



Anglican Diocese of Auckland

Stay alert for phishing emails

The Diocesan Office is aware of sophisticated phishing emails targeting parishes.

These emails can appear to come from trusted sources, including clergy, and may request sensitive information such as parish roll details or other personal information.

Should we receive emails like this, it's helpful to take a moment to pause and verify unexpected requests before responding. This is particularly important if the request involves money, personal information, confidential records, or urgent action.

If you're ever unsure, it's best to contact the person directly using a phone number or email address you already know and trust, rather than replying to the message.

For more information about staying safe online, visit:

- [Netsafe](#)
- [Own Your Online](#)

What to do if you receive a suspicious email

If something about an email doesn't seem quite right, consider the following steps:

- Avoid clicking links or opening attachments
Unexpected links and attachments can sometimes contain malicious software or lead to fraudulent websites.
- Don't reply straight away
Replying can confirm that your email address is active and may encourage further scam attempts.
- Take a closer look at the sender
Check the sender's full email address, not just the display name, and watch for unusual addresses or spelling errors.
- Verify the request through another channel
If the email appears to come from a known person or your parish, the Diocesan Office, the Bishop's Office, a bank, or another trusted organisation, contact them directly using known contact details to confirm the request.
- Report the email
Forward the message to your local IT support person or designated parish contact. If available, use your email system's "Report Phishing" or "Report Junk" feature.
- Remove the message
Once reported, delete the email from your inbox and deleted items folder.

If you have already clicked a link or opened an attachment

Don't panic. Taking prompt action can help reduce any potential risk.

You are encouraged to:

- Disconnect from the internet if possible.
- Change any passwords that may have been affected.
- Contact your IT support person for advice.
- Contact your bank immediately if the email involved banking or payment information.
- Contact the Diocesan Privacy Officer on 09 302 7201 if personal or confidential information belonging to another person or organisation may have been involved. You may also need to notify the Privacy Commissioner.
- Keep an eye on accounts and systems for any unusual activity.

Common signs of phishing emails

Be particularly cautious of emails that:

- Create a sense of urgency or pressure you to act immediately.
- Ask for passwords, banking information, or personal details.
- Include unexpected attachments or links.
- Appear to come from a senior leader requesting urgent action or payment.
- Contain unusual wording, spelling mistakes, or unfamiliar sender addresses.

If something feels unusual, it's always worth taking a moment to check before responding.