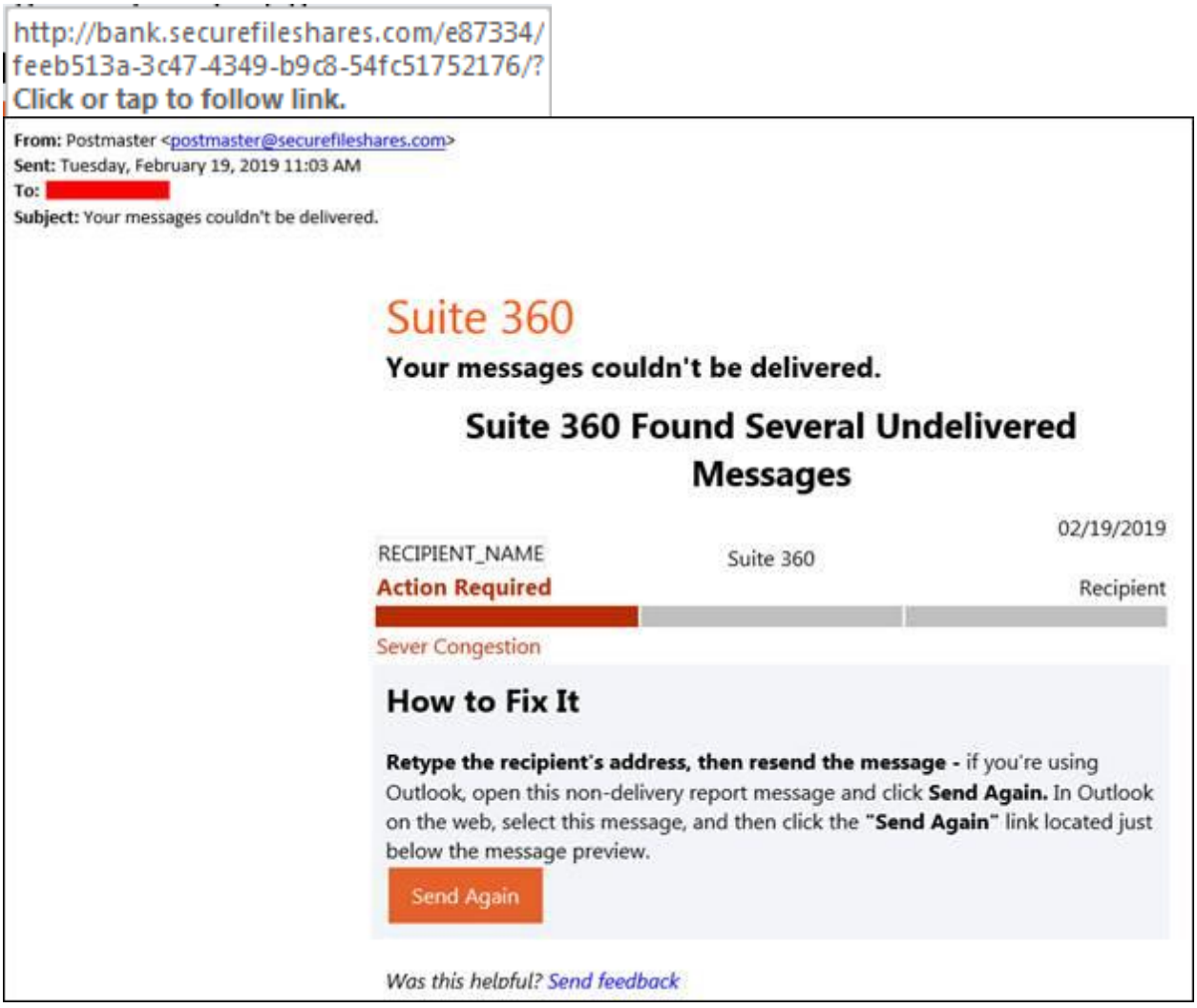
February 2019 Phishing Exercise Recap: Undelivered Messages
March 12, 2019

The Office of Information Technology's (OIT) February 2019 phishing scenario featured an Office 365 imitation email notification of "Undelivered Messages". A close examination of the email shows the fake "Suite 360" term, which resembles the real Office 365 (O365) brand name. Over 616 employees reported this look-alike phishing email to the PhishTrap. As a typical credential harvesting attack, this email baits the recipient into clicking on the link and requests the user to enter their login user name and password. In this scenario, 134 employees clicked on the link, and 23 submitted their MyMC user name and password.



Giving up your user name and password in a credential harvesting phishing email provides an attacker the key (password) to log in to your O365 email AND your MyMC account. To avoid falling victim to credential harvesting and general phishing emails, OIT recommends all employees:

- **Enroll in Two-Factor Authentication (2FA)** to protect your Office 365 account. 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.