Protect yourself from 'phishing'

Be more aware of ways hackers and scammers try to gain access to data by email, text, phone, WhatsApp etc.

NOTE: The world of spam emails and in particular email phishing is constantly evolving, but it's better for us to offer some advice rather than none.

What is phishing?

The practice of sending fraudulent communications that appear to come from a legitimate and reputable source, usually through email and text messaging. The attacker's goal is usually to:

- gain access to your email address and password.
- to install malware on your phone/computer.
- to steal sensitive data from you or your organisation.
- gain your bank or card details to be able to steal money.

How to protect yourself from phishing

If you come accross better video or written guides than we have here, please contact the Digital team with your suggestions.

- Spotting dodgy 'domains'
- Way to help you decide if an email is genuine

How to Recognize a Spam & Phishing Emails

1. Examine the Sender's Email Address:

Spammers often use: Strange, misspelled, or unfamiliar email addresses. They might also spoof addresses to appear legitimate.

Legitimate addresses: Typically use the company's domain after the "@" symbol (e.g. info@example.com). A spammer might use info@exampie.com or info@example.co

2. Review the Subject Line:

Spam subject lines: Often use excessive capitalization, promise unrealistic offers, or create a sense of urgency.

Be wary of: Subject lines that are too vague or seem overly promotional. Examples include "Urgent! Update your information", "Get paid today!" or "Don't delete! You won a prize!".

3. Check for Errors in Content:

Grammatical and spelling errors: These are common in spam emails, especially those sent from non-native English speakers.

Generic content: Spam often uses broad, impersonal language and lacks specific details.

4. Look for Suspicious Links:

Hover over links: Before clicking, hover your cursor over the link to see the actual destination address. Be cautious if it's different from what you expect.

Avoid unknown links: Don't click on links from unknown or untrusted senders. Unusual requests for financial transactions, login details and requests to install software should be approached with extreme caution.

5. Requests for Personal Information:

Legitimate companies will not ask for your personal information, such as passwords, credit card details, or Social Security numbers, via email.

6. Be Wary of Attachments:

Unknown attachments: Avoid opening attachments from unknown sources, especially if they are unfamiliar file types like .HTM, .HTML, .EXE, or .PDF.

7. Offers That Seem Too Good to Be True:

Be wary of offers that sound too good to be true, as they are often used to lure you into a phishing scam.

8. Contact the Organization Directly (If Needed):

If you're unsure about a legitimate message, contact the organization directly via their official website or known contact information.

Don't respond to the email: If you suspect it's a scam, don't reply or click on any links.
