

Phishing, Scams and Social Engineering

Guide to Identifying and Reporting Cyber Threats

For: New Zealand Registered Architects Board

Version: 1.3 – Final

Prepared by: CORUM Limited

Date: 01 October 2026

Division	Information Services
Publication Date	01/10/2026
Most recent review	01/10/2026
Review Period	Annually
Owner	Stefanie Joe, Executive Officer - Operations
Approved By	Stefanie Joe, Executive Officer - Operations

Version	Author	Date	Description
V 1.0	Adam McDonald	28/09/26	Initial draft
V 1.1	Janine Corke	29/09/26	Updates
V 1.2	Chris Corke	30/09/26	Review and updates
V 1.3	Chris Corke	01/10/26	Final Revision

Table of Contents

INTRODUCTION3

CURRENT THREATS TARGETING MICROSOFT 365 USERS.....3

WHAT YOU SHOULD LOOK FOR4

PROTECTING YOUR CREDENTIALS5

IDENTIFICATION AND REPORTING PROCESS6

Introduction

As an organisation that relies heavily on Microsoft 365, email, Teams and cloud collaboration tools, NZRAB is a target for cybercriminals. Modern phishing attacks increasingly use realistic branding, AI-generated content, compromised accounts and fake login pages.

Current Threats Targeting Microsoft 365 Users

Fake Microsoft 365 sign-in pages

Hover your mouse over the web link to check that the link is taking you to the website you are expecting. If the link name isn't what you expect, you can go to your expected website to find the link/location on their site.

Note, if this is on your phone, hover won't work, so simply don't click – leave until you get into the office and can run through the steps above on a protected PC. Remember, no email is so important that a phone call cannot first verify its validity.

QR code phishing (Quishing)

Read the preview URL: When you point your phone's camera at a QR code, a preview link usually hovers on your screen. Read it carefully before tapping.

Watch for fake domains: Check for misspelt words, extra numbers, or weird dashes in the web address (e.g., brand-5443XXX.com instead of brand.com)

Malicious SharePoint and OneDrive invitations

Be alert to messages sharing a link to SharePoint/OneDrive folders. If the message is from someone in the office, ask them to confirm first. Hover over the link to ensure the link is pointing to the location you are expecting.

Microsoft Teams phishing

A cyberattack where scammers use the Microsoft Teams platform - often via external chat or calls - to trick employees into compromising their accounts, downloading malware, or granting remote access. Don't respond to these and treat them in the same manner as a suspect email.

SMS scams (Smishing)

A cyberattack that uses deceptive text messages to trick people into sharing personal information, sending money, or clicking on malicious links for courier packages, etc. Don't respond to these and treat them in the same manner as a suspect email. If it is confirmed phishing, block the number.

AI-generated voice calls (Vishing)

Vishing, short for "voice phishing," is when someone uses a phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them. AI tools are making this attack easier and can match the voices of the person being imitated.

MFA fatigue attacks

Where a hacker floods a user's device with relentless multi-factor authentication (MFA) push notifications, hoping the overwhelmed victim will eventually tap "Approve" just to stop the spam. If you haven't requested, then

always deny the prompt, then advise Silicon and the Executive Officer – Operations.

What You Should Look For

You should look beyond the initial request. Urgency and pressure, unusual sender information, unexpected requests, unexpected file shares or links, and authentication requests you did not initiate.

Before responding to any unexpected email, message, phone call, file share or request: Pause, Assess, Check Independently, and Report if Uncertain.

Urgency and Coercion

Demands for immediate action, threats of service termination, or requests to bypass standard approval channels (e.g., "Do this immediately or your account will be locked"). Taking time to read through what is being requested and then discussing it with someone near you can give you time to think that this request might not be real.

Anomalies in Sender Identity

Display names that match a colleague or manager paired with an external, misspelt, or completely unrelated email domain. Inspect the full sender address: Scammers often spoof display names to make it appear to be a coworker or boss, but the underlying email address belongs to an external domain.

Unexpected MFA requests

Receiving an MFA request when not accessing specific work portals could be an attempt to hijack your MFA security keys and spoof your mobile device to authorise MFA requests.

Unexpected File Shares or Links

Notifications from SharePoint, OneDrive, or document portals that come from unexpected senders or point to external domains rather than official authentication portals.

Unusual Requests for Data or Financial Changes

Requests to provide or update bank account details, change payroll settings, or purchase gift cards under NZRAB or management's name.

Generic Greetings and Formatting

Impersonal greetings or corporate branding inconsistencies that feel "off," even if they lack traditional typos.

Verify unusual requests

Out-of-band: If a manager, HR, or finance team member sends an unexpected message demanding an urgent bank transfer, gift card purchase, or sensitive payroll data, do not reply directly. Call the staff member using a known phone number or chat with them via an internal channel (Microsoft Teams) to confirm. Verify Independently: Contact organisations using official phone numbers found on the back of bank cards, bills, or verified web domains.

Since phishing is the most common form of social engineering, let's take a closer look at seven areas in an email and their corresponding red flags.

FROM

- An email coming from an unknown address.
- You know the sender (or the organization), but the email is unexpected or out of character.

TO

- You were copied on an email and you don't know the other people it was sent to.

DATE

- You receive an email that you would usually get during normal business hours, but it was sent at 3:00 a.m.

HYPERLINKS

- There are misspellings in the link.
- The email contains hyperlinks asking you to take an action.
- When you hover your cursor over the link, the link address is for a different website.

From: hr@yourorganization.net
 To: judy@yourorganization.net
 Date: Tuesday, December 3:00 AM
 Subject: Urgent Notice

Hi Judy,

Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey](#) or download the attachment.

Thanks in advance for your cooperation!

<https://survey-monkee.com/>

Thanks so much. This really helps me out!

Your CEO

SUBJECT

- The subject line of an email is irrelevant or doesn't match the message content.
- It's an email about something you never requested or a receipt for something you never purchased.

CONTENT

- The sender is asking you to click on a link or open an attachment.
- The email is asking you to look at a compromising or embarrassing picture of yourself or someone you know.
- You have an uncomfortable feeling, or it just seems odd or illogical.

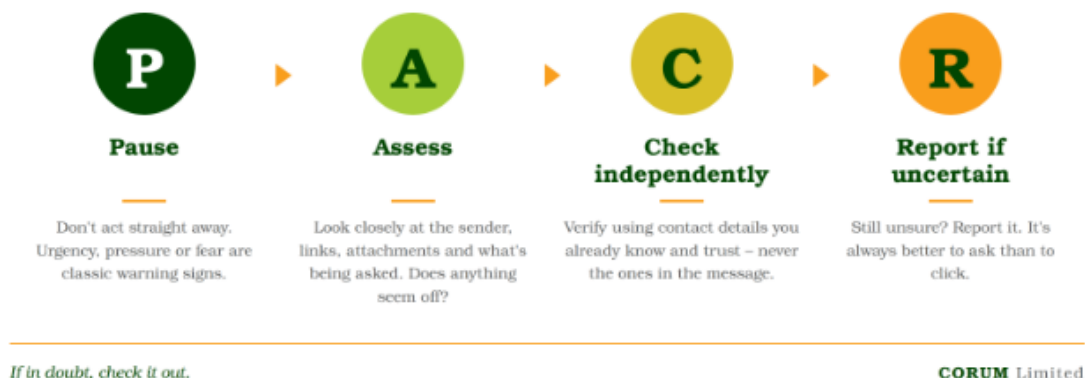
ATTACHMENTS

- Any attachment you receive that you aren't expecting.

PHISHING GUIDE

Think before you click: P.A.C.R.

Four steps to take whenever an email, text or call doesn't feel right.



Protecting Your Credentials

Never share passwords, MFA approval requests, MFA verification codes, recovery codes, Microsoft Authenticator number matching codes, account recovery information, or security question answers. No legitimate representative from NZRAB, Microsoft, suppliers, or technical support should ask for these details.

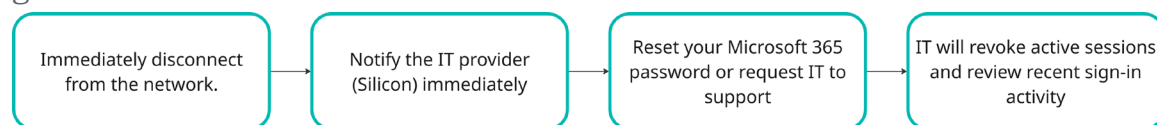
If personal or confidential information may have been exposed, notify the NZRAB Executive Officer – Operations immediately.

Identification and Reporting Process

1. Stop and do not click links, open attachments or scan QR codes.
2. Verify independently using a trusted phone number or known contact method.
3. Report suspicious messages using Microsoft 365 Report Message.
4. If personal, confidential or sensitive information may have been exposed, notify the Executive Officer – Operations immediately and notify IT.

If You Think You Have Been Compromised

Change your Microsoft 365 password if you can, report the incident immediately to Silicon and the Executive Officer – Operations (and advise if you have already changed your password), review account activity and follow IT guidance.



Silicon Contact Details

Log faults via:

Telephone: 0800 474 542

Email: helpdesk@silicon.co.nz

Good Security Habits

Pause before acting, independently verify unusual requests, keep devices updated, use MFA, and report anything suspicious.

Helpful Resources

<https://www.ownyouronline.govt.nz/> - good for checking current scams and to verify anything you find suspicious.

NCSC NZ Alerts - contains time-sensitive announcements about specific cyber threats, vulnerabilities and scams

NCSC NZ - Keeping personal information safe: a guide for organisations