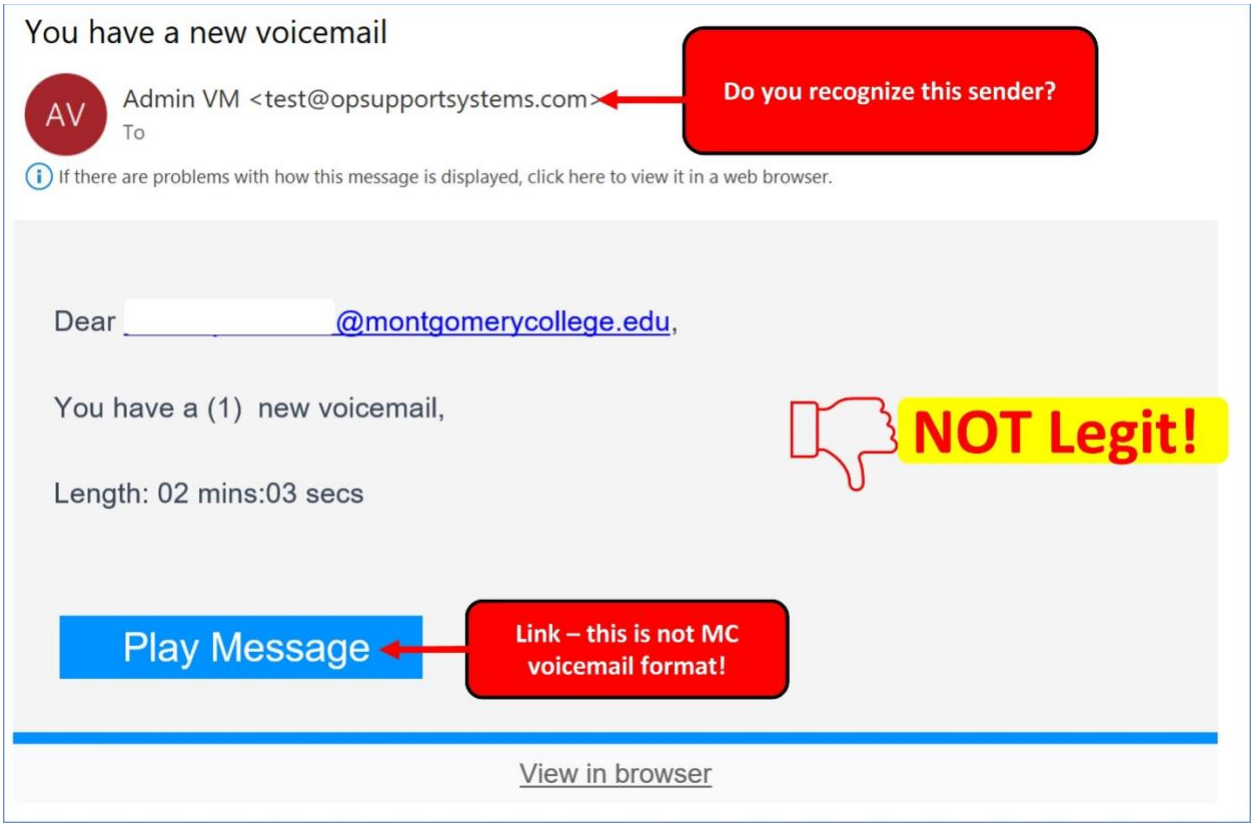
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *You have a new voicemail*, with a link to "Play Message". Voicemail phishing emails are most often used to capture employee login credentials. This phishing type will spoof legitimate brands to look like typical office communications you may receive. They imply a sense of urgency, refer to your job duties, and prey on your emotions of curiosity and fear.

602 employees reported the phishing scenario to the Phishtrap! Reporting is the preferred action as it provides IT Security the threat intel it needs to respond.

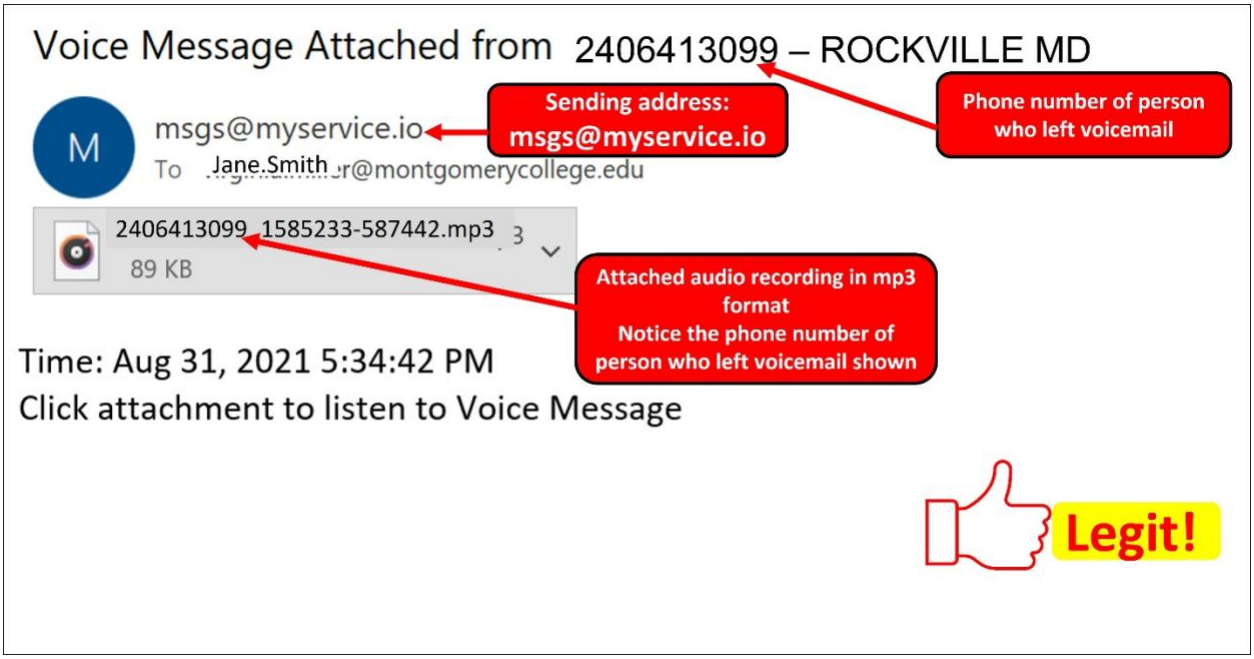
870 employees clicked the link within the training email.

Please review the differences between a phishing voice message email and the legitimate MC voice message email.

Phishing Voicemail example:



Legitimate Voicemail sample from MC phone system:



1. MC's voice messaging service will send an email with the included audio file of the voicemail left on your College phone. The Sending address is: msgs@myservice.io
2. The subject line in the MC voice messaging service email will include the phone number of the person leaving a voicemail
3. The MC voice messaging service provides the voicemail as an attachment in mp3 format
4. NO login credentials are required to listen to the voicemail!

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

Let IT Security analyze the email for you - **REPORT** the email! The Report Phishing button within Outlook allows you to quickly report suspicious emails to IT Security.

If using Office 365 on the web, follow these steps to pin the Reporter Button to your email message surface. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Complete (or revisit) DataSecurity@MC: Annual Review!

DataSecurity@MC: Annual Review 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. The range of training topics takes about 35 minutes to

complete and can be accessed in MC Learns through Workday under the **MC Required Training** category.

Below are some common clues to look for in identifying a suspicious email:

- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- Check your emotions. Do not be curious and investigate the link – **REPORT** the email.
- 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, shipping notices, 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.

If you don't catch the phish, the phish will catch you.

If you have any questions or concerns regarding this process, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology