www.ConsultantsLikeUs.Co.UK

PHISHING ATTACKS

How to spot a sneaky Phish!

Scammers are working harder to get into your inbox!
Everyday they send millions of emails to millions of people in the hope to catch you in their net!

Don't give them the satisfaction... Let's take a look at a recent example, and identify what to look out for.

01.

Look at who the email came from... Does this look like an Email from Gary?

If you can't see the email address, just 'hover' your mouse over the address to reveal it.

From: **Gary Hibberd <batman781@gmail.co.uk>**
Date: Tuesday, 14 November 2023 at 13:14

Subject Urgent

Hello

How are you doing today? Well I'm in a conference right now, can't talk on phone, but let me know if you got my message and if you do kindly send me your personal number.

Thanks**, Gary Hibbert**

CEO, MD Gary Hibberd of CLU

02.

Is there some pressure? i.e. "this is urgent" or "You must respond in 2hrs"?

They put pressure on you, so that you'll react, rather than taking the time to respond.

03.

Does it 'sound like' the sender? Would they normally be so formal, or informal?

04.

Does the footer of the message look right? Is the graphic missing, or is the job title wrong?

Here are some more tips and advice...

POOR GRAMMAR

Is the grammar proper not good?! Does it sound like a professional email?

If not, then it may have been written using AI, or someone who doesn't have English as their first language.

POOR SPALLING

Does the email contain spelling errors?

Again, it may have been written using AI, or someone who doesn't have English as their first language. Or using a template. For example, does it contain American spellings, not UK? (e.g. Color Vs Colour)

UNEXPECTED ATTACHMENTS

If you receive an attachment - were you expecting it? Does it feel appropriate for the email?

Emails with attachments like this are known as 'Trojan Horses', which have killer viruses within them. If you're not sure.. seek advice from IT.

LINKS THAT STINK!

Contaminated links that send you to fake websites can expose your information, or data.

Don't click links from untrusted sources. If you want to check if it's legitimate, then open a browser and visit the host site - just don't click that link!

If you receive something you suspect is phishing... Simply Block The Sender | Forward to IT | Delete the email.

For more information speak to your line manager