THINK EMAIL, THINK S.C.A.M!

**SENDER**

Who’s really sending you the email?
- An email address containing an IP is probably fake! (e.g. Microsoft@[172.16.123.135])
- Organisations will not use a free email service (e.g. mses@microsoft.com)
- Look out for unusual domain names (e.g. vaevk.in)

**ACTION**

What does it want you to do?
- Always look under the link (Tip – Hover over the link to make sure the URL is safe)
- Businesses do not use IP addresses in URLs (e.g. http://192.168.55.163/)
- Beware of opening attachments in suspicious emails
- Never fill a form embedded in an email

**CONTENT**

What’s in the email?
- Spelling and grammatical errors can be an indication of a phishing attack
- Creating a sense of urgency is designed to make you click on suspicious links
- If you receive an unexpected email, always dig deeper to ensure it’s legitimate

**MANAGE**

It’s a SCAM, what do you do?
- Don’t ever respond to a SCAM email
- Don’t do anything that the SCAM email wants you to do
- Click on the Report Phishing button on your Outlook ribbon

PHISHING AWARENESS TRAINING AND SIMULATION

www.phriendlyphishing.com
support@phriendlyphishing.com

The University of Queensland
Australia