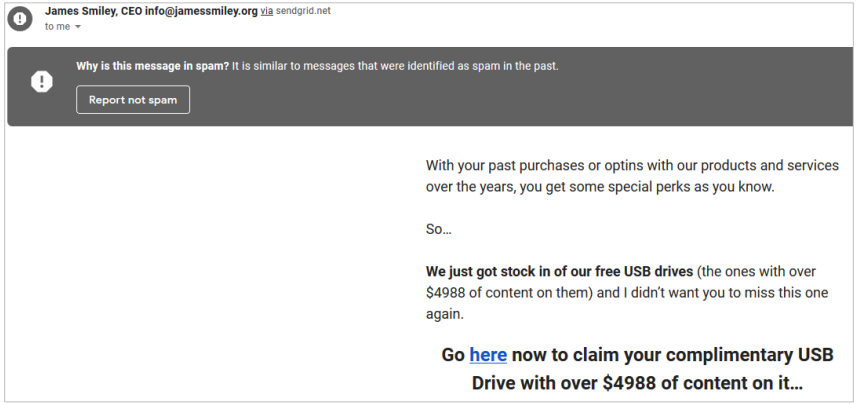
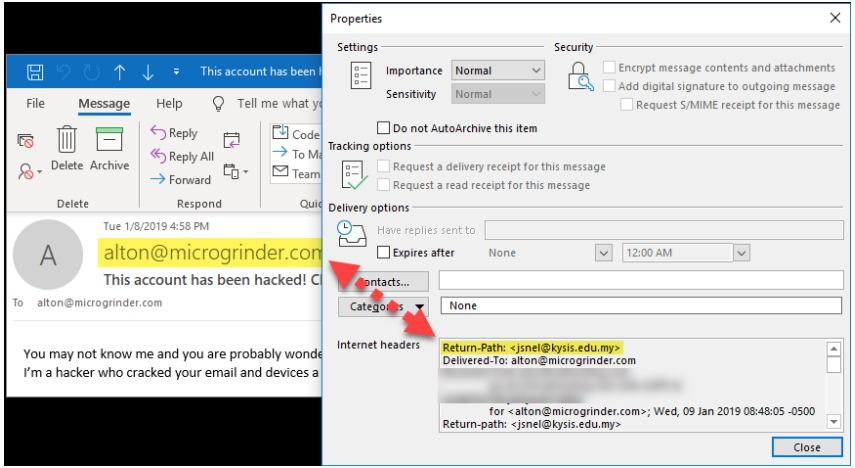
Spam Email

- **Spam email** is unsolicited emails, commonly advertising emails, but sometimes phishing and scamming attempts.
- Such email can clutter our inbox, getting in the way of emails that matter, as well as potentially carry malware.



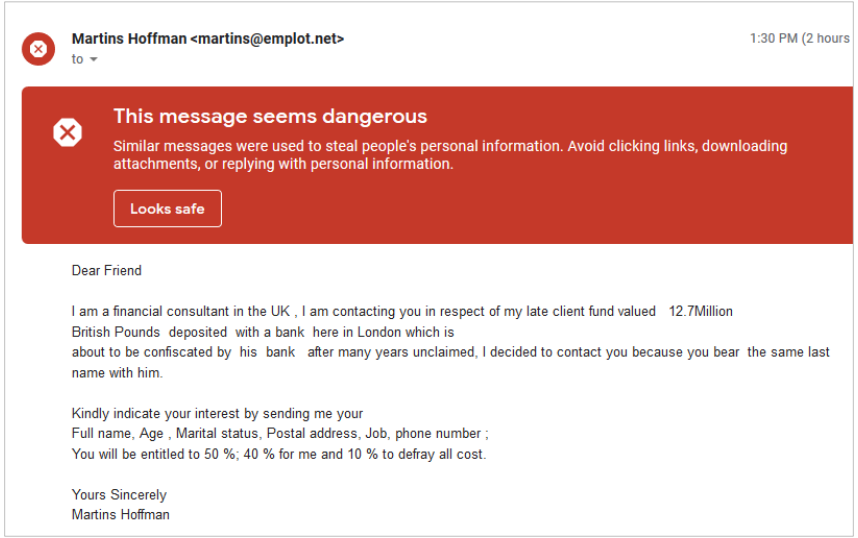
Spoofed Emails

- **Email spoofing** is the forgery of an **email header** so that the email seems to have originated from someone or somewhere other than the actual source.
- It's used in **phishing, pharming** and **spam campaigns** because people are more likely to open an **email** when they think it has been sent by a legitimate source.



Email Phishing

- **Phishing** is the practice of sending unwanted email to users with the purpose of tricking them into revealing personal information (such as bank account information) or clicking on a link.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email.
- Their goal is to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords.
- They then use your information to steal your money or your identity or both.



Email Pharming

- **Pharming attacks** redirect users from legitimate websites to fraudulent fake websites.
- This can be done server-side via DNS spoofing and also client-side.
- With **email pharming**, a user will open up an email with malware, which then installs malicious code on the user's PC.
- In one form of pharming attack, code sent in an e-mail modifies local hosts file on a personal computer.
- This code then redirects URL clicks to a fraudulent website without your knowledge or consent.