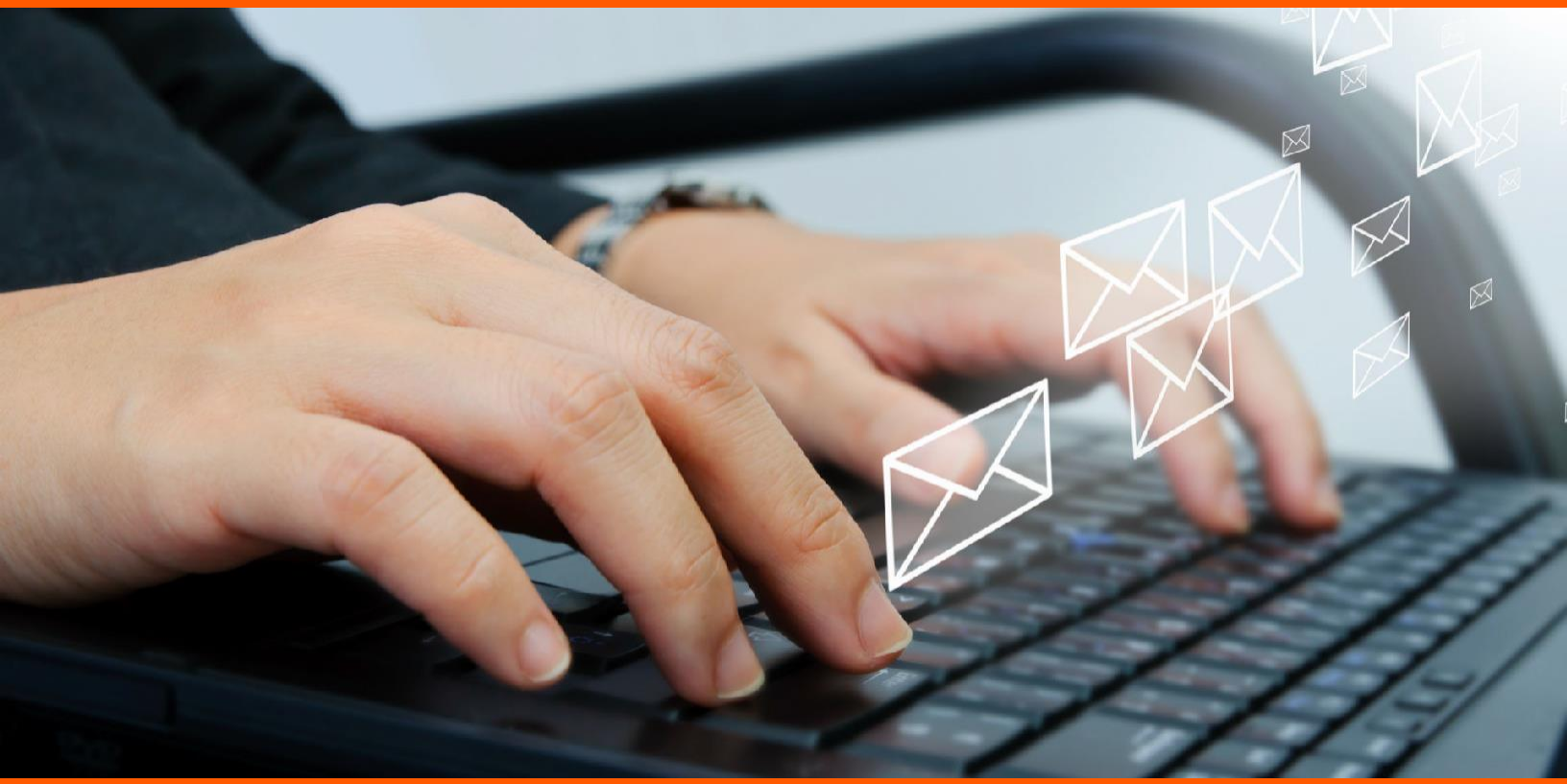
DDTN Desktop Procedure – Phishing Email



Phish Alert Button

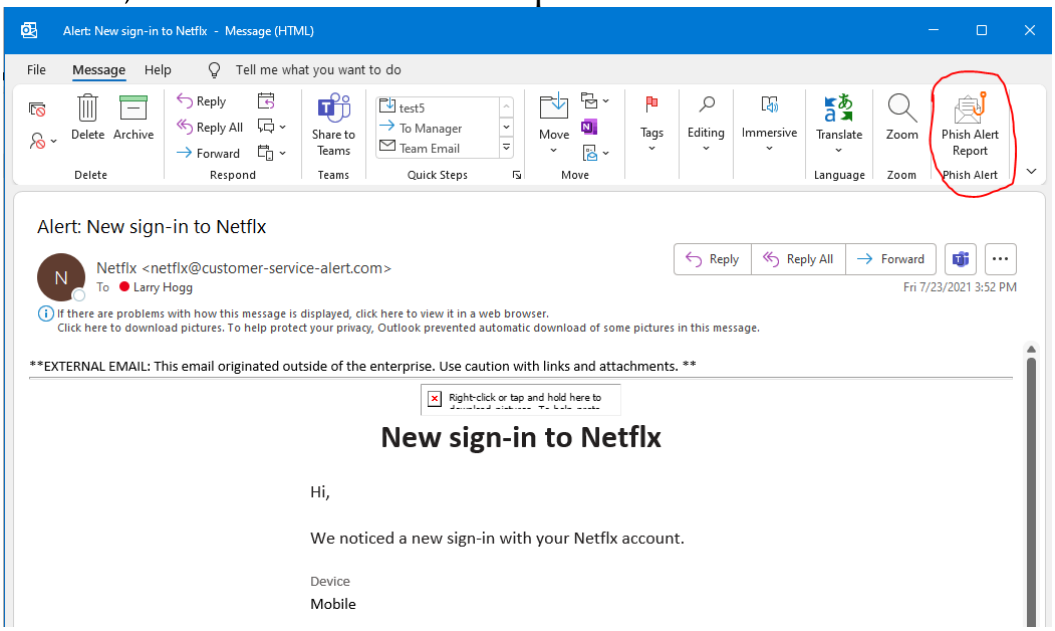
Employees report phishing attacks with one click

A Phishing Email is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake,or otherwise deceptive) message designed to trick a human victim into revealing sensitive information tothe attacker or to deploy malicious software on the victim's infrastructure like ransomware, generally though means of an attachment or clicking a link within an email.

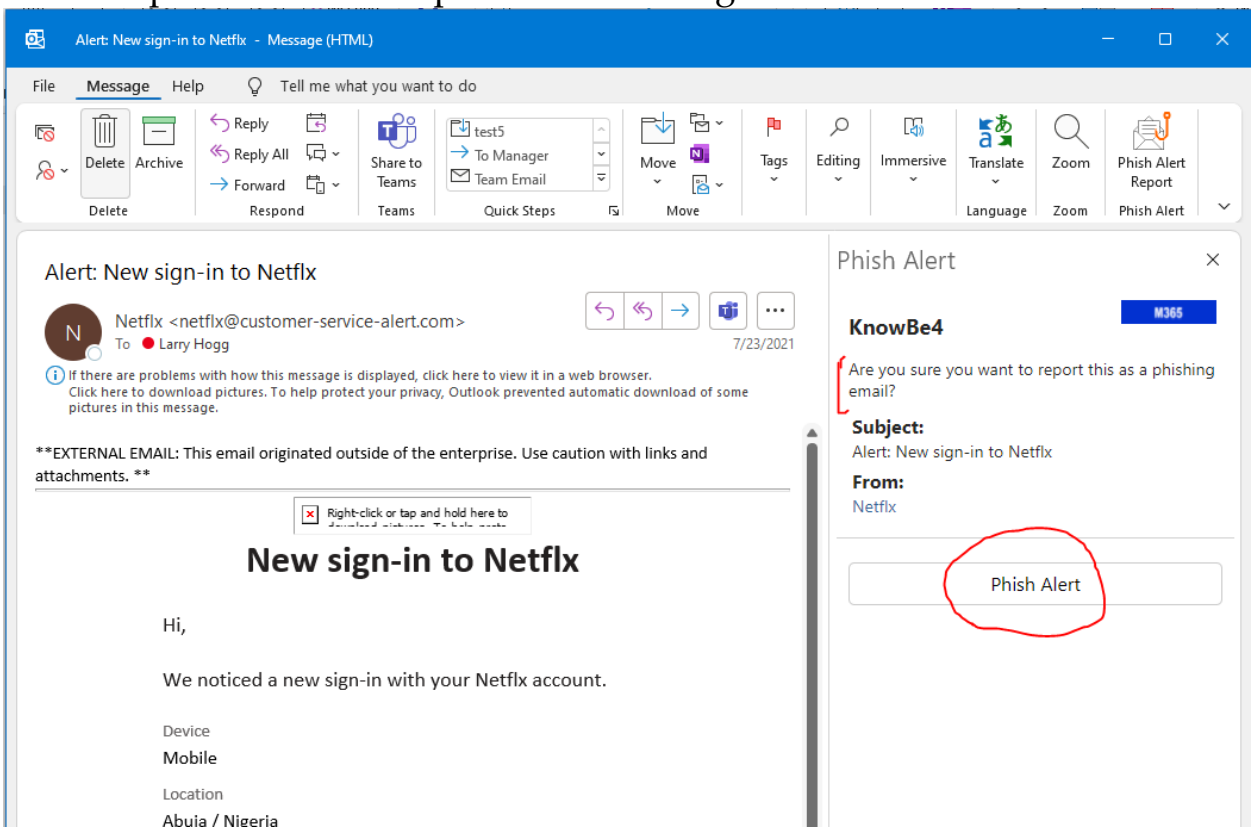
To help train DDTN employees on how these types of emails look in real-life scenarios we use a tool called KnowBe4 that crafts and sends simulated Phishing Emails to all of our employees, but the PhishingEmails that come from KnowBe4 are harmless even if an attachment or link is clicked. If you click link or attachment within one of the KnowBe4 emails you will automatically be enrolled in training session that you will be required to complete within a particular timeframe.

Our company policy also notes that you are supposed to report these types of events to the HIPAA Security Officer. Previously the procedure was to forward the emails to the HIPAA Security Officer andthe IT team. We now have a new procedure to do this built into Outlook on your computer using the KnowBe4 tool. For anything you suspect is a Phishing Email follow the procedure below:

- In the picture below there is Phishing Email that should be reported. While viewing the email,click the “Phish Alert Report” button circled.



- You will then see on the right side of the email the KnowBe4 tool pop up and ask if you're sure you want to report the email. Click the "Phish Alert" button to report the email as potential Phishing.



- If the email was one of the simulated training emails sent by KnowBe4 you will see a message that indicates, you successfully identified the email.

- If the email is truly a malicious Phishing Email you will see the below notification and KnowBe4 will automatically notify the HIPAA Security Officer and the IT team. No further action is required on your part, unless someone on the IT team contacts you to gather more information.

If you have any questions or concerns, contact your manager or the HIPAA Security Officer directly.