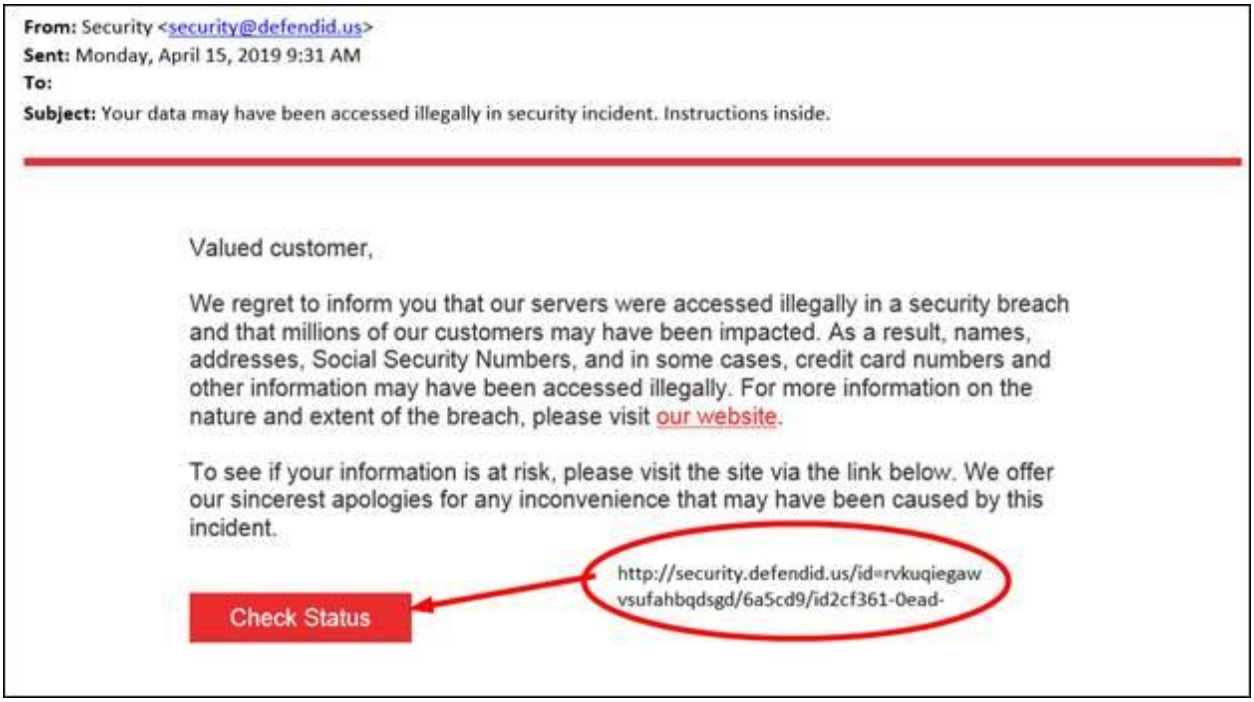
April 2019 Phishing Exercise Recap: Information at Risk
May 6, 2019

The Office of Information Technology's (OIT) April 2019 phishing scenario invoked a sense of fear upon the recipient to "see if your information is at risk" on an unnamed account from an unknown vendor. This email used fear tactics by using phrases such as "security breach" and "your information is at risk" to get employees to click on the link and to not pay attention to the details in the email. A close examination of the email shows an unknown, fictitious sender and no information on the account entity that suffered the breach. Over 1,013 employees reported this phishing email to the PhishTrap and 225 employees clicked on the link. The link led to a fictitious credential harvesting webpage where 72 employees entered their MyMC credentials.



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 credential harvesting and general phishing emails, OIT recommends all employees:

- **Enroll in Two-Factor Authentication (2FA)**
  All staff and faculty must enroll in 2FA according to the following schedule:

  June 30, 2019 – Staff enrollment
  September 30, 2019 – Faculty enrollment
  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.