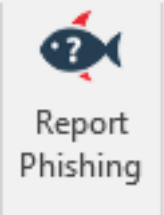
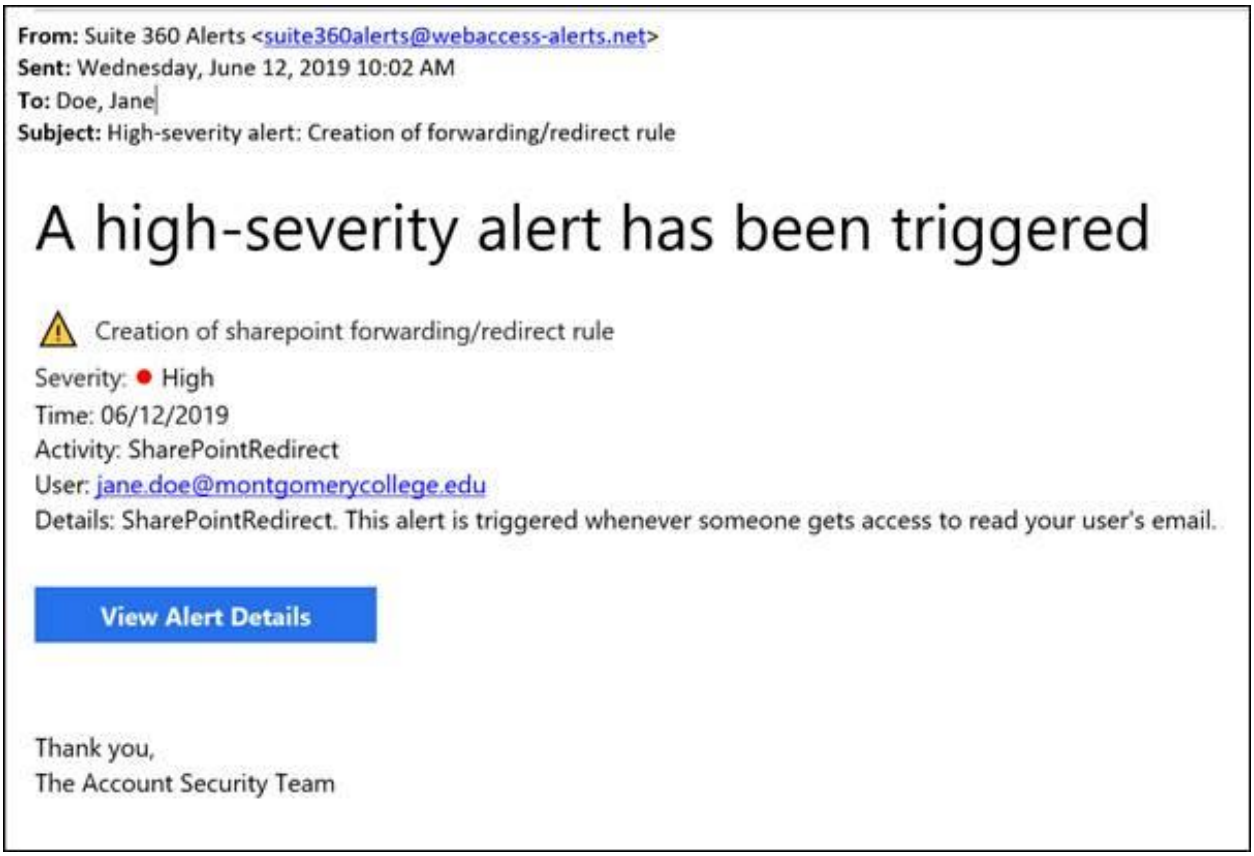
June 2019 Phishing Exercise Recap: High-Severity Alert
July 17, 2019



The Office of Information Technology's (OIT) June 2019 phishing scenario invoked fear upon the recipient to "see if someone has access to read the user's email." This email used fear tactics by using phrases such as "high-severity alert" to get employees to click on the "View Alert Details" button in the email. A close examination of the email shows an unknown sending domain and email address. Over 761 employees reported this phishing email to the PhishTrap and 413 employees clicked on the link.



From: Suite 360 Alerts <suite360alerts@webaccess-alerts.net>
Sent: Wednesday, June 12, 2019 10:02 AM
To: Doe, Jane
Subject: High-severity alert: Creation of forwarding/redirect rule

A high-severity alert has been triggered

Creation of sharepoint forwarding/redirect rule
Severity: High
Time: 06/12/2019
Activity: SharePointRedirect
User: jane.doe@montgomerycollege.edu
Details: SharePointRedirect. This alert is triggered whenever someone gets access to read your user's email.

View Alert Details

Thank you,
The Account Security Team

The goal of a fear-based email threat is to get employees to act without verifying. Clicking on unknown links and giving up your user name and password provides an attacker the key (password) to log in to your Office 365 email AND your MyMC account. To avoid falling victim to phishing emails, OIT recommends all employees:

- **Enroll in Two-Factor Authentication (2FA)**
  All staff and faculty must enroll in 2FA by September 30, 2019. 2FA is an added layer of security that requires log on authentication using the first factor, your user name and password, and the second factor, your mobile phone, tablet, or landline to easily confirm

your login requests. To learn more about 2FA, please visit https://mcblogs.montgomerycollege.edu/itprojects/2fa.

- **Report** all suspicious emails to the Phishtrap for analysis using the Report Phishing tool located on the Microsoft Outlook toolbar or in the Outlook mobile app for iPhone and Android. IT Security will analyze the content and web links and if legitimate, will send the email back to you.
- **Review and assess before clicking on the links.** Do not click on the links in an email. If you have a business relationship with the sender or an account (MyMC, O365, Amazon.com, your bank, etc.), log in to the account by using the known web address for the account, i.e. montgomerycollege.edu – Access MyMC.

OIT encourages all employees who need assistance in spotting a phishing email to take the Cybersecurity e-courses within MC Learns. The e-courses are short videos that provide employees with the skills needed to detect malicious emails.