Recognising and Reporting Phishing Emails

Overview

Phishing emails are fraudulent messages designed to trick you into clicking malicious links, downloading harmful files, or revealing your password. They are the most common way attackers gain access to an organisation's systems.

At PBR, we also conduct **simulated phishing exercises** through Phriendly Phishing — these look like real phishing emails and are designed to test your awareness. Treat every suspicious email the same way, whether it is real or a simulation.

Warning Signs of a Phishing Email

Warning sign	What to look for
Unexpected urgency	"Your account will be closed in 24 hours", "Immediate action required"
Suspicious sender address	The display name looks legitimate but the actual email address is odd (e.g. support@pbr-helpdesk.net instead of @pbr.org.au)
Generic greeting	"Dear Customer" or "Dear User" instead of your name
Unexpected attachments	You weren't expecting a file, especially .zip, .exe, or Office files asking you to enable macros
Suspicious links	Hover over a link before clicking — the URL shown at the bottom of your screen doesn't match where the link claims to go
Requests for credentials	PBR IT will never ask for your password via email
Too good to be true	Prize notifications, unexpected refunds, gift card requests from "management"

What To Do If You Receive a Suspicious Email

1. **Do not click** any links or open any attachments
2. **Do not reply** to the email or provide any information
3. **Report it** to IT using the Report Phishing button in Outlook (see below)
4. If you accidentally clicked a link or entered your credentials, **contact IT Helpdesk immediately** at helpdesk@pbr.org.au

---

How to Report a Phishing Email in Outlook

Outlook Desktop (Windows)

1. Select the suspicious email in your inbox (do not open it)
2. In the ribbon at the top, look for the **Report Phishing Email** button (it may be under the "..." more options menu)
3. Click it — a confirmation dialog will appear
4. Click **Report**

Outlook on the Web (Browser)

1. Open the suspicious email
2. Click the **three dots (...)** menu at the top right of the email
3. Select **Report** then **Report phishing**

If You Cannot Find the Report Button

Forward the email to helpdesk@pbr.org.au with a brief note that you believe it is a phishing attempt.

About Phriendly Phishing Simulations

PBR uses **Phriendly Phishing** to periodically send simulated phishing emails to staff. These are safe — they do not contain real malware — but they look convincing on purpose.

If you click a link in a simulation, you will be redirected to a short awareness page explaining what to look for. This is not a punishment — it is a learning opportunity.

The best response to any phishing simulation is to report it using the Report Phishing button in Outlook, just as you would a real one.

Revision #3
Created 2026-05-08 05:36:36 UTC by PBR_Documentation
Updated 2026-05-08 05:45:34 UTC by PBR_Documentation