**Phishing Attack**

A Phishing Attacks is when malicious actors posing as a trusted entity use **social engineering** in order to manipulate users into performing self-harming actions. This ranges from requesting users enter their personal information to getting the user to install malware on their device.

Three fake emails found on the devices composing the botnet have been mixed in with one legitimate email. Each has five words underlined and numbered by their position in the security question sentence that could be a part of the security question: only the legitimate email is accurate. Determine which are phishing attacks to uncover the correct security question words to progress.

**Identifying a Phishing Attack**

The following elements compose many phishing attacks, and can help narrow down the emails to reveal the most likely legitimate one. If an email contains two or more of these elements, consider it a phishing attack.

Phishing emails try to create a sense of urgency to lower your critical thinking skills.

The sender’s email address is unfamiliar or odd.

Links within them are suspicious; sometimes long, sometimes just hyperlinks, often odd domains you don’t recognize, or a series of unintelligible characters.

The email itself contains generic phrases that could be directed towards any person.

It contains ample grammar or spelling errors.