CITL

EMAIL SCAMS

@

TOP TIPS TO AVOID EMAIL SCAMMERS

1 CHECK THE 'FROM' ADDRESS

Always check the email address in the 'from' field. If you do not recognise the email address, or if the address looks suspicious - it probably is! For e.g. banking@barlcays.com would not be an email from Barclays Bank. Their 'from' address would end with barclays.com OR register@dfe-uk-edu.co.uk could be used to mimic and email from DfE (@dfe.gov.uk or @gov.uk)

2 CHECK THE CONTACT INFO

Does the contact information listed at the bottom of the email look genuine? Verify them against a quick web search against the name of the apparent Business or Organisation. Check dates within the body of the email - do they correspond to anything current or relevant?

3 AN IMPERSONAL GREETING?

Often, scammers won't know your name and may start with the email with a simple 'Hi', instead of being addressed to you. Or your email address may be written, rather than your name.

4 CHECK COMPANY BRANDING

Usually, scammers try to impersonate big brands such as Banks, Online Retailers, and Government Departments. Check the quality of the artwork in logos and information within the signature of the email -is it genuine?

IF IN DOUBT - CHECK IN WITH YOUR IT TEAM FIRST

WEB LINK OR ATTACHMENT? 5

If it is asking you to open a web link to enter information, ensure you check the URL the link is actually pointing to before clicking on it. Hover over over the link before you click on to it and your computer will usually show you the web address the link is actually pointing to. Ensure it is legitimate. Carry out the top checks before opening any attachments. This can lead to a computer virus or worse, a ransomware attack

PAYMENT OR BANK INFORMATION? 6

If an email asks you to send the recipient your bank information or personal data, this is cause for suspicion. Being asked to settle an invoice from an unrecognised source? Sign of a scammer. Be careful when anyone is asking for personal data such as: Bank Information, NI Numbers, Pin Numbers, Credit/Debit Card no., Security Questions or Passwords.

SPELLING OR GRAMMATICAL ERRORS? 7

Scammers often lock consistency in their communications. Watch out of basic grammatical or spelling errors - this is often a tell tale sign. If the email is pushing hard to look official, by using the words 'official' or 'warning', this would also raise suspicion.

CITL - MAKING IT EASIER FOR YOU

T: 0345 094 1005 | WWW.CITL.CO.UK | INFO@CITL.CO.UK

ARE YOU SECURE?

Speak to us about our enterprise grade security, backup and protection options at non enterprise prices!

CITL

INTERCEPT X
SOPHOS
Security made simple

Malwarebytes

Bitdefender

Acronis Backup

ico.
Information Commissioner's Office

GDPR

Dropbox

CITL

CLICKON IT LONDON

*Making **IT** easier for you...*

Hounslow Chamber
supporting business across the borough

WWW.CITL.CO.UK | T: 0345 094 1005

IT SERVICES FOR EDUCATION & BUSINESS | AV | DATA & FIBRE

REMOTE BACKUP | CLOUD SERVICES | GOOGLE | WINDOWS | iOS