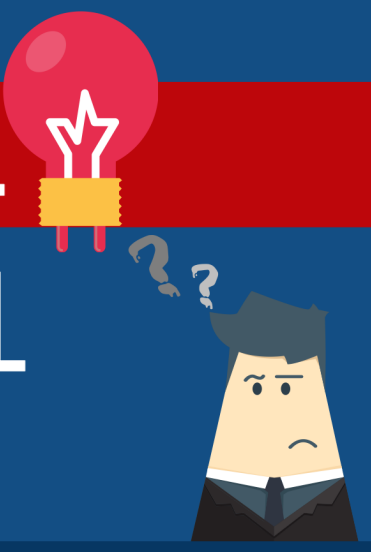
DO YOU REALLY KNOW..



..WHERE THAT EMAIL CAME FROM?

Email spoofing is when a sender's email address has been forged to appear as though it was sent from someone, or somewhere, other than the actual source. Email spoofing tools are widely available, and criminals often use them as part of Phishing attacks. For example, an email can be spoofed to appear as though it came from your bank, utility company, a well known company, or even a friend or family member. The purpose of these emails is to trick people into opening malicious attachments, or clicking on links that take them to fraudulent websites which will steal details such as usernames, passwords, as well as other sensitive information. What appeared to be a legitimate email could actually be the first step in a sophisticated scam designed to defraud you.

23%

Of people that receive phishing emails will open them .

2015 Verizon Data Breach Investigations Report

95,556

The number of phishing reports made to Action Fraud between Nov 2014 and October 2015.

Action Fraud

82s

The time it takes for cyber criminals to ensnare their first victim in a phishing campaign.

2015 Verizon Data Breach Investigations Report

BEHAVIOURS THAT PUT YOU AT RISK..

Opening attachments, or clicking on links within emails that are unsolicited or unexpected.

Responding to emails that ask for your personal or financial details.

Logging in to a webpage that you have arrived at via a link in an email.

HOW TO PROTECT YOURSELF..

Don't open attachments or click on the links within any unsolicited emails you receive, and never respond to emails that ask for your personal or financial details. Remember, you can hover over a link to see where it will really take you.

An email address can be spoofed, so even if the email appears to be from a person or company you know of, but the message is unexpected or unusual, then contact the sender directly via another method to confirm that they sent you the email.

If you receive an email which asks you to login to an online account, for example, due to suspicious activity on your account, instead of clicking on the link provided in the email, go directly to the website yourself.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

GET SAFE ONLINE
Get Safe Online
Free expert advice

CITY OF LONDON POLICE
National Policing Lead For Fraud