

## CYBER-ATTACKS! WHAT CAN WE DO?

As you will know, we have had a number of “phishing” (pronounced ‘fishing’) attacks on priests’ email of late. I asked Bruce Thom, Senior Advisor at Codeblue, our diocesan IT provider, if he could give us some tips and explanation as to what is happening. You might find the below helpful, and feel free to replicate some or all of it in your newsletters and bulletins if you think it will help educate your parishes and communities too.

In an effort to further enhance our cyber defence, we want to highlight some common methods of cyber-attack that everyone should be aware of:

### 1. Phishing Attacks

**Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.** It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack [*more on that later*], or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

The following illustrates a common phishing scam attempt - there are thousands of examples:

1. A spoofed email (ostensibly from Microsoft or some other well-known multi-national organisation such as a bank or telco provider) is mass-distributed to as many people as possible.
2. The email claims that the user’s password is about to expire. Instructions are given to **“Recover Account”**.

Microsoft account team

Sep 13 at 11:51 PM

To Me

Microsoft account

## Security alert

We think that someone else might have accessed the Microsoft account [nj\\*\\*\\*\\*\\*@y7mail.com](#). When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, we can help you do it now.

[Recover account](#)

Learn how to [make your account more secure](#).

Thanks,  
The Microsoft account team

[Reply](#), [Reply all](#) or [Forward](#) | [More](#)

Another example - *as is happening in our case* - is receiving an email from an unknown source acting as the Parish Priest [or other “trusted person”] asking for you to buy them gift voucher cards (e.g. iTunes, etc.).

**Note the email address is not correct** and more often than not the grammar is incorrect and there are spelling mistakes!

**From:** "Fr. Tony Dunn" <[parishpastor7700@gmail.com](mailto:parishpastor7700@gmail.com)>  
**Date:** 16 August 2019 at 2:17:38 PM NZST  
**To:** Helen Luxford <[helen@luxford.net.nz](mailto:helen@luxford.net.nz)>  
**Subject:** Re: Peace be with you

Can you help me to get a Google play card worth \$500 at \$100 or \$50 denominations for a friend of mine going through cancer in the hospital. He needs the cards to download his favorite musics and videos to boost his confidence on his next phase of surgery and fight over cancer which he's going to undergo. Can you get it from any store around you now and have it sent directly to my friend email at the hospital, I will pay back as soon as i can. Thanks

On Thu, Aug 15, 2019 at 7:14 PM Helen Luxford <[helen@luxford.net.nz](mailto:helen@luxford.net.nz)> wrote:

Ok - what can I do?

Kind Regards,  
Helen

On 16/08/2019, at 1:24 PM, Fr. Tony Dunn <[parishpastor7700@gmail.com](mailto:parishpastor7700@gmail.com)> wrote:

Hi,how are you doing?

I need a favor from you, email me as soon as you get this message.

God Bless,  
Fr. Tony Dunn

A further example follows on the next page.



----- Forwarded message -----  
From: **Sally Jones** <sjones1234@aol.com>  
Date: Sat, Aug 11, 2018 at 2:43 PM  
Subject: Re: Hello  
To: [jsmith@gmail.com](mailto:jsmith@gmail.com)

Alright, I'm sorry I'm putting this to you. I'm currently in a meeting. Please I need you to purchase iTunes gift card 5 pieces - \$100 each at the store? I would reimburse you when am through, Let me know if you can help with that right now. Thanks

Regards  
Sally Jones

On Saturday, 11 August 2108, Joe Smith <[jsmith@gmail.com](mailto:jsmith@gmail.com)> wrote:

Sorry had a 10:15 with my mentor.

On Sat, Aug 11, 2018 at 1:28 PM, Sally Jones <[sjones1234@aol.com](mailto:sjones1234@aol.com)> wrote:  
Joe. Are you free at the moment?

Regards  
Sally Jones

Sent from my iPhone

## 2. Ransomware

Ransomware is increasingly being used by hackers to extort money from organisations. Ransomware is a type of malicious software that takes over your computer and prevents you from accessing files until you pay a ransom.

Here are some simple things you can do to help avoid a ransomware / malware attack:

### Think Before You Click

The most common way ransomware enters organisational networks is through email. Often, scammers will include malicious links or attachments in emails that look harmless. To avoid this trap, please observe the following email best practices:

- Do not click on links or attachments from senders that you do not recognise. Be especially wary of *.zip* or *.pdf* files with links imbedded in them, or any other 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.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

If your computer is infected with ransomware, you will typically be locked out of all programmes/ files and a “ransom screen” will appear. In the unfortunate event that you click a link or attachment that you suspect is malware or ransomware, please contact your IT support immediately!

---

*“Beware, keep alert; for you do not know when the time will come...  
what I say to you I say to all: Keep awake.” [Mark 13:33,37]*

Nothing's new under the sun, is it!!!!