Computer checklist to help avoid fraud and scam attacks

1. Never ever call a number that pops up on your screen or your email...ever! No matter how convincing and "urgent" it is!

2. Never save your bank account password to your web browser...if you have, then change your password immediately.

3. Never click a link or call a number provided on an email using credentials provided within the email from anyone saying they are from Windows, Microsoft, Office, Adobe, ATO, Telstra, Optus, AMP, ANZ, NAB….etc.. not limiting this list to any other "trusted" company or person. Always lookup the number or web address separately first, then call the number or type in the website manually if need be.

4. Never just pay via "BSB and account" to a first time invoice that has been emailed to you, even if the email is sent from the person you are expecting to receive it from. Instead call the business first (not using the number on the email) to confirm the correct BSB and account. And especially do not pay it if you notice the bank details are different to what you have used in the past. Confirm via phone first.

5. Never grant a stranger (a stranger being anyone that you do not know in person and fully trust) remote access to your computer for any reason, no matter how convincing they are. Observe stranger danger; Scammers will stop at virtually nothing to convince you to let them access your computer/bank account.

6. Never follow instructions from a stranger on any computer issue, be it a printer driver not working to the more dangerous territory of assistance with emails or PayPal and banking.

7. Never write your passwords into notepad, sticky-note, word etc. Don't even take a photograph of your passwords, as these can now be harvested by computer robots. If you must, then instead, physically securely record them on paper with a strong personal cipher that no one could guess.

8. Avoid click bait. That news update about Harry & Megan, video of a dancing dog or cat falling off a shelf might be the bait that leads you away from a Facebook, craft or news site right into the scammers lair. If you do get trapped however, disengage, turn off you computer and seek immediate advise.

9. Ensure that your Windows 10 or MacOS has the latest support and security patches turned on and updated at all times. Note: Windows 11 is the current OS and Windows 10 support ends 14/10/25

10. Make sure that your computers webcam is covered at all times except when in use. Many computers these days have a privacy shutter, but a bit of dark coloured tape will suffice for those that don't.

11. Setup a password locked "admin only" account on your PC & only use the "standard" user account.

12. Never install "browser extensions" or password managers to the same web browser that you use for banking. Browser extensions can be used to "scrape" data such as bank passwords and other logins.

Get professional help from your local computer specialists.

Warragul Computer Repair
6 Smith St Warragul
03 56232777

Disclaimer: These computer and phone checklists are not exhaustive, and subject to change, and should be used as a guide only.

Phone checklist to help avoid fraud and scam attacks

1. Never hand your unlocked mobile phone to anyone that you would not happily hand that same person a blank signed check or credit card and pin – the end result may well be the same.

2. Ensure that you have a PIN lock on your phone as the very minimum security. Don't hand out your pin, and try to avoid letting it be seen when you enter it. Many people choose the fingerprint and faceID options as these are harder to copy, and cant be recorded so easily as a pin code or pattern unlock by security cameras. When choosing a pin… don't use your postcode or date of birth.

3. Turn off text preview!!...or you might as well have your phone unlocked due to a security flaw in SMS authentication.

4. Ensure you only use a current model phone with the latest support and security patches applied.

5. Only use the official banking app supplied by your bank and downloaded from the relevant official Google, Apple, or Microsoft store.

6. Never allow anyone to turn on "developer mode" or "side-load" an app outside of the relevant official Google, Apple, or Microsoft store...actually just don't let anyone use your phone.

7. Leave NFC (near field communication) turned off unless it is actually being used and make sure that it cannot be accessed when the phone is on the lock screen. Only let NFC access "need to" applications.

8. Avoid installing any unnecessary "apps" and games to your phone. While apps from the store are generally screened, there have been cases of some apps getting through and being used to steal data.

9. Set a screen lock time out of no more than 15-30 seconds as a fail safe in case you forget to manually lock the phone. It only takes seconds to loose everything with an unlocked phone in the wrong hands.

10. If you get a text message from a number that you do not recognise, treat it as a scam. "Hi mum I lose my phone here is my new number I need help" or "something went wrong and your parcel missed deliver reply here to get back" are just a some of the common attacks that are effectively going around.

When it comes to computers, security & maintenance, don't take on a scammer or major problem yourself.

Get professional help from your local computer specialists.

Warragul Computer Repair
6 Smith St Warragul
03 56232777