July 2020 Phishing Exercise Recap: Brand Impersonation Tactics
July 21, 2020

The Office of Information Technology's (OIT) July phishing awareness exercise focused on brand impersonation tactics used in phishing emails. This phishing scenario resembled Skype with a lure of "pending Skype notifications..." The link led to a log in prompt with the expectation of capturing your login credentials.

920 employees reported the phishing scenario email: *Notification for Jane.Doe@montgomerycollege.edu on 07/01/2020*. Thanks to these employees, IT Security would have the time advantage it needs to respond to potential threats.

73 employees clicked the link AND entered their MyMC credentials within the training email. There were several clues within the email to help you identify this "Skype notification" as suspicious. Please review the email again and pay close attention to the red flags:

What should you do if you suspect an email may be a phishing attempt?

Educated employees are our last line of defense to thwart phishing attacks and help us prevent data breaches. The Report Phishing button within your email client allows you to quickly report suspicious emails to IT Security. Learn how to access the Phishing Reporter button when using Office 365 at home.If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Complete (or revisit) the DataSecurity@MC training!

Data Security@MC training provided by SANS will teach you how to better identify common methods used by cyber attackers who try to gain access to account credentials and information systems. This training will also provide tips and techniques to help detect and defend against these threats. The range of training topics takes about 35 minutes to complete and can be accessed through MC Learns. Below are some common clues to look for in identifying a suspicious email:

- Remote work has increased our usage of online conference technologies. When communicating with outside parties about meetings ask in advance what conference technology platform they use and who will be sending the invite.
- Familiarize yourself with MC's conferencing tool, Zoom, and the recommended security precautions detail here.
- Check your emotions. Beware of emotional triggers such as an urgent deadline for completion or severe consequences if the request is not complete -i.e. follow MC processes and procedures.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, and stimulus check scams.
- Trust your instincts**.** If the email content, sender, and link or email attachment seems suspicious, do not open it. Play it safe and REPORT it.
- The email has no identifying characteristics, such as corporate branding, valid contact information, or known sender information.
- The message is overly generic, the request is outside of your scope of responsibility, and/or the action requested is not typical of a current business process.