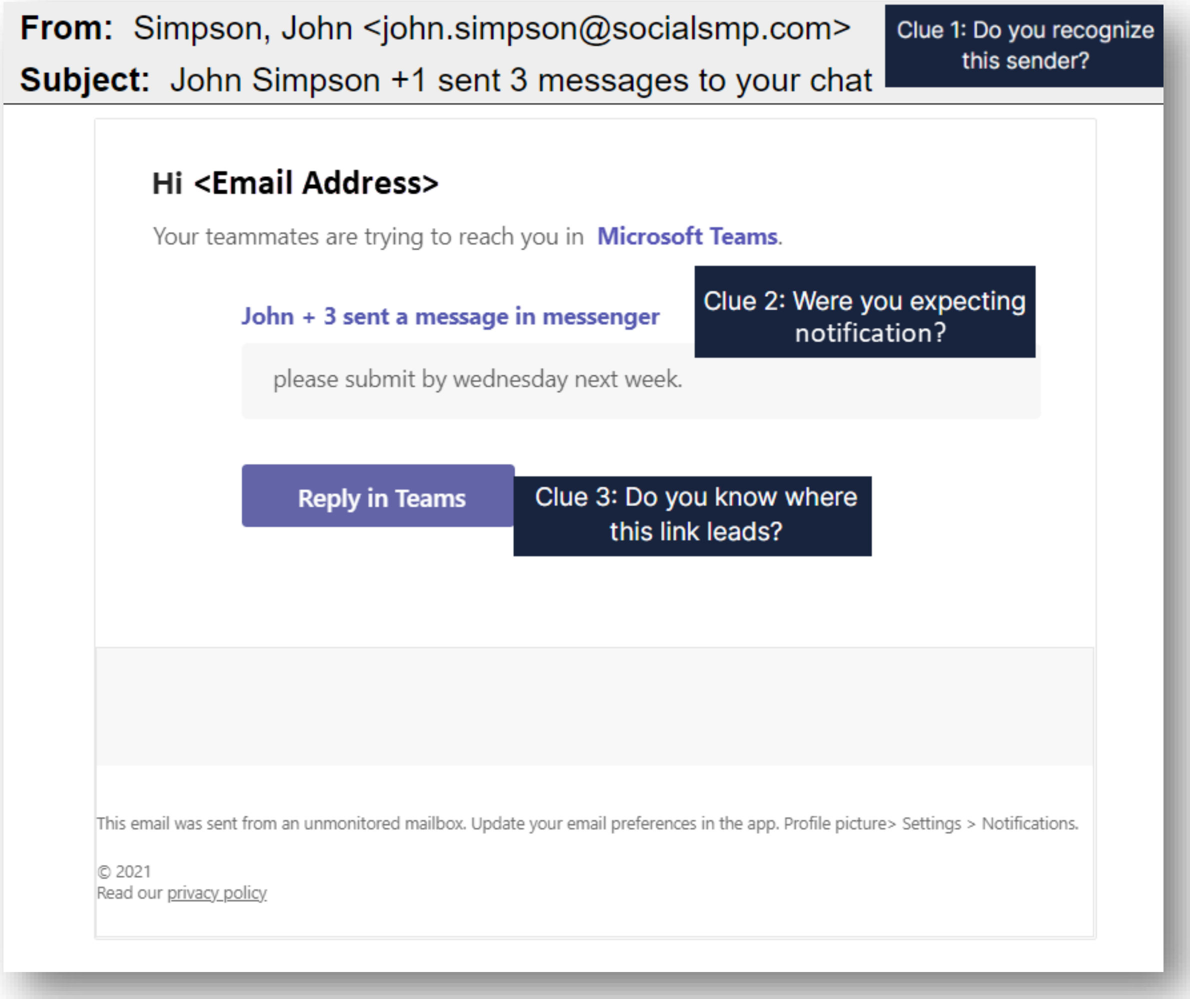
February 2021 Phishing scenario results: *Microsoft Teams Message*

The Office of Information Technology (OIT) completed a simulated phishing training exercise, which prompted you to click a link and sign in to review missed chat notifications. This email mimicked Microsoft Teams. Teams is Microsoft's collaboration tool, which has become a popular choice during our remote work status. It is also an attractive brand for attackers to impersonate. Legitimate Microsoft (MS) email notifications are plentiful and can be hard to distinguish between real or fake. When you are uncertain – do not click on the link! Open **your Teams instance** (or respective MS application) and check the chat and notifications within the application.

773 employees reported the phishing scenario to the Phishtrap! Reporting is the preferred action as it provides IT Security the email threat intel it needs to respond.

281 employees clicked the link within the training email; of these individuals, 76 entered their credentials. There were several clues within the email to help you identify this message as suspicious. Please review the email again and pay close attention to the red flags:



From: Simpson, John <john.simpson@socialsmp.com>

Subject: John Simpson +1 sent 3 messages to your chat

Clue 1: Do you recognize this sender?

Hi <Email Address>

Your teammates are trying to reach you in **Microsoft Teams**.

John + 3 sent a message in messenger

Clue 2: Were you expecting notification?

please submit by wednesday next week.

Clue 3: Do you know where this link leads?

This email was sent from an unmonitored mailbox. Update your email preferences in the app. Profile picture> Settings > Notifications.

© 2021
Read our privacy policy

What should you do if you suspect an email may be a phishing attempt?

Let IT Security analyze the email for you - **REPORT** the email! Educated employees are our last line of defense to thwart phishing attacks and help us prevent data breaches. The Report Phishing button within your email client allows you to quickly report suspicious emails to IT Security. Learn how to access the Phishing Reporter button when using Office 365 at home. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Complete (or revisit) DataSecurity@MC: Annual Review!

DataSecurity@MC: Annual Review training provided by SANS will teach you how to better identify common methods used by cyber attackers who try to gain access to account credentials and information systems. The range of training topics takes about 35 minutes to complete and can be accessed in MC Learns through Workday under the **MC Required Training** category

Below are some common clues to look for in identifying a suspicious email:

- Be wary of emails from unknown senders. PERIOD.
- Treat the Teams email notification as just a nudge to get you to check your Teams application instead of clicking on the link.
- Carefully review the sending email domain – it should read noreply@email.teams.microsoft.com
- Check your emotions. Do not be curious and investigate the link – REPORT the email.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, shipping notices, and stimulus check scams.
- Trust your instincts**.** If the email content, sender, and link or email attachment seems suspicious, do not open it. Play it safe and REPORT it.
- Visit IT Security's Phishing Alerts web page to view the latest threats – this month's feature is on Stimulus Phishing Scams.

If you have any questions or concerns regarding this process, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology