CloudyIT®

Stay Safe: How to Recognise and Avoid Phishing Emails

Phishing emails are a common tactic used by cybercriminals to trick individuals into providing sensitive information or downloading malicious software. Here's a comprehensive list of things to be wary of when identifying phishing emails, using UK English spellings and grammar:

1. Suspicious Sender Information

- **Unknown Sender:** Be cautious of emails from unknown or unexpected senders.
- **Spoofed Email Addresses:** Check the sender's email address carefully. It might look similar to a legitimate one but with slight variations.

2. Generic Greetings and Lack of Personalisation

- **Generic Salutations:** Phrases like "Dear Customer" or "Dear User" instead of your name.
- **Lack of Personal Information:** Absence of personalised details that a legitimate sender would know.

3. Urgent or Threatening Language

- **Sense of Urgency:** Phrases like "Immediate action required" or "Your account will be suspended."
- **Threats:** Statements threatening consequences if action is not taken immediately.

4. Suspicious Links and Attachments

- **Unfamiliar Links:** Hover over links without clicking to see the actual URL. Look for mismatches with the displayed text.
- **Unexpected Attachments:** Avoid opening attachments from unknown sources, especially if the email urges you to open them quickly.

5. Grammar and Spelling Errors

- **Poor Language Quality:** Phishing emails often contain noticeable spelling mistakes, grammatical errors, and awkward phrasing.

6. Request for Sensitive Information

- **Unusual Requests:** Be cautious if asked for sensitive information such as passwords, credit card details, or National Insurance numbers.
- **Forms:** Legitimate companies typically do not ask for personal information through email forms.

7. Mismatched or Fake URLs

- **URL Discrepancies:** Compare the URL in the email to the official website address. Look for slight variations or misspellings.
- **Fake Login Pages:** Be wary of links directing you to login pages; verify the website's authenticity.

8. Email Formatting and Design

- **Poor Design:** Low-quality logos, incorrect colour schemes, or amateurish design can be indicators of a phishing email.
- **Inconsistent Branding:** Look for inconsistencies in logos, brand colours, and overall email design compared to official communications.

9. Unusual Requests

- **Odd Instructions:** Be wary of unusual or out-of-the-ordinary requests, such as transferring money or purchasing gift cards.

10. Email Header Information

- **Check Headers:** Email headers can provide information about the actual source of the email. If unsure, examine the headers to trace the email's origin.

11. Spoofed Websites

- **Fake Webpages:** If directed to a webpage, ensure it is legitimate by checking the URL, SSL certificate, and overall design consistency with the company's official website.

12. Inconsistent Language and Tone

- **Tone Mismatch:** Be cautious if the email's tone doesn't match the typical communication style of the purported sender.

13. Requests for Login Information

- **Login Prompts:** Legitimate companies will never ask for login credentials through email.

14. Verify the Sender's Identity

- **Contact the Company:** If in doubt, contact the company directly using contact information from their official website, not from the suspicious email.

15. Phishing Report Mechanism

- **Report Suspicious Emails:** Use your email provider's phishing report feature to report suspicious emails.

By staying vigilant and using these strategies, you can greatly minimize the risk of phishing scams. For more details on top services and tools to safeguard your council, visit our Cyber Defence Hub here - Cyber Defence & Security - Cloudy IT

If you have concerns about your IT security, you can also schedule a one-on-one session with our Security & Incident Response Manager, Martyn Boyle. He will be happy

to review your IT security. Book a meeting for an introduction to our Products and Services (office365.com)