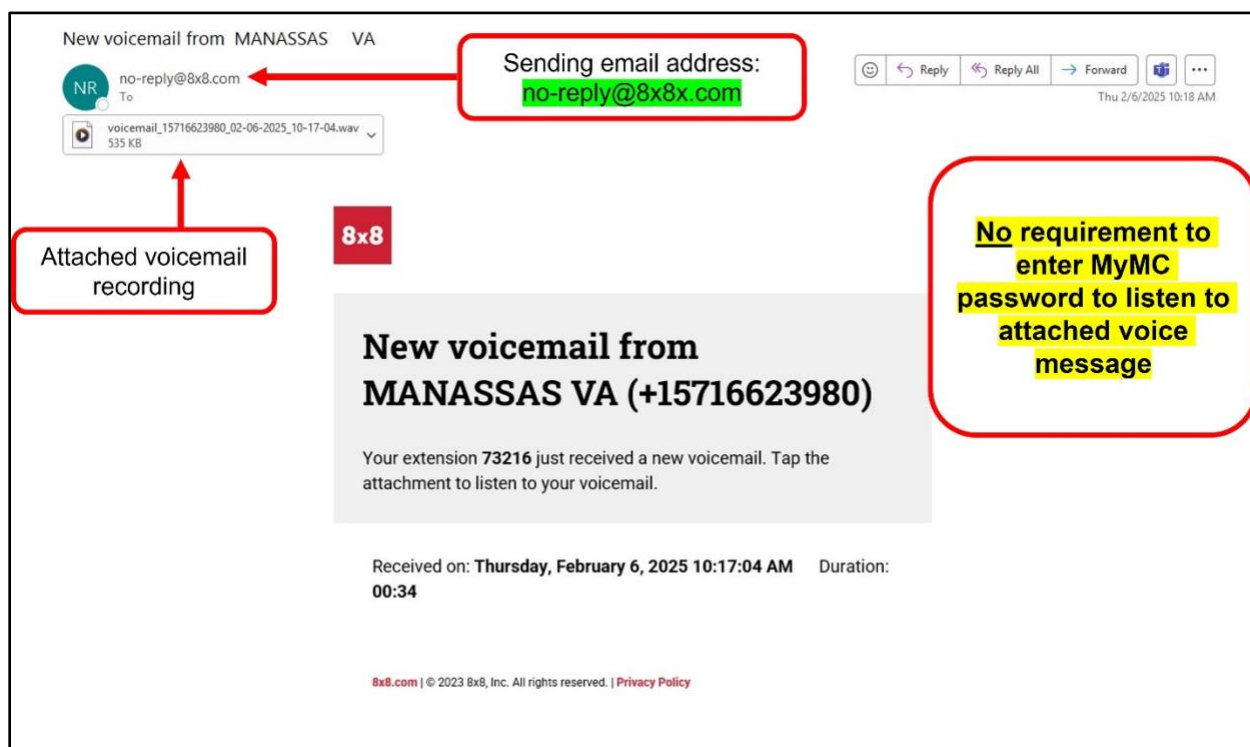


January 2025 Phishing Scenario Results

As part of our Security Awareness Education Program, OIT sent a simulated phishing scenario titled, *Audio Message(s) for first.last.name@montgomerycollege.edu*. The email indicated “You have a new message...”, and provided the date, duration of message, and phone number of the caller that left the message. Voicemail themed phishing emails urge you to open malicious attachments or links and enter your credentials to listen to the message. This type of phishing attack is often successful because legitimate brands are spoofed to look like a typical office communication.

The best way to detect this type of attack is to familiarize yourself with MC’s voicemail sending format and authorized sender:

- Sender is: no-reply@8x8.com
- Sample subject format is:
New voicemail from WIRELESS CALLER
Note: The **from** portion will show what the caller ID detected
- MC’s 8x8 voicemail email notifications do **NOT** require employees to login with MyMC credentials in order to listen to the attached audio recording
- Please review the **legitimate MC voicemail** email below for reference:

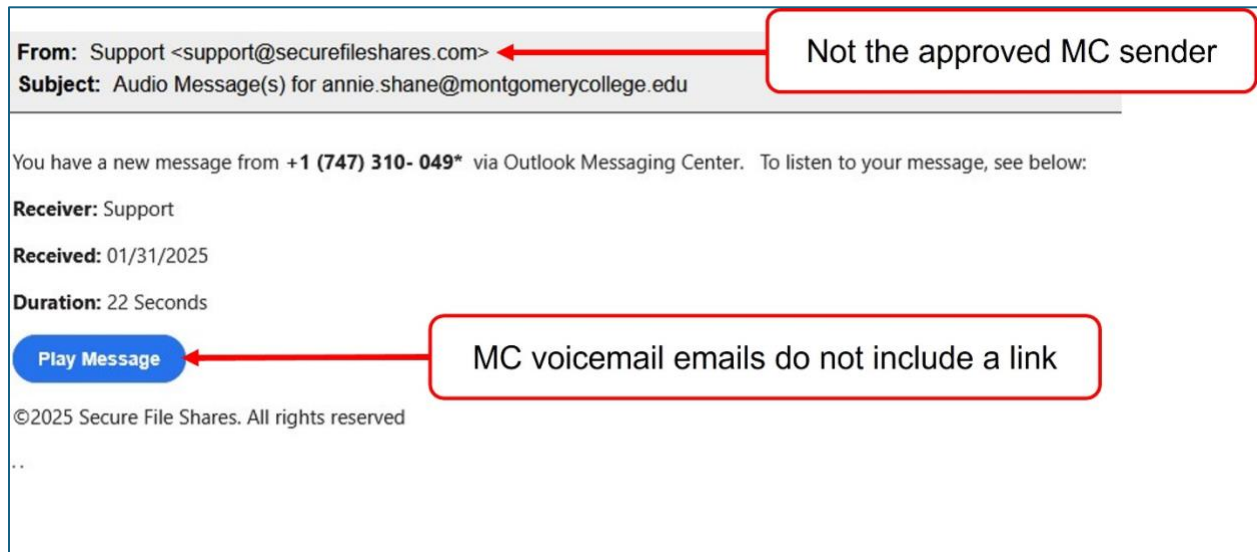


Good news: 902 employees reported the phishing scenario to the Phishtrap. Nice work MC!

Opportunities for Improvement: 616 employees clicked the link within the training email; of these individuals, 122 entered their credentials. Ouch!

Did you know that even **ONE** click puts the entire MC network at risk?

In a real-world phishing attack clicking the link may have prompted you to give up your login credentials. **View the red flags in the January phishing scenario** to learn about this type of attack and ways to spot a suspicious email.



The screenshot shows an email header with the following details:

- From:** Support <support@securefileshares.com> (A red arrow points from a callout box to this address.)
- Subject:** Audio Message(s) for annie.shane@montgomerycollege.edu

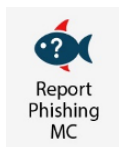
The body of the email contains the following information:

- You have a new message from +1 (747) 310- 049* via Outlook Messaging Center. To listen to your message, see below:
- Receiver:** Support
- Received:** 01/31/2025
- Duration:** 22 Seconds
- A blue button labeled "Play Message" (A red arrow points from a callout box to this button.)
- ©2025 Secure File Shares. All rights reserved
- ..

Two red callout boxes highlight red flags:

- "Not the approved MC sender" points to the sender's email address.
- "MC voicemail emails do not include a link" points to the "Play Message" button.

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 your email application allows you to quickly report suspicious emails to IT Security.