Security Awareness

Protecting your PBR account — recognising phishing emails, completing security training, and staying safe online.

- Recognising and Reporting Phishing Emails
- Accessing Your Security Awareness Training (Phriendly Phishing)
- Keeping Your Account Secure

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.

Accessing Your Security Awareness Training (Phriendly Phishing)

Overview

PBR uses **Phriendly Phishing** as its security awareness training platform. You may be assigned training modules periodically — you will receive an email notification when a module is assigned to you.

Completing assigned training is mandatory for all staff.

Accessing Training via the Email Link

1. Open the training notification email sent to your PBR inbox
2. Click the link in the email to open the Learner Hub
3. Sign in with your PBR email address and password if prompted
4. You may be asked to approve an MFA prompt on your Microsoft Authenticator app
5. Your assigned training modules will be listed — click **Start Course** to begin

---

Accessing Training via the Learner Hub Directly

1. Open a browser and go to https://learnerhub.phriendlyphishing.com/login
2. Enter your PBR email address and click **Next**
3. Sign in with your Microsoft 365 credentials if prompted
4. Your assigned modules will appear under **Assigned Learning**

Managers — Viewing Your Team's Training Progress

1. Log into the Learner Hub as above
2. If you manage staff, you will see a **Team View** button in the top right — click it
3. Click **Course Results** to see who has completed or has outstanding training
4. You can filter by person's name or training status (complete, incomplete, failed)
5. Managers can view up to four levels of staff below them

If a staff member you manage is not visible in your Team View, contact IT Helpdesk — their reporting line may need to be updated.

Need Help?

Contact IT Helpdesk at helpdesk@pbr.org.au

Keeping Your Account Secure

Overview

Your PBR account gives access to email, files, financial systems, and customer data. Keeping it secure is your responsibility — and one of the most important things you can do to protect PBR.

Strong Passwords

- Use a **long passphrase** — three or four random words are more secure than a short complex password (e.g. *correct-horse-battery-staple*)
- Never use your PBR password on any other website or service
- Never share your password with anyone — including IT staff. IT will never ask for your password

---

Multi-Factor Authentication (MFA)

MFA adds a second layer of security to your account. Always approve MFA prompts yourself — if you receive a prompt you did not initiate, **deny it immediately** and contact IT Helpdesk, as someone may be attempting to access your account.

See: Multi-Factor Authentication (MFA)

Lock Your Screen

Always lock your screen when stepping away from your computer — even briefly.

- **Windows shortcut:** `Windows key + L`
- Your screen will also lock automatically after a period of inactivity

---

If You Think Your Account Has Been Compromised

Contact IT Helpdesk **immediately** if you:

- Receive MFA prompts you did not initiate
- See emails in your Sent folder you did not send
- Cannot log in with your normal password
- Accidentally entered your password on a suspicious website
- Accidentally clicked a link in a suspicious email

The faster we know, the less damage can be done. There is no shame in reporting — acting quickly is what matters.

IT Helpdesk: helpdesk@pbr.org.au

Approved Devices Only

Only access PBR systems on PBR-issued or IT-approved devices. Do not log into PBR systems on personal computers at internet cafes, libraries, or shared kiosk devices.