it so no one else can use it.

If you keep sensitive information on a USB Flash Drive or external hard drive, make sure to keep them password locked as well.

For desktop computers shut-down the system when not in use or lock your screen. If you are using a device in a library or hotel foyer etc. – don't forget to log out!

Protect sensitive data

Be aware of sensitive data that you come into contact with.

Keep sensitive data (e.g student records, health information, etc.) from being saved to your device. Keep it off of your workstation, laptop, or mobile devices.

Securely remove sensitive data files from your system when they are no longer needed.

Always use encryption when storing sensitive data.

Use mobile devices safely

Considering how much we rely on our mobile devices, seriously consider implementing all of the following.

Lock your device with a PIN, password or a biometric (fingerprint or facial recognition).

Only install apps from trusted sources.

Keep your device's operating system updated.

Don't click on links or attachments from unsolicited emails or texts.

Regularly backup your data

Most devices are capable of employing data encryption through two-factor authentication consult your device's documentation for available options.

Use Apple's Find my iPhone
https://www.apple.com/icloud/find-my-iphone/

alternatively, the Android Device Manager
https://support.google.com/accounts/answer/6160491?hl=en

Back up on a regular basis - if you are a victim of a security breach, the only guaranteed way to repair your computer is to erase and re-install the system.

Install anti-virus protection

Only install an anti-virus program from a known and trusted source. Keep device software up to date to ensure your anti-virus program remains effective.

A list of some of the best Anti-Virus software can be found here:

https://www.top10bestantivirus.com/free-antivirus-software?gclid=EAIaIQobChMIxOX1uJuP4AIVFK6WCh3rGwp4EAAYASAAEgKY0fD_BwE

Use a VPN (Virtual Private Network)

A VPN creates a virtual encrypted tunnel between you and a remote server operated by a VPN service. All your internet traffic is routed through this tunnel, so your data is secure. Your device will appear to have the IP address of the VPN server, hiding your identity and location.

If you are not using a VPN, it is wise to avoid public Wi-Fi networks, perhaps at a cafe or airport. Typically, you might connect without a second thought. However, do you know who might be watching the traffic on that network? Can you even be sure the Wi-Fi network is legit? It could have easily been set up to steal personal and financial information from people that logon to the "free wi-fi".

Keep in mind that it's tough to tell whether or not a Wi-Fi network is what it appears to be. Just because it's called Sydney Airport WiFi doesn't mean they own it.

If you connect to that same public Wi-Fi network using a VPN you can rest assured that no one on that network will be able to intercept your data not even the operators of the system itself.

One free implementation is SecurityKISS https://www.securitykiss.com which offers ad-free VPN access with data limited to 300MB/day. That's plenty of scope for checking email, looking at maps and other casual Wi-Fi uses.

CyberGhost https://www.cyberghostvpn.com/en_US/ is another option that offers a free tier, but also has a paid version that boosts speed.

There are many other VPN services available, including paid and free options (there is a basic version available within ios12). It's worth doing your research to work out which is best for your needs, especially if you are a heavy-duty user.

Disconnect.me https://disconnect.me helps to protect against session hijacking via browser extensions for Chrome and Safari; it also offers a standalone Android VPN app called Secure Wireless that automatically detects unsecured Wi-Fi and activates a VPN where needed.

w: safeonsocial.com

e: wecanhelp@safeonsocial.com