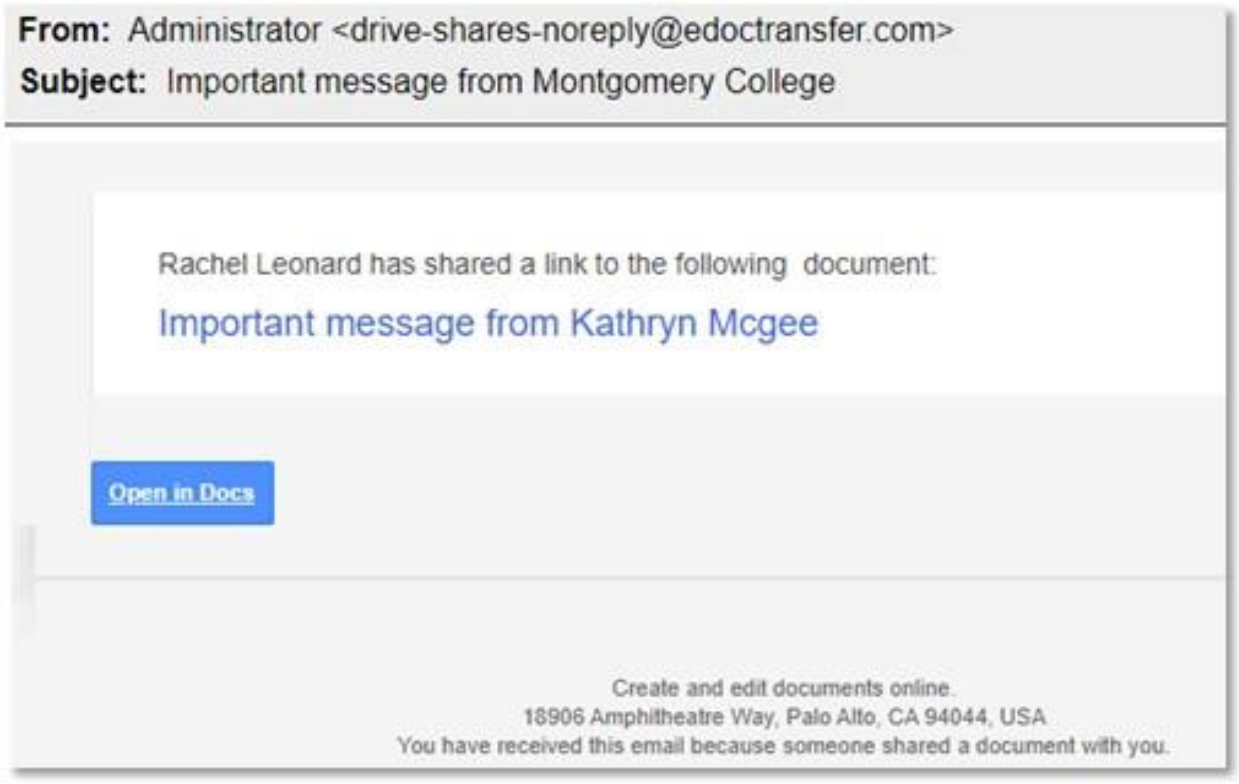
September 2019 Phishing Exercise Recap: Google Docs
September 30, 2019

The Office of Information Technology's (OIT) September 2019 phishing scenario mirrored Google docs, a shared document email. This is a common exploit used to entice the recipient to enter credentials and view the document. The subject in the email, "Important message from Montgomery College" provided a link labeled, "Open in Docs", implying the link and subsequent attachment is trustworthy because Google docs is a trusted cloud-sharing medium. Over 584 employees reported this phishing email to the PhishTrap, **160 employees clicked on the link and submitted their MyMC or personal account credentials; 373 employees clicked on the link and did not submit credentials.**



Cloud applications such as Google Docs, Dropbox, and OneDrive are often trusted by users and criminals count on that. Those criminals are exploiting these services by creating fake secure login links to harvest employee credentials. Phishing emails that make use of a trusted service rely on you to trust the entire process, i.e. trust Google Docs means to trust the sender and the link or attachment. **DO NOT FALL FOR IT!**

To avoid falling victim to this false sense of trust and other phishing emails, OIT recommends all employees:

- **Review and assess before clicking on the links**

- Check the sending email address and name(s) of the person sharing the document. If you do not know the sender or expect an email with a “shared link”, do not click on the link.
  - *Kathryn Mcgee* and *Rachel Leonard* are fictitious names
- Check the sending email domain. Google the domain to see if it is a legitimate entity.
  - *@edoctranser.com* is a fictitious domain
- If you are setting up communication with a sender and using one of the collaborative document sharing services, discuss ahead of time the exact subject, sending email address and domain, and which platform will be used.
- If you are unable to verify, call the sender on the phone to verify the email. Do not email the sender back and ask for verification!

- **Enroll in Two-Factor Authentication (2FA)**
  All employees 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 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.

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.