

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

Can you spot the S.C.A.M. tactics used in this email?

Account Reactivation

Accounts <accounts@winningfootytips.com>

lnb

Recently we have reactivated the product for your account and you can tak advantage in the next 24 hours. You were given a prize worth \$lk and you can claim it right now.
> YOU MUST CLICK HERE IF YOU STILL WANT IT <

You have 24 hours or else it will expire. It will NOT be able to get re-instated. This will be your last notice. – Support

If you no longer wish ro recieve communication from us, please manage your subscription HERE.

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



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.



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.



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.
Notify your company's IT service desk immediately.