



Technology can be quite powerful, and although it assists in many ways, there are risks associated with its use that range from unwanted spam to viruses as well as malicious attacks and scams.

Scams are everywhere now, almost everyone is receiving phone calls, text messages and emails from scammers. These scammers are looking to gain access to your devices to steal money from your bank account or to convince you to purchase gift cards so they can launder the money from those gift cards.

No one will ever call you from financial institutions, telecommunications providers such as Telstra or NBN, Australia Post, ATO, Microsoft or Amazon to offer you support, a refund or to tell you that you have been hacked. Treat every form of contact from anyone you do not already know as suspicious. Scammers will do everything they can to convince you that they need access to your computer. Do not ever allow someone you do not know to access your computer remotely. They will commonly use Supremo, TeamViewer, LogMeIn or another form of remote access. As soon as someone says they need access to your computer or device, disconnect the call.

There are some simple steps that can help you stay safe online:

1. **Don't give up Screen Control** - Never install new software on any device at a stranger's request and never give anyone remote access to your device. Some scammers claim they can improve your technology or fix an issue with a quick remote access session. It's a trick designed to let them in.
2. **Complicate Passwords** – A good password policy is key to keeping safe online. It is best to avoid using the same password for all online accounts. While this is difficult, endeavour to make sure online banking passwords and email account passwords are different. It is a good idea to include upper case, lower case, numbers and special characters in all passwords.
3. **Privacy of Passwords** – Never provide your passwords or access to your devices to anyone that is not known to you. Many scams are very sophisticated; they usually occur by phone or email and may even know some information about you already which is how someone can fall victim to a scam. Financial institutions will never call you asking you to provide information by phone.
4. **Check validity of emails** – often scammers create an email address that looks similar to the email address of the person you may know in an attempt to deceive the recipient. For example, the person you know is Joe Bloggs, but the email address that the scammer is using does not belong to Joe, it belongs to the scammer.

The subject line will often say, urgent or please help, it may even say that they cannot talk on the phone because they are sick. If the person you know is asking for money or gifts via email or text messages, it will be a scam as the person you know will or should be asking you in person. See the image below, you can confirm if an email is a scam by checking the email address in the brackets and comparing it to other valid emails received from the person you know:

From: Joe Bloggs <jb011@gmail.com>

Date: Fri, 11 Jul 2025 at 8.00 pm

Subject: Urgent – please help

PROBUS CLUB INFORMATION SHEET

Staying Safe Online

Effective: 4 August 2025



Sometimes, the email address is hidden with only the name of the person showing on the email, by hovering a mouse over the name Joe Bloggs, the email address will show allowing you to confirm if that is the email address that belongs to the person you know.

If you receive an email asking for money or help and you are unsure if it is legitimate, ring the person that claims to be the sender to confirm.

5. **Check source of links and attachments** – never click on a link or open an attachment unless you know they are from a reputable source.
6. **Use a generic Club Email Address** – if you are on the Club's Management Committee, avoid using personal email addresses on behalf of the Club. Often the Club's email address will be published on the Club's website or Newsletter. Displaying emails on the internet increases the risk of the email being used for unwanted spam or hacking.

It is suggested that Clubs use a generic email address which has the benefit of all correspondence being received at one central location. There are several free email providers, and these include Gmail - which is the preferred option as it is user friendly. Sample generic email addresses can be created for each Management Committee position such as presidentsampleprobus@gmail.com, secretarysampleprobus@gmail.com.

Instructions on how to set up a gmail address are available in the Club Administration section of our website.

7. **Use a generic contact number for the Club** – similar to a generic email address, Clubs should consider obtaining a dedicated phone number for the Club for publishing to potential members. This could be a simple phone on a prepaid plan which can be retained with the Secretary or Membership officer as the calls received on this dedicated Club number will be from potential members. This reduces the ability for scammers to contact various Committee members on their private phone numbers. Members can still have access to personal contact numbers of the Committee provided they are not shared outside of the Club.
8. **Verify Payment Information verbally** – always confirm any payment details that have been requested by email verbally with the sender. There are some sophisticated scammers who can intercept emails and change the payment information on an invoice to look quite legitimate. It is good practice to verbally confirm all payment information before making a payment. Similarly, if a company that you regularly make payments to change their bank details these should also be confirmed verbally before a payment is made.
9. **Do not install software unless verified appropriately** – Never install applications or software unless you know they are from a reputable source.
10. **Install Anti-Malware/Anti-Virus** – It is important to have a software package on your computer that actively runs in the background that scans for any kind of malicious software also known as malware. Malwarebytes Anti-Malware is a free option that is available at: <https://www.malwarebytes.com> –

PROBUS CLUB INFORMATION SHEET

Staying Safe Online

Effective: 4 August 2025



this is available for Windows, Mac and Android devices. Once installed, run a scan on your computer to check for malware, it is recommended that you run a scan once a week.

11. **Update devices regularly** – All computers and devices receive regular updates. It is recommended that you keep them up to date.
12. **Backup all devices** – Backing up your devices at regular intervals is something that must be done. Backing up to a USB Flash Drive or USB Hard Drive is a great option. Windows 10/11 have a feature called File History that can be enabled. This will allow your computer to automatically backup files whenever your USB Hard Drive is connected. Mac computers have Time Machine, this can be enabled when you attach a USB hard drive, and it will back up the whole computer.
13. **Do not use Public WiFis** – Public WiFis should be avoided completely unless you have a VPN (Virtual Private Network) in place. Public WiFis are not encrypted and everything that happens on them can be captured. They are often hotspots for capturing passwords and other details.
14. **Consider a VPN (Virtual Private Network)** – A VPN service is extremely useful to have. A VPN will encrypt and protect you while you use the internet, and it blocks anyone from seeing what you are doing online. A suggested VPN service to use is: <https://www.privateinternetaccess.com/>
15. **Enable Firewalls** – Windows and Mac computers all come with built-in firewalls. By default, these will be enabled. It is a good idea to check that your firewall is enabled and working. This can be done by searching for Firewall on either Windows or Mac.
16. **Use the latest Operating System** – Moving to the latest version of an operating system is best practice for security. Windows 11 is the latest version of Windows and MacOS Sequoia 15 is the latest version of Mac. Microsoft will be dropping support for Windows 10 in October 2025.

If you have any questions about this information sheet, please contact our Team.