

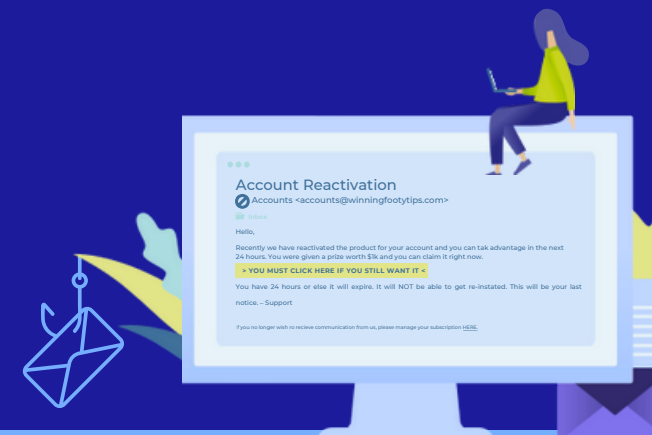
STAY SAFE ONLINE

CYBER SECURITY AWARENESS MONTH



Think Email, Think S.C.A.M.!

How to spot S.C.A.M. tactics in phishing emails



S Sender

Who is really sending you the email?

- An email address containing an IP address is probably fake. e.g. Microsoft@172.16.123.135
- Organisations will not use a **free email service** provider. e.g. microsoft@gmail.com
- Keep an eye out for **unusual domain names**. e.g. vaevk.in

C Content

What's in the contents of the email?

- **Spelling & grammatical errors** can be a good indication of a phishing attack
- Always look under links (tip: hover your mouse over the link to make sure the URL is safe)
- Beware **attachments!** Check the email for signs of phishing before opening any attachments
- Never fill out a **form** embedded in an email.

A Action

What does the email want you to do?

Be careful of clickbait tactics such as:

- **Sense of urgency** – getting you to act (or click) quickly without thinking.
- **Sense of curiosity** – the need to know or learn more.

m Manage

It's a S.C.A.M.!

What should you do?

- Don't ever respond to a SCAM email.
- Don't do anything that the SCAM email wants you to do.
- **Report it**