Technology Connections.com.au
Cam Stirling
0414 482 542
Patient | Friendly | Professional Help

Cyber Safety Suggestions

The internet or “online” as it is often called, connects most of the computers, phones, iPads, even TV’s in the world together, allowing information, photos, stories etc to be shared. Unfortunately, the internet also exposes us to the risk of theft and fraud. The following list of suggestions is intended to help reduce the risk of using the internet. It is **not** an exhaustive list. Unfortunately, the people who use the internet for theft tend to come up with new ways of stealing and deceiving people faster than those who seek to prevent internet theft and fraud. If in doubt, please seek multiple perspectives on this topic.

Context is very important	If you receive an email, text message or phone call, ask yourself “have I done business with this person or organisation?”, “am I expecting this message from them?” If the answer is “no” it’s likely a scam. If the answer is “I’m not sure” exercise caution. For example, if you receive a message claiming to be from PayPal and you don’t have a PayPal account, that message is likely to be fraudulent. If you receive an email saying that you have won a prize but you don’t remember entering a competition, this is likely fraudulent. Similarly, if you receive a text message regarding a parcel you didn’t actually order, that is likely to be fraudulent and should be ignored. If you receive an email from Google whilst you are setting up Gmail on your phone or iPad, the context suggests that this email is real.
Check email addresses carefully	Carefully check the part of the email address after the @ symbol - if it perfectly matches the internet address of an organisation that you do business with (e.g. anz.com.au) then it is more likely that the email really does come from someone in that organisation. Be careful as scammers create websites and email addresses which are very similar to legitimate addresses. Email addresses from Gmail, Hotmail and other free email services and email addresses with lots of numbers and letters are often used by scammers and should be treated with additional caution.
Don’t click links from unverified senders	Only after you are certain that an email comes from a verified source, person or organisation, should you consider clicking a link. This is because links may run programs which open your computer or phone to fraudulent activity. Most banks and large service organisations (energy, insurance, government departments etc) no longer send links in emails and text messages for this reason, so any link should be treated with great caution.
Use “fit for purpose” passwords	Remembering passwords for different systems is challenging. Most people keep a record of their passwords and many people “re-use” passwords or subtle variations on passwords, to assist in remembering. Ensure that passwords for critical services including banking, superannuation and financial services are longer, stronger and different (unique) to those passwords which you may use for less critical services like news subscriptions, ABC iView etc. This will reduce your risk of theft and fraud across multiple service providers if one password is compromised.
Never provide remote access to your computer or phone	Scammers might be able to take remote control of your computer, phone, iPad or other devices but usually this can only happen if you provide consent. Usually this consent looks like clicking on “ok” or “yes” when remote control software including AnyDesk, RemotePC, TeamViewer, UltraViewer or others are on your device. If scammers take remote control of your device, they can often also take control of your banking and transfer large sums of money quickly which are very difficult, if at all possible, to get back.

Use multi-factor authentication for financial services	Multi-factor authentication means that in addition to a password, for larger transactions or transactions involving transfers of money to people or organisations to whom you've not previously transferred money, your financial services provider (bank etc) will send a text message to your phone to verify that you really want to transfer money. You may need to contact your bank to set up this worthwhile extra security.
Limit potential financial losses	For online purchases and/or overseas travel, consider setting up a separate credit card with a small limit or a debit card for an account with limited funds. This way, if your details for this limited account are obtained by scammers or thieves, they can only access limited funds, not your entire life savings. Is the cost and hassle of having another bank account worthwhile? It depends upon the value of your life savings and how widely you shop online.
Buy online from reputable suppliers	When we buy things on the internet, we usually provide our name, credit card details and postal address. This information may be shared and used for illegitimate purposes. For this reason, it is prudent to buy online from larger service providers that we know and trust. Check with friends and family. Read reviews on the internet. Consider buying from an organisation which you can visit or contact if something goes wrong. If you really must make a purchase from a lesser known online provider, consider the previous point re: limiting financial losses and the next point re: the padlock.
Look for the padlock	For any websites regarding money or your personal information including banking, purchasing things etc, make sure that the little padlock (see below) or similar symbol in Google Chrome is showing in front of the internet address bar near the top of your web browser (Chrome, Safari, Firefox, Edge etc). This means that "Secure Sockets Layer" is encoding the messages between your computer or phone and the systems running the website, making it harder for scammers to intercept and read that information. For example - 
Consider a second SIM for banking	If scammers have enough of your personal information, they might be able to "port" (move) your mobile phone number off your SIM card (Subscriber Identity Module) on to a different SIM card, thereby taking over your phone number which may allow them to receive text messages from your bank and anyone else. This means that the Multi-Factor Authentication mentioned earlier would no longer protect you from scammers accessing your bank accounts. If your phone is publicly available (my phone number is posted everywhere on the internet, so that people can contact me for technical help) and if your phone supports dual-SIM cards, you may wish to consider purchasing a second SIM card and keeping the phone number on that SIM card private, for banking only. Is the cost and hassle of having another SIM worthwhile? It depends upon how widespread your phone number is known and the value of your life savings.

Keep up to date copies of your valuable information	As a back-stop, in case all of the suggestions above and other measures that you have taken to protect your information have still failed to stop scammers from disabling your computer, phone or iPad, keep up to date copies (sometimes called “backups”) of your valuable information, which may include documents, photos, financial information etc. In the worst case scenario, where you may need to start from scratch with your computer or phone, you can at least re-load the copies of your information. You might choose to back up your information on an external hard disk drive or USB/thumb-drive. You’ll also need to know how to restore the information, or know someone who can help you to do that. If you wish to reduce the risk of losing your information in the case of a house fire or theft from your home, you might consider backing your information up using a “cloud based” system such as Google Drive, Microsoft OneDrive or Apple iCloud.
If you do get scammed or hacked, there are suggested steps to help reduce your losses	If the worst case scenario occurs and you are scammed or hacked, it is important to notify as many important parties as quickly as possible to try to reduce your losses. This can be stressful and time-consuming. I have helped people to deal with this type of situation and will help anyone in this situation. As well as the obvious organisations, such as your bank(s) there are many organisations which you should inform as soon as possible if you are scammed or hacked. The Office of the Australian Information Commissioner (Australian Federal Government) has some information regarding parties to contact on their website, here – https://www.oaic.gov.au/privacy/data-breaches/identity-fraud