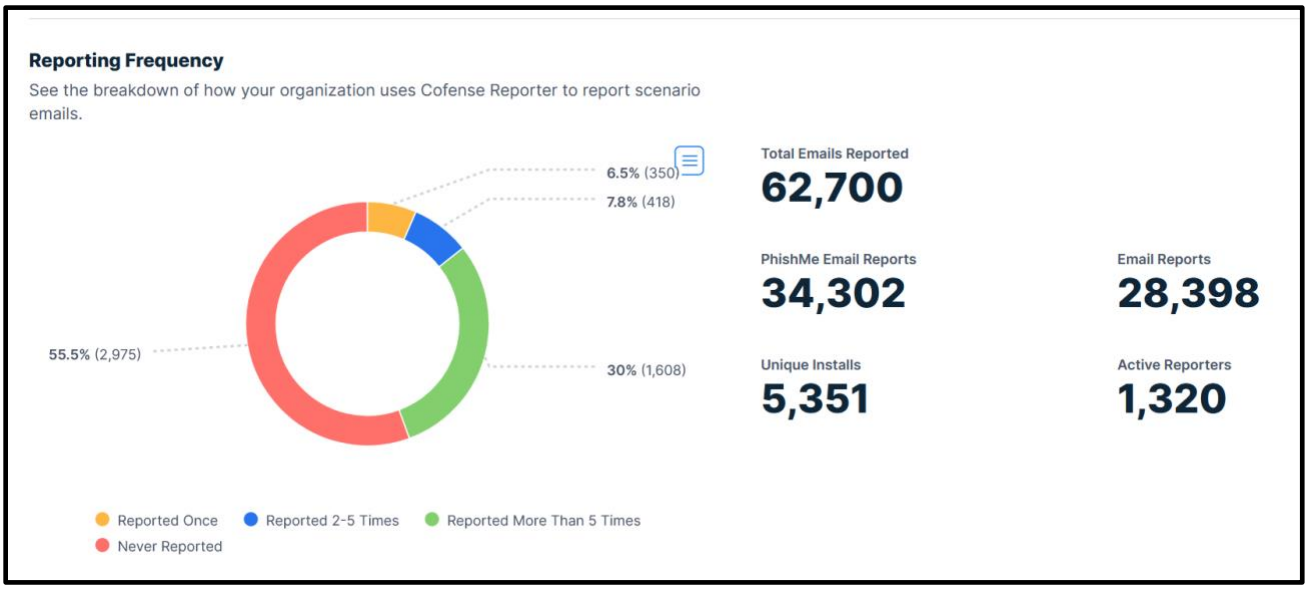
May 2021 Phishing Results: Microsoft Impersonation

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Digest Summary 05/11/2021.* This scenario used a common trick - Microsoft (MS) brand name impersonation. For a successful credential harvest, that captures usernames and passwords, attackers design the login page as an Office 365 look-alike to gain your trust. Do not be fooled!

We Need a Reporting Boost!

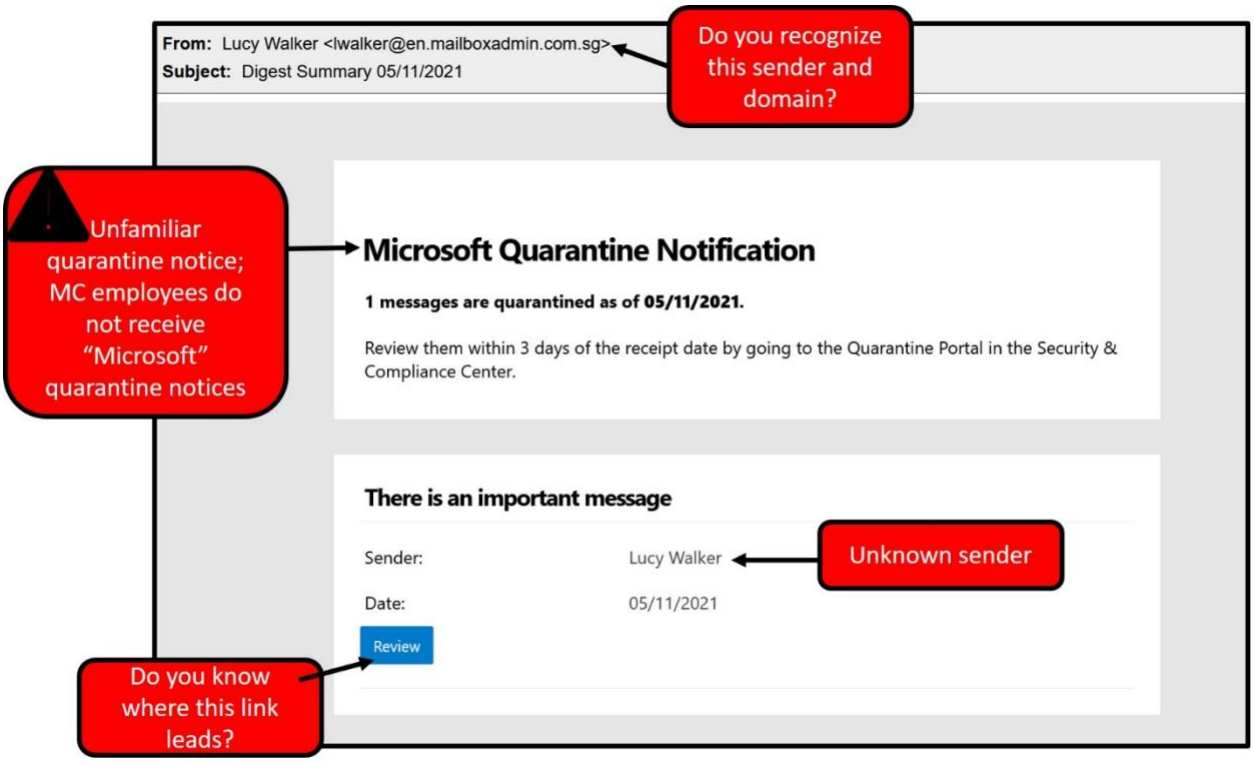
Over 55% of our employees have <u>never</u> reported a phishing scenario. The statistics show we need to do better:



In this latest scenario:

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

109 employees clicked the link within the training email; of these individuals, 9 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:



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! 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:

- Montgomery College quarantine summary emails are delivered through our email filter vendor Proofpoint, not Microsoft. The sending address is: MCSpamFilter@montgomerycollege.edu

- No username or password is required to manage your MC Proofpoint account via the daily quarantine summary email.
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- 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 scams, 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.

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