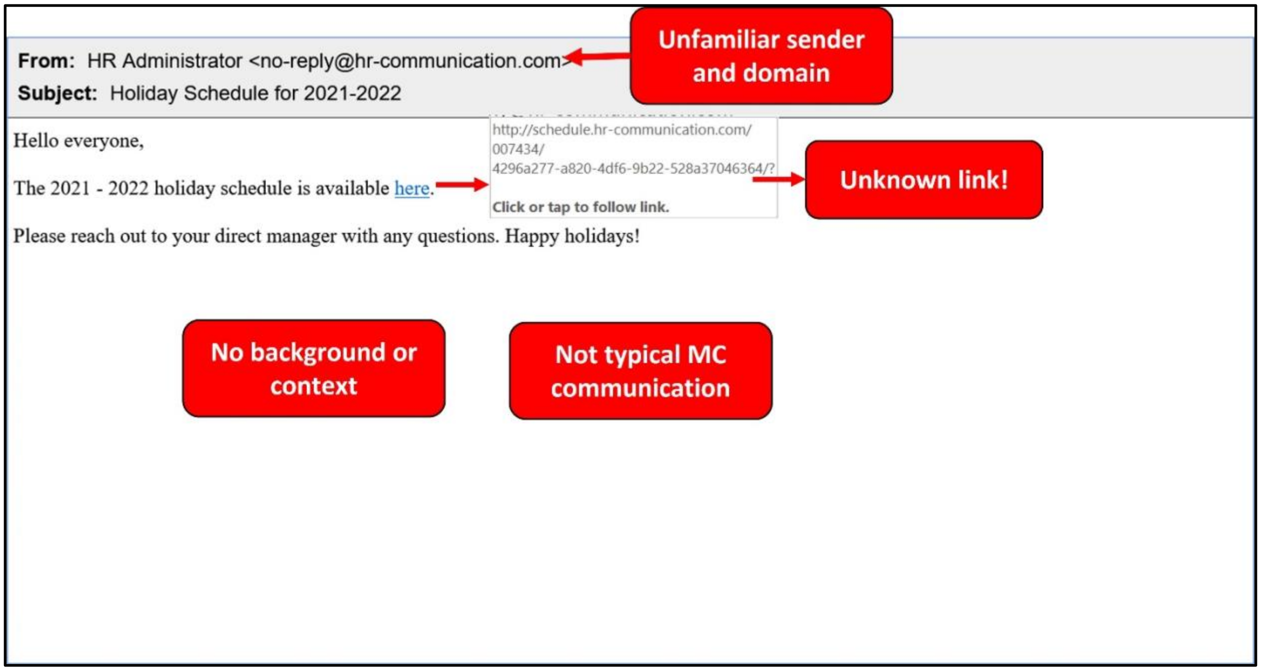
December Phishing Results: Holiday Schedule

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Holiday Schedule for 2021-2022*, with a link to view the *holiday schedule*. Phishing attackers use malicious links or attachments to solicit personal information and login credentials by posing as a trustworthy organization. One phishing tactic used to lower your suspicion is to imply it comes from a trusted sender. In this case the sending address is: "HR Administrator <no-reply@hr-communication.com>."

506 employees reported the phishing scenario to the Phishtrap.

611 employees clicked the link within the training email.

We need to do better! **The number of employees reporting the scenario should be higher than the number of employees clicking on the link**. Please review the scenario and clues:



From: HR Administrator <no-reply@hr-communication.com>
Subject: Holiday Schedule for 2021-2022

Hello everyone,

The 2021 - 2022 holiday schedule is available here.

http://schedule.hr-communication.com/
007434/
4296a277-a820-4df6-9b22-528a37046364/?
Click or tap to follow link.

Please reach out to your direct manager with any questions. Happy holidays!

Unfamiliar sender and domain

Unknown link!

No background or context

Not typical MC communication

Report Phishing MC

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:

- Familiarize yourself with MC's communication media and email sending addresses:
  - Human Resources and Strategic Talent Management Reply@mcemail.org – Employee Matters Office of Human Resources and Strategic Talent Management newsletter
  - MCCommunications@montgomerycollege.edu – all employee College announcements/information
  - PublicSafety@montgomerycollege.edu - announcements from Office of Public Safety and Emergency Management
  - Workday@montgomerycollege.edu – Workday, MC's system of record for human resources and finance, communications.

- Only use your Montgomery College email address for College business. This helps you organize your known contacts and distinguish between personal and business email sending addresses.

- 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.

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