Keep Yourself Safe Online

The internet and the World Wide Web (www) have opened up opportunities for people to learn and in some ways; it has made the world a smaller place. However, there are people and groups out there who use these modern tools to exploit others. The cartoon on the left is what people experience by way of email on many days. In many ways the old saying of "If it sounds too good, it is".

The way we make ourselves "safe" on the "www" is dependent on a range of factors. For many parts of the Church people use computers connected directly to the internet and the "www" while at the other end of the scale, people use computers connected to a large local internal network that then funnels and secures its users to the "www". How you keep yourself safe is also a function on how "tech savoy" you and the organisation are. Small parishes may rely on others to provide them with support while larger parts of the Church (like the Board of Administration) have both internal and external people providing advise as to the best solutions to protect their users and the data stored in their systems "safe".

No matter what your size, there are some simple things that we should all think about to make ourselves (and the wider Church) safe. All this "stuff" comes under the general heading of "cyber security". The most common forms of cyber-crime reported in New Zealand are computer viruses and malware, credit card fraud, online frauds, phishing (pronounced "fishing"), identity theft and mail take-overs. There are no guarantees and the days of "lone wolf" individuals working by themselves in isolation are long gone. Today there are vast networks of organisations and some nations actively involved in cyber-crime.

Here is a list of simple steps that can be taken to protect yourself, the Parish and therefore the wider Church. It can also make your home computer safe.

1. **Protect your Computer**
   - Ensure that the computer itself is in a safe place and less likely to be visible to the outside world.
   - Ensure that users have a strong password to logon onto the computer (NOT password, password123, 123456,1111111, etc.).
   - Ensure that you have anti-virus, anti-spyware and firewall software installed, and working and that the software you use is kept up to date. All modern operating systems (such as Microsoft Windows 10 and 11) have firewalls and some sort of anti-spyware/malware software built into them (Microsoft Security Essentials). As a bare minimum, activate them and ensure they are kept up-to-date). There are also free systems available and subscription based products available. Google "5 best anti spyware" or 5 best antivirus" systems, read the reviews from several sources.
   - Make sure that the operating system you use (like Microsoft Windows 10, Windows 11, Apple IOS, and Linux) and applications (like Office) and other programs are updated with the latest versions or updated as soon as they become available. Using older operating systems such as the operating system Windows XP and Windows 7, which are no longer supported by Microsoft, are at risk of being exploited and should NOT be used at all.
   - Uninstall programs that you do not use or do not intend to use.

2. **Protect your Data**
   - Make regular backups of your data, onto an external device (external hard disk, USB stick, OneDrive, Google Drive, Drop Box, etc.) and keep that backup offsite or online. This can be undertaken by a simple copy from the hard drives of your computer to the external device or by using dedicated backup and restore software.
   - The main considerations are regular backups and store offsite.

3. **Create Strong Password**
   - Use strong password or a passphrase using letters, numbers and symbols. The modern way to create strong passwords is to use things like words in a song that you like. For example, it could be "StairwaytoHeaven" but it depends on the software you are using. Some software does not allow you more than eight characters.
   - Use different passwords for each of your applications or online accounts.
   - When you need to store your user names and passwords somewhere, use an application to do this. There are free ones, such as LastPass and KeePass and some of the paid products have free versions. Google "5 best password managers" and see what is on offer.
   - Change passwords on a regular basis.

4. <u>Monitor Access Management</u>

- While this may not be an issue in smaller Parishes, access to the local Parish computer should be limited and documented to all. Have a policy around access and make sure people know what it is.
- In a business environment, everyone should have their own logon details to the business systems, which are reviewed regularly to ensure they have access to the functions they require to perform their roles. If an employee changes their role, does that mean their access to certain systems needs to change?
- Remove Administrator access rights from users who do not need them. Remember that an Administrator to a computer can delete whatever they like and remove important applications and data.
- Work closely with the people who supply IT services for you. Ask if they have remote access to your system and how they do this, what security they have in place to limit their staff from access to your systems.
- If a person leaves the organisation, disable their log on account or just change their password.

5. <u>Take Care around Attachments and Links in Emails</u>

Email is currently the most common way most cyber threats are spread. The threat can vary from malicious software being sent in an email, to email accounts being taken over by cyber criminals who send emails that look and feel as if they have come you.

<u>Things to Remember and Look for</u>

- Emails are like sending post cards in the old way of doing things. Everyone can see them. Take care on what you send, whom you send it to and the language used.
- Emails that do not address you by name, or do not include information within the email to prove that the sender knows you.
- Emails that use urgency or appeals for emergency help or funds, which are designed to make you act quickly.
- Emails that ask you to make financial transactions (urgent transfers to an account you do not know about, payment of an invoice for work done you do not know about, etc.)
- Emails that ask you to update personal and financial information.
- Emails that contain links or attachments or links in emails from senders you do not know, or are not expecting.
- Do not respond to, click or open any attachments or links with these traits.

- Even if you know the sender, if the email is asking you to make a financial transaction that is not normal or unexpected or does not feel right, you should always check with them by phone, even if the email states they cannot be reached by phone. Remember that the person's email system could have been compromised.

6. Tips

- If it sounds too good or too bad a situation, it probable is.
- Do not provide your banking, credit card or other financial information to others via unsolicited emails or phone calls.
- Scrutinise all email requests for payments, and always contact the sender by phone to confirm the instructions if you have any concerns.
- Use two-step verification processes where available.
- Do not use unsecured third party supplied Wi-Fi networks for online banking. They are "open" systems for anyone to use and listen into.
- Do not use third party or untrusted app stores. Research the apps you download.
- Do not share too much information on social media.
- Keep your computers, devices and their applications up to date and ensure that anti-virus software is installed, working and kept updated.

The Methodist Church is able to offer email addresses with a @methodist.nz or @methodist.org.nz that works through the Microsoft online mail exchange server. This server has some features that helps minimise some of the "bad things" from getting to your PC. IT DOES NOT PROVIDE FULL PROOF PROTECTION, but is a start. This is done through Microsoft Office 365 which includes online data storage for backups to the "Cloud". It also uses two step authentication (also known as MFA) to protect you, the Church and the data. If you are interested in knowing more about this, please contact Peter van Hout (peterv@methodist.org.nz).

For more information visit:

www.connectsmart.govt.nz

www.netsafe.org.nz