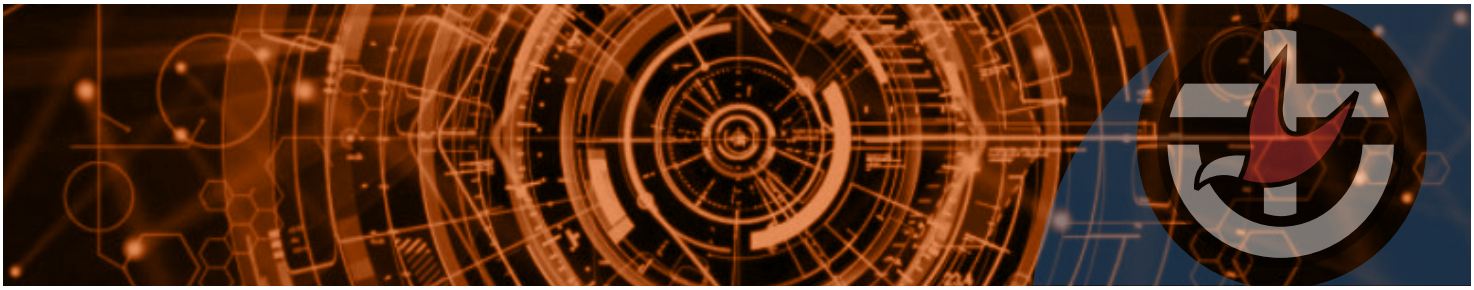

Cyber Security Information

Recently there has been increased cyber-attacks against Australian governments, companies, aged care and healthcare sectors across the country. There has also been COVID-19 themed malicious cyber activity by financially motivated cyber criminals are using different methods , which are designed to lock or encrypt an organisation's valuable information, so that it can no longer be used, and has been observed being used alongside other tools which steal important business information.

Since the pandemic's outbreak, the Government's Scamwatch has received more than 3,060 coronavirus-themed scam reports with more than $1,371,000 in reported losses.

In a recent Gartner (Leading research and advisory company) article the following survey results were stated, 71% of security professionals reported an increase in security threats or attacks since the beginning of the coronavirus outbreak. The leading threats are phishing attempts (cited by 55% of respondents), malicious websites claiming to offer information or advice about the pandemic (32%) and increases in malware (28%) and ransomware (19%).

If we look at just our environment for the month of July 2020:	
Firewall attacks and Network intrusion attempts	1M+
Spam blocked	11k+
Viruses blocked	470+

Scam Emails, SMS, Instant Messaging, Social Media:

'Dodgy' emails designed to trick recipients out of money and data. Phishing (pronounced 'fishing') they are emails from individuals or organisations you 'think' you know. They mimic phrasing, branding and logos to appear 'real', before conning users to click on a link or attachment. Here, they defraud users by asking them to provide or confirm their personal information, such as passwords and credit card numbers, or to pay a fake account. They can also send an attachment, designed to look genuine, with malware inside.

Spotting a scam

- Typos and grammatical errors
- Poor image quality
- Sense of urgency
- Suspicious links and attachments

What to do when you receive spam and Malicious email:

- Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types
- Do not provide sensitive personal information (like usernames and passwords) over email
- Watch for email senders that use suspicious or misleading domain names
- Beware of requests for details or money
- Be wary of unusual payment requests
- Choose passwords carefully
- If you are utilising Synod IT services you can forward any suspicious email by highlighting the email in question, then pressing CTRL + ALT + F and sending to **submit.spam@victas.uca.org.au**

How to reduces spam emails:

- Don't share your email address online unless you need to and consider setting up a separate email address just to use for online forms or shopping.
- As much as possible, have separate email accounts for personal and business use.
- Use a spam filter to catch these messages before they get to your inbox. Most modern email systems have reasonably effective spam filters to prevent spam appearing in your inbox. If you're not sure, ask your internet service provider.
- Delete spam messages without opening them.
- Before using your email address online, read the website privacy policy – it will tell you how they will use the personal information you provide.
- When you sign up for an online account or service, be aware of default options to receive additional emails about other products and services.