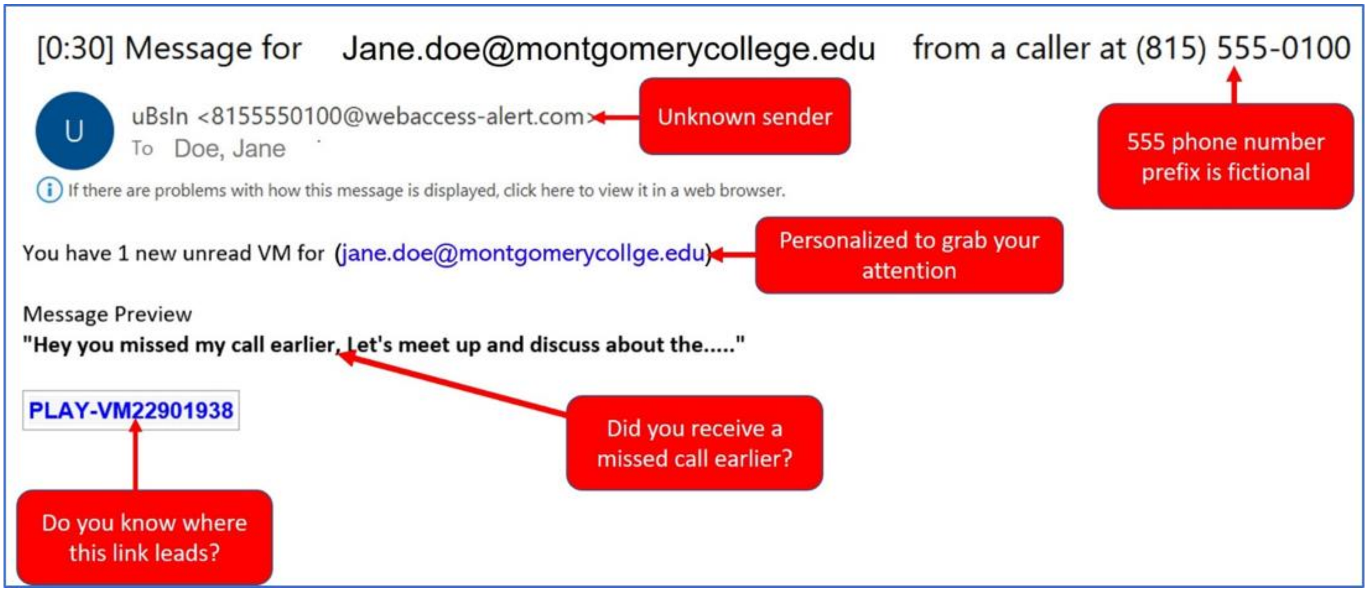
June 2020 Phishing Exercise Recap: New Voice Message
June 22, 2020

The Office of Information Technology's (OIT) June phishing training exercise demonstrated a common credential harvesting tactic in the form of a voicemail notification email. In order to listen to the voicemail, the user is directed to click on the link. The link leads to a fake webpage, most often mimicking the Office 365 login, which prompts the user to enter their credentials. Upon entering credentials, the user's account is compromised and provides unlimited access to email contents, as well as MyMC account information, to an attacker.

829 employees reported the phishing scenario email: *[0:30] Message for Jane.Doe@montgomerycollege.edu from caller at (815) 555-0100*. Thanks to these employees, IT Security would have the time advantage it needs to respond to potential threats.

393 employees clicked the link within the training email. There were several clues within the email to help you identify this voicemail notification as suspicious. Please review the email again and pay close attention to the red flags:



[0:30] Message for Jane.doe@montgomerycollege.edu from a caller at (815) 555-0100

uBsln <8155550100@webaccess-alert.com>
To Doe, Jane

If there are problems with how this message is displayed, click here to view it in a web browser.

You have 1 new unread VM for (jane.doe@montgomerycollge.edu)

Message Preview
"Hey you missed my call earlier, Let's meet up and discuss about the....."

PLAY-VM22901938

Unknown sender

555 phone number prefix is fictional

Personalized to grab your attention

Did you receive a missed call earlier?

Do you know where this link leads?

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:

- MC's voicemail notification emails DO NOT require a username or password to listen to the audio attachment.
- 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.