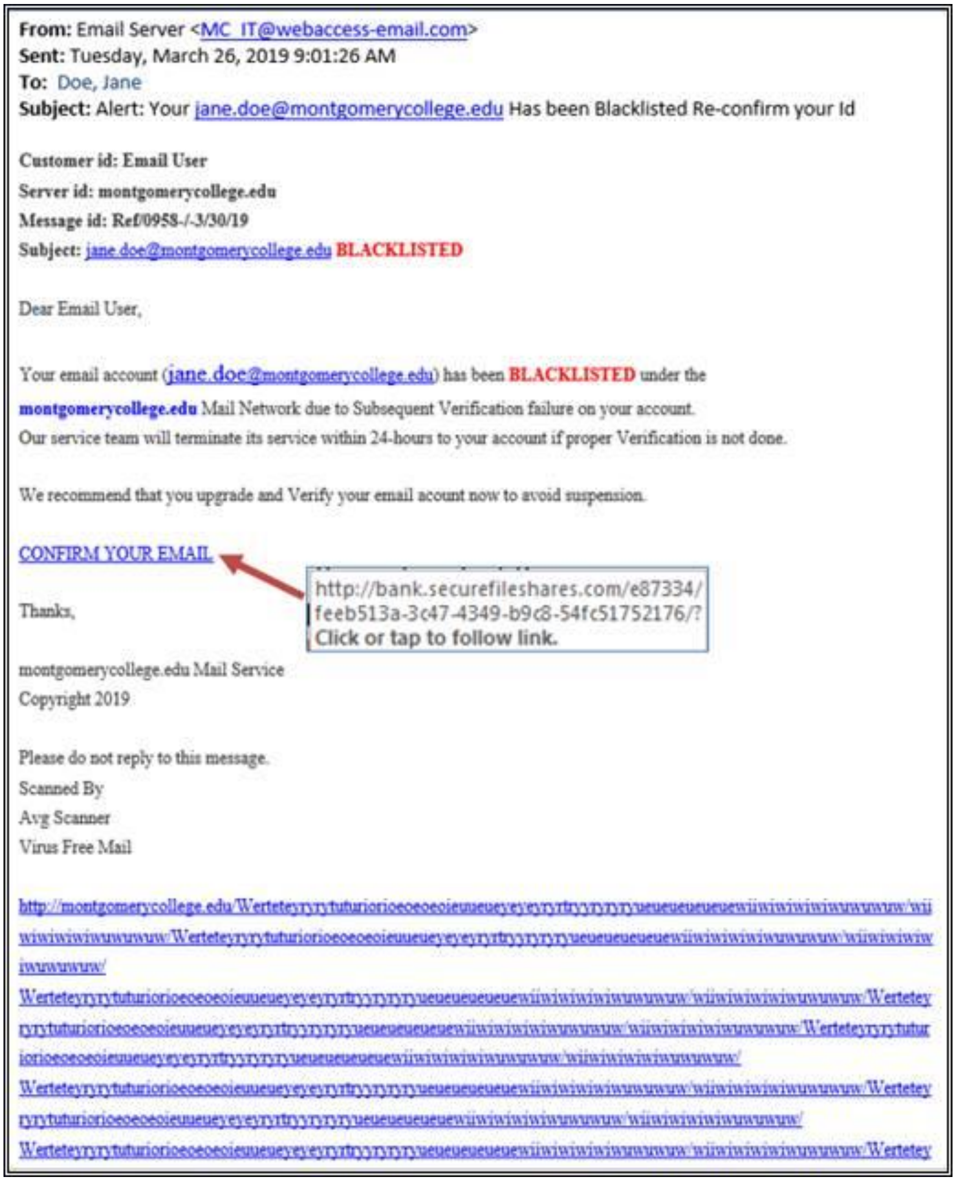
March 2019 Phishing Exercise Recap: Re-confirm ID
April 10, 2019

The Office of Information Technology's (OIT) March 2019 phishing scenario invoked a sense of urgency upon the recipient to "Re-confirm" their ID. This urgency tactic is a common emotional ploy used to get employees to act quickly – and to not pay attention to the details in the email. A close examination of the email shows a non-affiliated Montgomery College sender email address (@webaccess-email.com) and a link that leads to a non-Montgomery College web address (http://bank.securefileshares.com...). Over 1,030 employees reported this phishing email to the PhishTrap, and 225 employees clicked on the link.



From: Email Server <MC_IT@webaccess-email.com>
Sent: Tuesday, March 26, 2019 9:01:26 AM
To: Doe, Jane
Subject: Alert: Your jane.doe@montgomerycollege.edu Has been Blacklisted Re-confirm your Id

Customer id: Email User
Server id: montgomerycollege.edu
Message id: Ref/0958-/-3/30/19
Subject: jane.doe@montgomerycollege.edu **BLACKLISTED**

Dear Email User,

Your email account (jane.doe@montgomerycollege.edu) has been **BLACKLISTED** under the **montgomerycollege.edu** Mail Network due to Subsequent Verification failure on your account.
Our service team will terminate its service within 24-hours to your account if proper Verification is not done.

We recommend that you upgrade and Verify your email acount now to avoid suspension.

CONFIRM YOUR EMAIL

http://bank.securefileshares.com/e87334/feeb513a-3c47-4349-b9c8-54fc51752176/?
Click or tap to follow link.

Thanks,

montgomerycollege.edu Mail Service
Copyright 2019

Please do not reply to this message.
Scanned By
Avg Scanner
Virus Free Mail

http://montgomerycollege.edu/Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/
Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/
Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/
Werteteyryrytuturiorioeoeoeoieuueueyeyeyryrtryyryryryueueueueueuewiiwiwiwiwiwuwuwuw/wiiwiwiwiwiwuwuwuw/Wertetey

The goal of "account confirmation" email threats is to capture your account credentials. Clicking on unknown links and 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.