Learn How to **Detect a Spear Phishing Email**

1

Sender Address

Spear phishers trick users into thinking an email address is legitimate by using a variety of email spoofing techniques, such as using a display name that impersonates a colleague. If you're on a mobile device, expand the sender's name to see the entire email address. In addition, check for subtle differences in the domain name.

2

Subject Line

Spear phishing emails often include urgent subject lines to capture the user's immediate attention or to create pressure. Sophisticated spear phishers may be more subtle, but the subject line might still be financial in nature, including "purchase," "invoice," "direct deposit," or similar language.

3

Pretexting

Pretexting is a form of social engineering in which a cybercriminal will engage a victim over the course of one or more emails to gain the victim's trust. Based on information they've discovered about the victim, the spear phisher will engage in small talk with the victim to bring down their guard, such as "How was your vacation?" or "Congrats on the promotion."

4

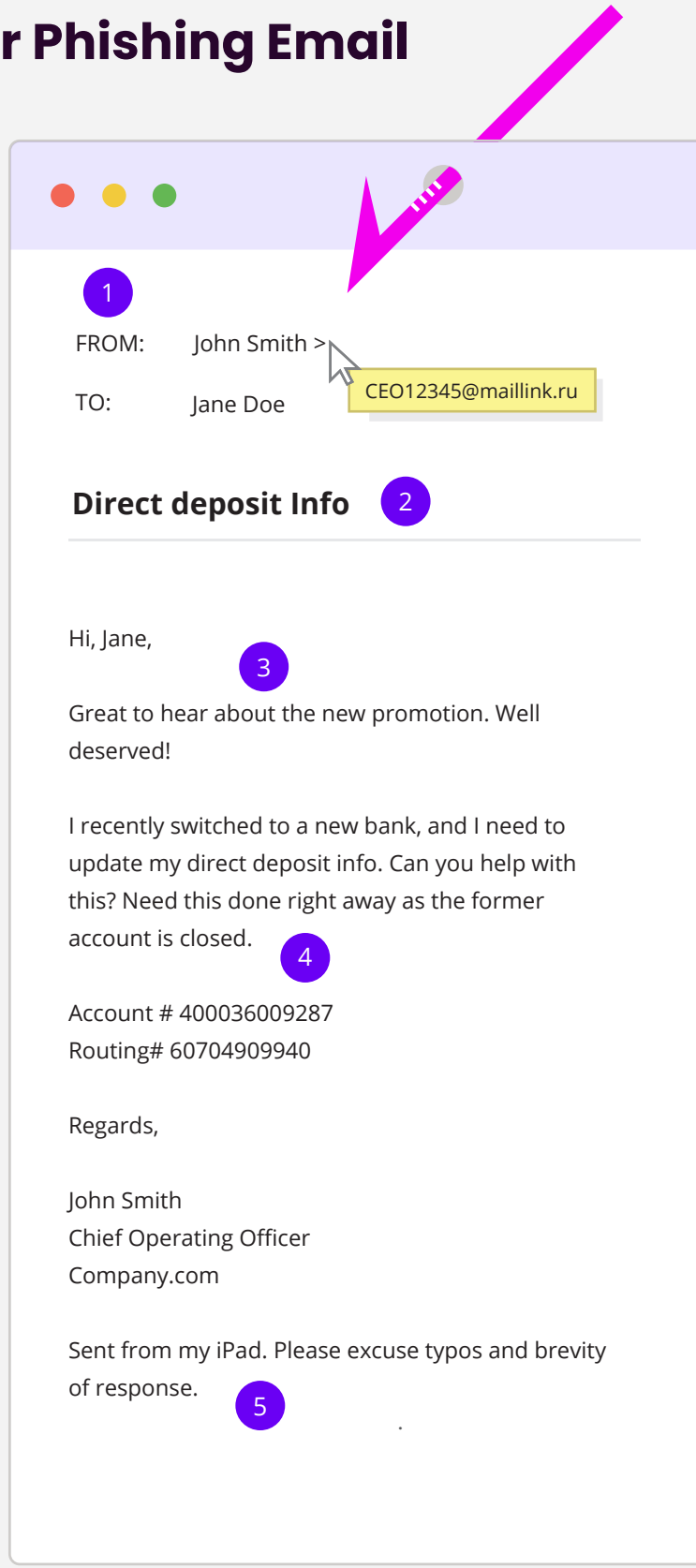
Body

Quick and to the point, the body of the email will almost always include a financial request. Spear phishers often use language designed to make the victim feel that they are the only person who can complete the request and that not doing so in a timely manner could be detrimental to the business.

5

Signature

Spear phishers often include an additional line in the email signature stating that the message was composed on a mobile phone or tablet. This helps reinforce the urgent nature of the message, creates an excuse for sending the email from a personal email address, and presents a cover for any potential grammar or stylistic mistakes in the email.



When in doubt, check it out.

If you receive a message that you think is spear phishing, we recommend forwarding it to your MSP or IT admin for further investigation.