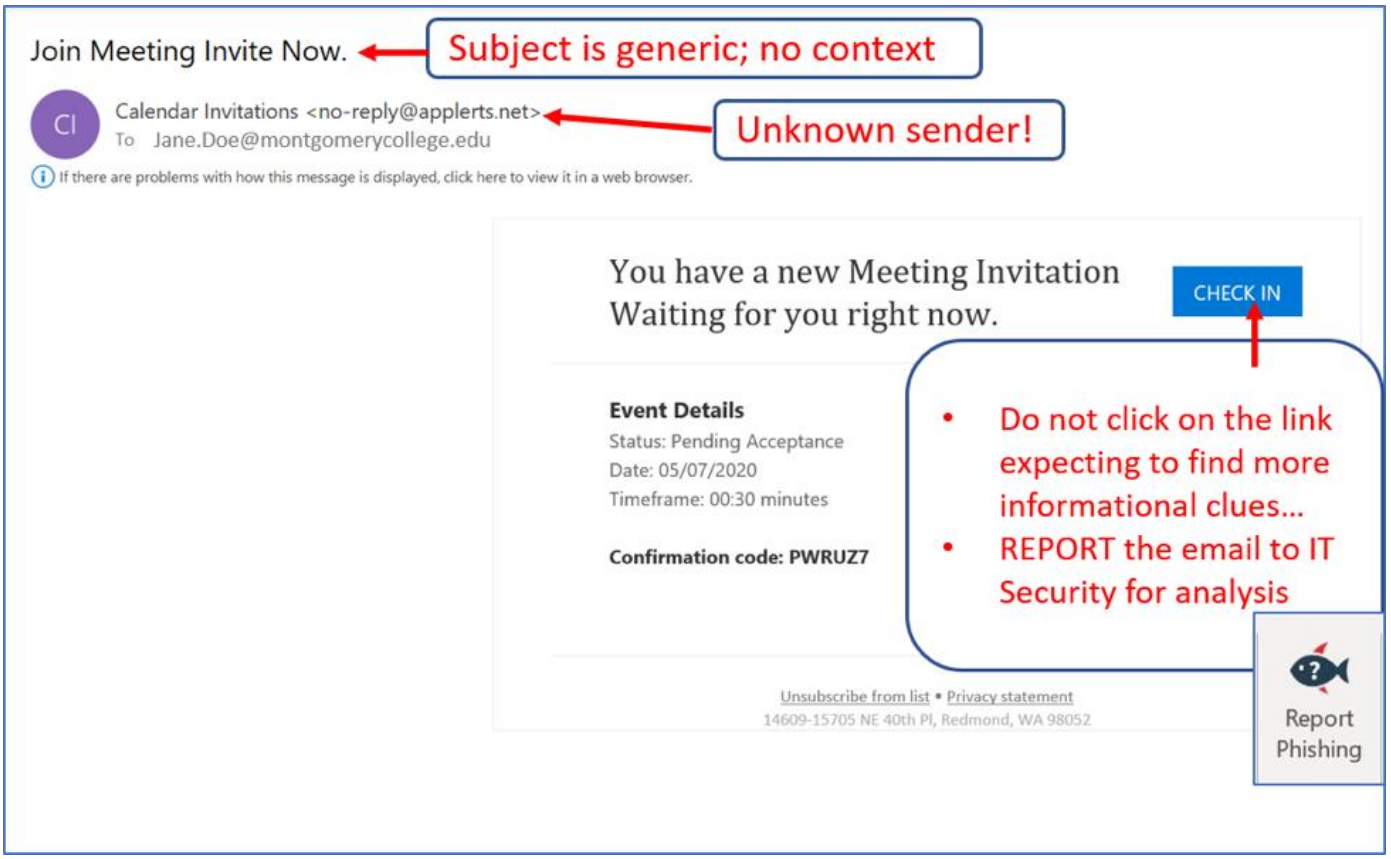
May 2020 Phishing Exercise Recap: Meeting Invitation
May 28, 2020

The Office of Information Technology (OIT) completed a phishing training exercise that mirrored a current threat in the form of a calendar meeting invite. Cybercriminals are modifying phishing campaigns using COVID-19 fear tactics to lure victims in with bogus meeting invites. The invites may have no subject or context, but may also include words such as, “termination”, or “All hands meeting with HR”. Unemployment rates have skyrocketed due to the COVID-19 pandemic and these topics coincide with the fear many families are feeling or experiencing. These meeting invites, like other phishing emails, provide a link requesting your login credentials. Upon entering your credentials your account is compromised and provides unlimited access to your email contents as well as MyMC account information to an attacker.

620 employees reported the “Join Meeting Invite Now” phishing scenario email. Thanks to these employees, IT Security would have the time advantage it needs to respond to potential threats.

323 employees clicked the link within the training email. There were several clues within the email to help you identify this invite 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 the Data Security@MC training by June 30

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:

- Check your emotions. The email includes an urgent deadline for completion or a severe consequence if the request is not complete - i.e. follow MC processes and procedures.
- The email uses strong emotional messaging. 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, don't 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.