LogRhythm®

10 Ways to Detect a Phishing Email

To reduce risk of a damaging breach, it is imperative to educate your employees to stay vigilant and avoid falling victim to phishing attacks.

Here is a list of the top 10 ways to spot and handle phishing emails.

1

Don’t trust the display name of who the email is from.

Do not solely rely on the name of a person you know or trust as an assurance of the email’s authenticity. Always verify the email address to confirm the true sender. Email sender addresses can be easily spoofed or sent from compromised accounts, making it a common occurrence.

2

Look but don’t click.

A straightforward approach to examine a hyperlink (or URL) is to hover or move the mouse cursor over different elements of the email — without clicking on anything. If the displayed alt text appears unusual or does not correspond to the description of the link, it is advisable not to click on it. Instead, report it to the security operations center (SOC).

3

Check for grammatical errors.

While anyone can make typographical errors, stay vigilant when encountering emails with grammatical mistakes. Scammers often rely on spellcheckers or translation tools when crafting their messages, resulting in correctly spelled words but with improper context.

4

Consider the salutation.

Attackers occasionally employ a generic or ambiguous greeting (such as “Dear valued customer”) that aligns with automated templates. Alternatively, they may omit the salutation altogether. While this practice does not always signify a scam, it can serve as a “red flag” if something feels amiss.

5

Is this email asking for personal information?

Be cautious when emails ask for sensitive or personal information. To confirm if action is needed, contact the company's customer support or access your account directly through their official website. It is important to note that legitimate organizations rarely request such information via email, so be cautious if emails deviate from the norm by asking for unusual help or data.

6

Be careful with attachments.

Stay cautious of enticing or seemingly normal email attachments that may harbor malware. Avoid opening suspicious unsolicited attachments and verify with the sender if necessary. Beware of attachments that appear official but contain hidden malicious links, and never trust HTM/HTML attachments as they can execute code directly from your computer's memory.

7

Beware of urgency.

Exercise caution when encountering emails that employ urgency as a tactic. Phishing emails often exploit people's trust or willingness to help by creating a sense of urgency, aiming to prompt hasty decisions.

8

Check the email signature.

Always check the email signature within the body of the email to ensure it matches the sender or the claimed identity. Phishing attempts often involve mismatched or inconsistent email signatures when attempting to impersonate another person or co-worker.

9

Don’t believe everything you see.

If something appears even slightly suspicious or deviates from the norm, it is advisable to prioritize safety over taking risks. If you notice any unusual or concerning signs, it is best to report the issue to your SOC for further investigation and guidance.

10

When in doubt, contact your SOC.

Report any concerns to the SOC, as they prefer to investigate potential threats rather than risk a compromise. With the ongoing and successful nature of phishing attacks, it is crucial to exercise caution and avoid becoming another victim.

Want more tips and tricks delivered to your inbox?

Sign up for LogRhythm's **newsletter**.

Link in the comments!