Phriendly Phishing

Phishing on Your Mobile

Stay safe when accessing your emails on your mobile device. Whenever you receive an email on your phone, always check for signs of S.C.A.M.

Sender

Who is really sending you the email?

Open the email and click on the sender email, this should display the full email addresses in the To and From fields. **Ensure you know the sender** before taking any further action.

Content

What is in the contents of the email?

- **Spelling & grammatical errors** are a good indication of a phishing attack.
- **Always look under links** – hold your finger down on a link until a URL pop-up appears with the destination web address. If the URL looks suspicious, don't click.
- **Beware of attachments** – check the email for signs of phishing before opening any attachments.
- **Never fill out a form embedded in an email.**

Phriendly Phishing

Action

What does the email want you to do?

Be aware of clickbait tactics such as a:

- **Sense of urgency** – getting you to act (or click) quickly without thinking.
- **Sense of curiosity** – playing on your need to know or learn more.
- **Sense of authority** – getting you to act out of fear or respect toward a trusting authority figure.

Manage

It's a S.C.A.M.! What should you do?

If you think you've clicked on a malicious link on a phishing email, you should:

- **Use another device to reset your passwords** to all social media accounts.
- **Install an antivirus application to your phone** and scan your device.
- **Ensure your Spam filtering is switched on.**

Tips

- Spam filters help detect unwanted, virus-infected emails. You can set the feature to only allow emails from trusted sources and block the rest.
- Selecting a good antivirus app can be difficult so only download a trusted app from the Apple or Google Play Store. Be sure to read the reviews and ratings.