Subject: October Phishing Results – **We Can Do Better!**

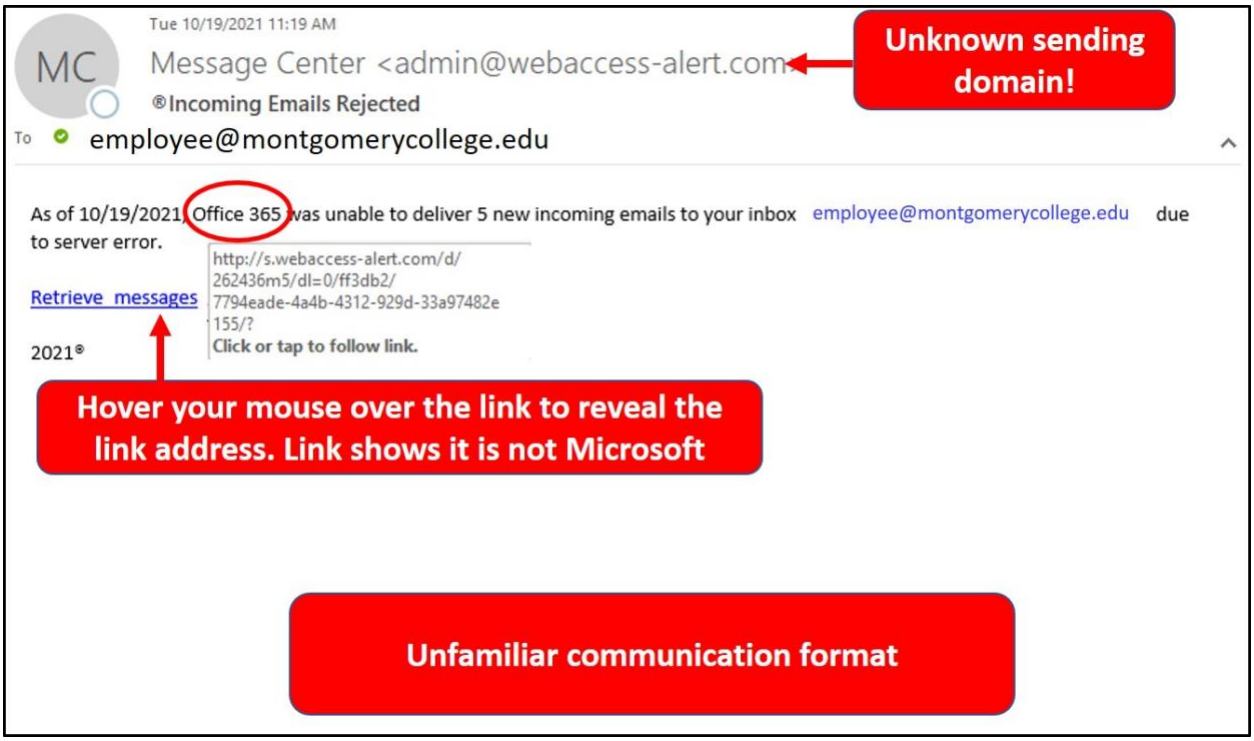
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Incoming Emails Rejected*, with a link to "Retrieve messages". This type of phish is designed to look like a typical Office 365 notification. This scenario should look familiar as it is a repeat from October 2020. The statistics show we need to do better:

	Number of employees who reported	Number of clicks on the malicious link
October 2020	**717**	**682**
October 2021	**744**	**560**

The numbers only slightly improved this year, with 27 more employees reporting the phish, and 122 fewer clicks on the malicious link. As a reminder the IT security awareness program is designed to educate employees on how to spot and report suspicious emails. Keep in mind:

- Reporting is the preferred action as it provides IT Security the threat intel it needs to respond.
- Clicking on links in a real phishing email have consequences, such as, providing the attacker:
  - Access to your MyMC account
  - Allow the attacker to steal sensitive College data
  - Introduce ransomware to your workstation and other key systems
  - Cause disruption in College business

If you were one of the clickers, **and you know who you are**, please review the red flags within this type of phishing attack:



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 Outlook allows you to quickly report suspicious emails to IT Security.

If using Office 365 on the web, follow these steps to pin the Reporter Button to your email message surface. 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:

- Mismatched email domains - In this scenario the email notice identifies Office 365, a Microsoft product, yet the sending domain is *admin@ webaccess-alert.com*

- Unfamiliar MC communication notice – Stay alert to unusual College communication formats and sending domains.
  Approved senders are:
  - ✓ Montgomerycollege.edu (email address)
  - ✓ Mcemail.org (mass MC communications)
  - ✓ Msgs@myservice.io (MC voicemail notice)
  - ✓ MCSpamFilter@montgomerycollege (daily email quarantine summary)

- 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.
- 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