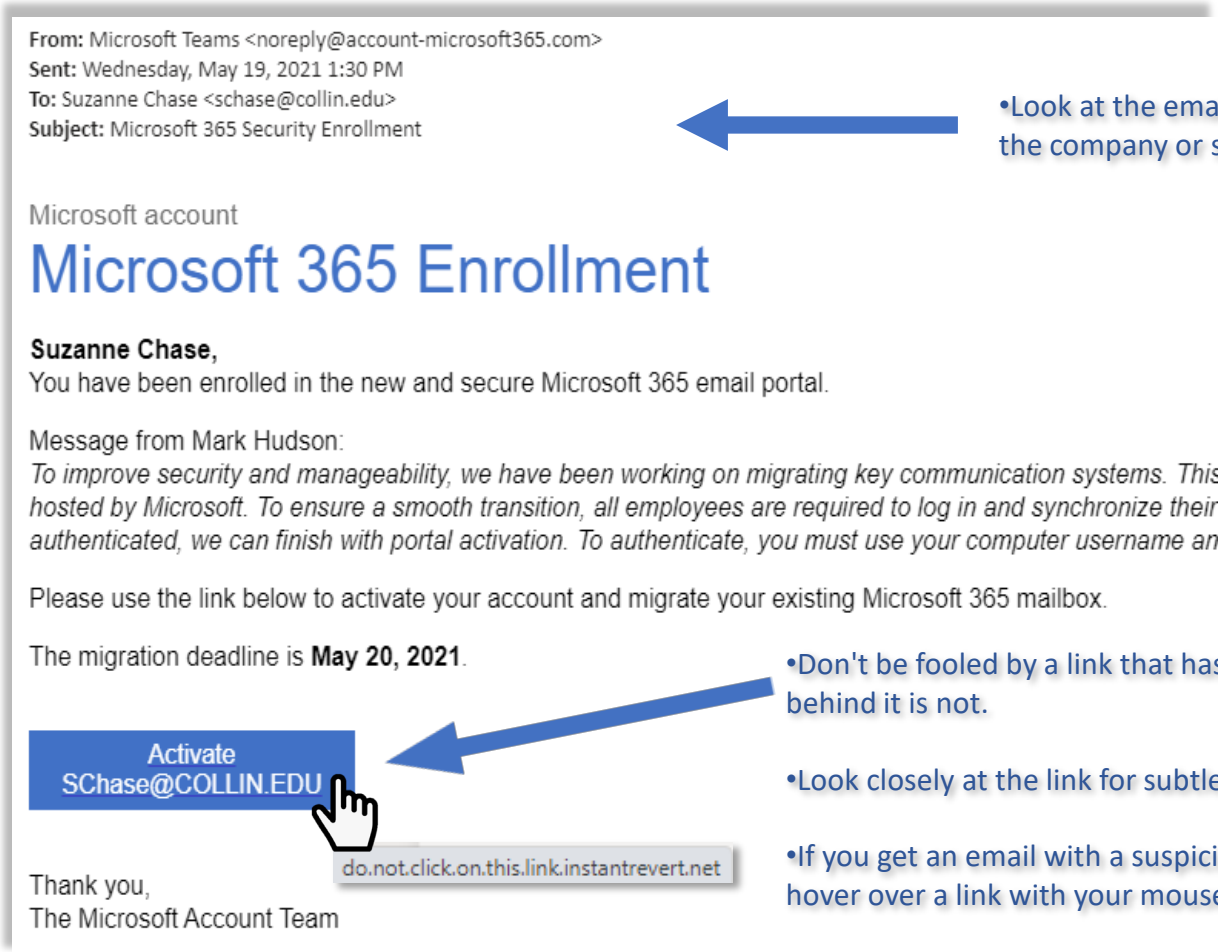
Identifying Phishing emails

Think before you click…



From: Microsoft Teams <noreply@account-microsoft365.com>
Sent: Wednesday, May 19, 2021 1:30 PM
To: Suzanne Chase <schase@collin.edu>
Subject: Microsoft 365 Security Enrollment

Microsoft account

Microsoft 365 Enrollment

Suzanne Chase,
You have been enrolled in the new and secure Microsoft 365 email portal.

Message from Mark Hudson:
To improve security and manageability, we have been working on migrating key communication systems. This hosted by Microsoft. To ensure a smooth transition, all employees are required to log in and synchronize their authenticated, we can finish with portal activation. To authenticate, you must use your computer username an

Please use the link below to activate your account and migrate your existing Microsoft 365 mailbox.

The migration deadline is **May 20, 2021**.

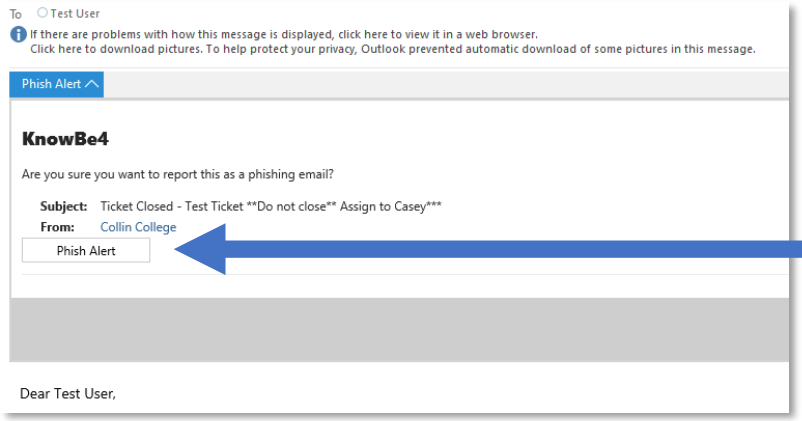
Activate
SChase@COLLIN.EDU

do.not.click.on.this.link.instantrevert.net

Thank you,
The Microsoft Account Team

- Look at the email address, not just the company or sender's name.
- Don't be fooled by a link that has text that is descriptive, but the link behind it is not.
- Look closely at the link for subtle misspellings in domain names
- If you get an email with a suspicious link, remember, you should first hover over a link with your mouse cursor to help verify its validity.
- If you are unsure, use the Phish Alert button **(see next steps on page 2)** and this will forward the email to the HelpDesk and create a ticket for investigation.

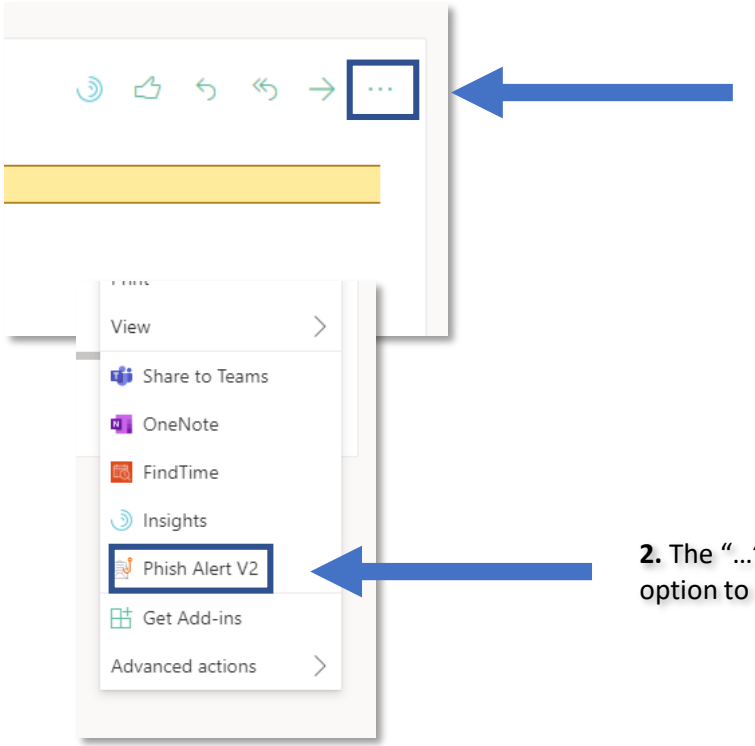
Mark Phishing emails using Outlook (Client)



1. There will be a "Phish Alert" menu option below the to: field on the email on your inbox

2. There will be a "Phish Alert" button

Mark Phishing emails using Outlook (Office365/www.office.com)



1. Next to the "reply", "Reply All" and "Forward" icons there is another menu "…"

2. The "…" menu will activate the option to use "Phish Alert"