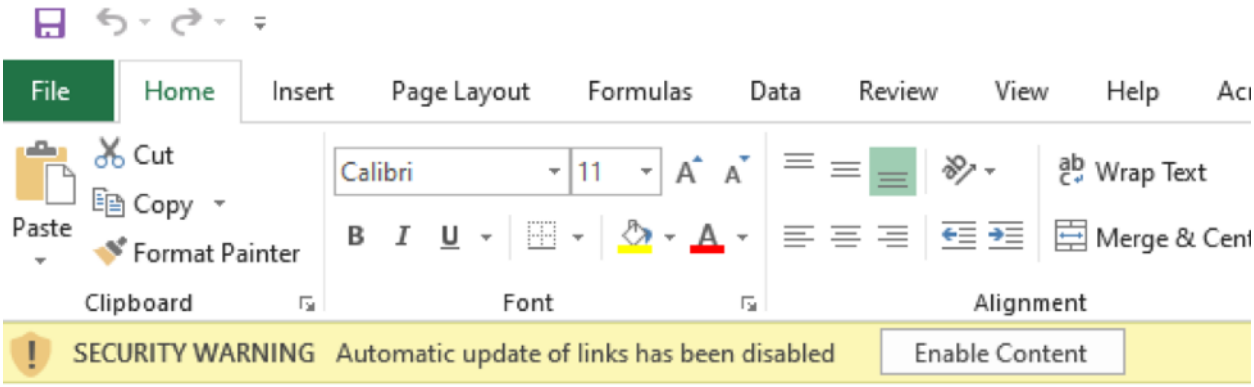
Subject: Widespread Phishing Attacks
Date: February 2022

On February 1, you received a message from the IT Urgent mailbox alerting you to a widespread phishing attack targeting Montgomery College employees. This has been a sustained malicious campaign, continuing even today. This particular attack includes a message with an Excel spreadsheet attachment, though any attachment could include malware, particularly Microsoft Excel, Word, or PowerPoint, where the user may be prompted to “Enable Content” as shown in the example below.



IT Security has leveraged its defensive capabilities and has largely prevented the malicious emails from getting to your inboxes. However, this attacker continues to change tactics, and while IT Security is working hard to catch every message, some may slip through and reach users.

Attackers are constantly looking for ways to capture our online information. We urge all employees to stay vigilant and watch out for fraudulent emails, phone calls, and text messages.

Let IT Security analyze any suspicious 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.

Common clues to look out for:

- 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.
- 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.

- Be cautious. Malicious actors and aggressive spammers are preying on our stress levels and hoping our guard is down with COVID-19, gift cards, meeting invites, shipping notices, and stimulus check scams.
- Keep your passwords private. No reputable company will ask for your password over email. If you entered your credentials into a fraudulent website, change it immediately and notify your security team.

If you have any questions or concerns, 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