Phishing

Phishing and Vishing

Phishing is defined as the sending of fraudulent messages purporting to be from trustworthy sources, such as a company, employer, or friend. While traditionally sent by email, these scams have evolved to text message scams known as smishing, and phone call scams known as vishing. To identify phishing threats, use the SLAM Method.

Artificial Intelligence

While some messages have spelling or grammar errors, many scammers are using chatbots or other applications to craft more sophisticated messages. The rise of artificial intelligence has some benefits, like quickly identifying threats, and increasing website security, but it also allows for more cybercriminals to make malicious code and craft error-free phishing messages.

S Sender. Slightly misspelled names or domains are common red flags.

L Links. Hover the mouse over links, without clicking to show its true path.

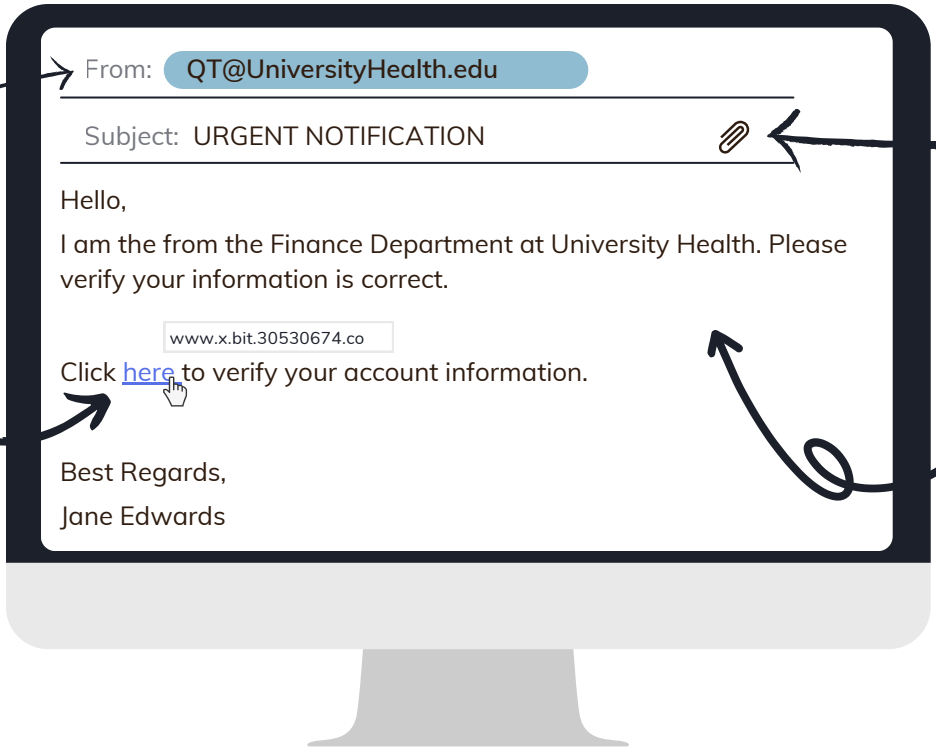
A Attachments. Any file can carry malware and should be regarded with caution.

M Message. Look for urgent requests to act and offers that seem too good to be true.

SLAM Analysis

Sender: Does the sender look familiar? Even if the answer is yes, the account could be compromised.

Links: When hovered over, the link does not lead to a legitimate site.



Attachments: Random attachment that is not mentioned in the email.

Message: The message is urgent and generic. It doesn't have grammar errors, but it could be written by AI.