WHAT NOT TO DO WITH A SUSPICIOUS EMAIL

KnowBe4 Security Tips

Learning how to identify suspicious emails is essential to keeping your organization safe from cybercriminals. But did you know that mishandling a phishing attack could be just as dangerous as falling victim to one? Here are some examples of what NOT to do when you receive a suspicious email:

DO NOT REPLY TO THE EMAIL FOR VERIFICATION.

If you receive a suspicious email that appears to be from someone you know, you may be tempted to investigate further. Replying to the email with questions like, "Have you been hacked?" or "Is this attachment safe?" only increases the security risk. If an email account has been compromised, the person who replies back to your question probably won't be who you expect. You could be communicating with a cybercriminal in disguise.

DO NOT FORWARD THE EMAIL TO SOMEONE ELSE.

The best practice is to never click a link or open an attachment that you were not expecting. But if you are fooled by a phishing email and you click a malicious link or open a malicious attachment, you may find that the link or attachment will not behave as expected. For example, after you open what appeared to be an image attachment, the file may open an installer window instead. Another example is when a malicious link redirects you to an unrelated login page. If you see the unusual behavior of a malicious link or attachment, you may think about forwarding the email to a coworker for help. But, don't do it! Whenever you click on a link or open an attachment, consider any unusual behavior as a red flag. Never forward unusual or suspicious emails to other users. If you forward a phishing email, you increase the risk of a security breach because it helps cybercriminals reach more potential victims.

DO NOT MARK THE EMAIL AS SPAM.

First, let's clarify the difference between spam and a phishing attack. Spam emails are typically annoying or unwanted advertisements. Spam is often unsolicited, but it is usually just a harmless attempt to sell you something. On the other hand, a phishing attack is a malicious email designed to look and feel like real correspondence. Phishing emails typically include a call to action such as clicking a link, opening an attachment, or even transferring money. Marking an email as spam moves that email, and any other emails that you receive from that sender, to a different folder. This means moving a phishing email to spam would only hide the problem, not resolve it.

WHAT SHOULD I DO WITH A SUSPICIOUS EMAIL?

The best way to handle a suspicious email is to notify your organization. If you report a suspicious email, your cybersecurity specialists can assess and mitigate the threat.

Here are some tips for reporting a suspicious email:

- Be sure to follow your organization's process for reporting suspicious emails. Following cybersecurity protocols will help keep everyone's information safe.
- If you don't know how to report the email, leave it in your inbox and ask a manager or supervisor for help.
- If you're not sure whether an email is spam or a phishing attack, report it and let the experts decide.