National Cybersecurity Awareness Month 2025
Phishing Contest Recap

WINNERS!

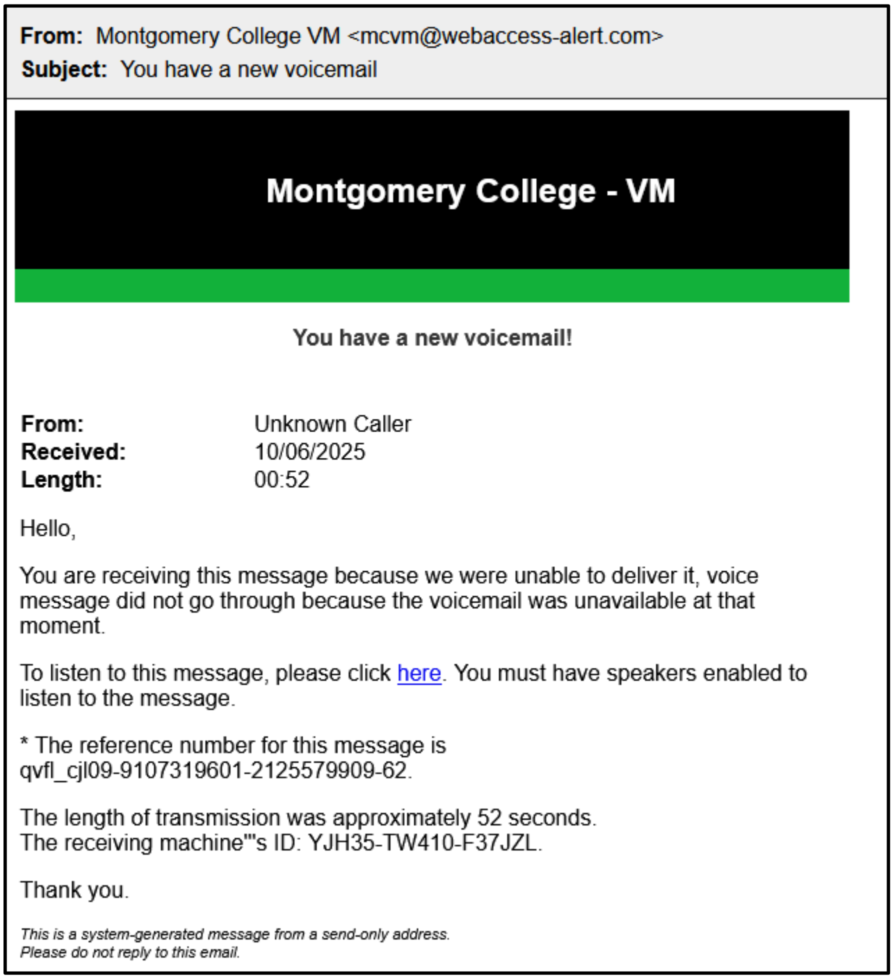
Congratulations to our 50 randomly drawn winners that will receive their well-earned Phishing Pro t-shirt:

Adora Nwigwe	Lauren Valentine
Alex Huebner	Lisa Thomas-Kaonohi
Angela Wright	Lorraine Green
Antonio Gutierrez	Margaret Birney
Bill Weich	Mariam Sherani
Brady Patton	Matthew Carin
Britanny Rodriguez	Michael Spinner
Carolina Turciossorto	Michaela Pacesova
Chu Li Shen	Niya Todorova
Dayan Grero	Ola Cole
Desiree Harvey	Pamela Jones
Donna Kinerney	Priyanka Kalia
Elizabeth Cruz	Raana Hughson
Evelyn Cordova	Sadi Ahmad
Gayle Weisbaum	Samantha Mattocci
Getachew Borena	Samantha Wu
Getnet Habteselassie	Scott Waterman
Gillian Anderson	Sharon Kauffman
Gladys Egbo	Sonia Pruneda-Hernandez
Inger Swimpson	Susan Kushner
Jill Kronstadt	Thomas VanPatten
Joshua Feranil	Tiffany Waters
Kai Fang	Timothy Fuss
Kam Yee	Tumpa Rahman
Kimberly Maffeo	William Valentin

Scenario One: You have a new voicemail

Reported: 876

Clicked: 240



From: Montgomery College VM <mcvm@webaccess-alert.com>
Subject: You have a new voicemail

Montgomery College - VM

You have a new voicemail!

From:	Unknown Caller
Received:	10/06/2025
Length:	00:52

Hello,

You are receiving this message because we were unable to deliver it, voice message did not go through because the voicemail was unavailable at that moment.

To listen to this message, please click here. You must have speakers enabled to listen to the message.

* The reference number for this message is qvfl_cjl09-9107319601-2125579909-62.

The length of transmission was approximately 52 seconds.
The receiving machine'"s ID: YJH35-TW410-F37JZL.

Thank you.

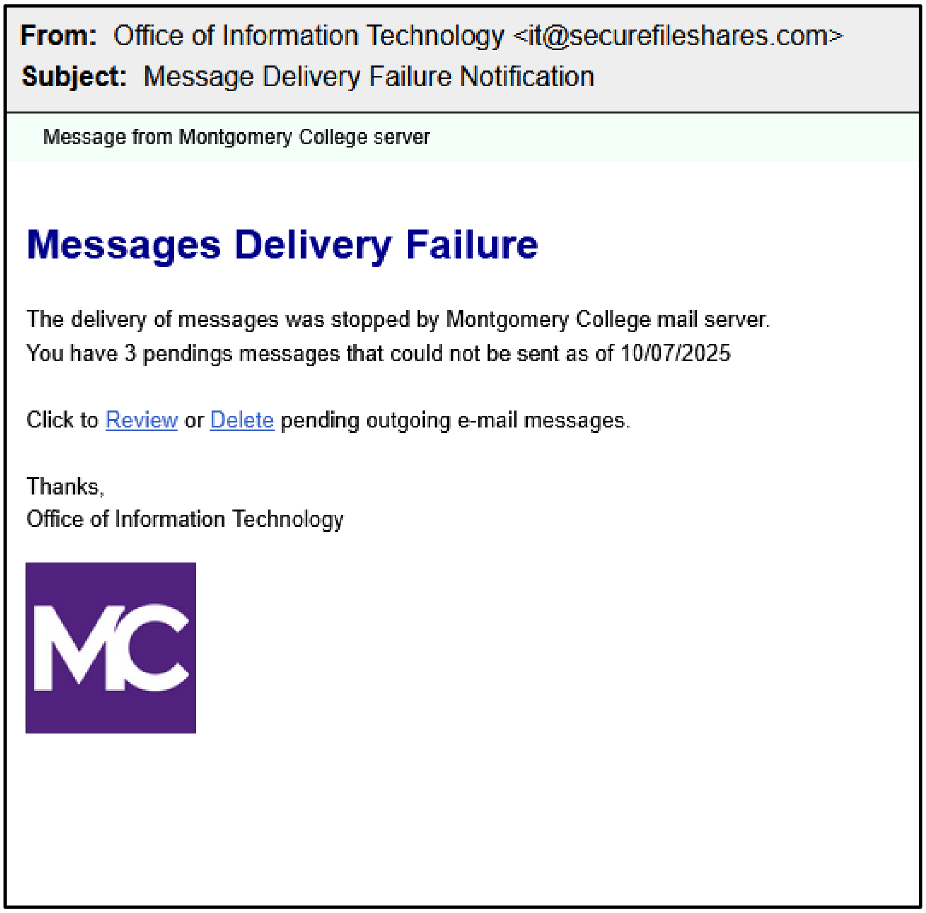
This is a system-generated message from a send-only address.
Please do not reply to this email.

Threat actors use “new voicemail” emails to trick employees into clicking a link in order to listen to the voice message. The link leads to a “login” page prompting the user to enter their username and password. This is how attackers capture your credentials! Legitimate voicemail announcement emails often come from an automated system and in phishing attacks the threat actors capitalize on the “system-like” appearance in hopes you will not question or scrutinize the content. This scenario’s sending address used the display name, “Montgomery College” to trick you into thinking it was from MC. However, the actual email address is from an unknown sender, *mcvm@webaccess-alert.com*. For reference, the MC legitimate voicemail sending address is: no-reply@8x8.com

Scenario Two: **Message Delivery Failure Notification**

Reported: 835

Clicked: 248



From: Office of Information Technology <it@securefileshares.com>

Subject: Message Delivery Failure Notification

Message from Montgomery College server

Messages Delivery Failure

The delivery of messages was stopped by Montgomery College mail server.
You have 3 pendings messages that could not be sent as of 10/07/2025

Click to Review or Delete pending outgoing e-mail messages.

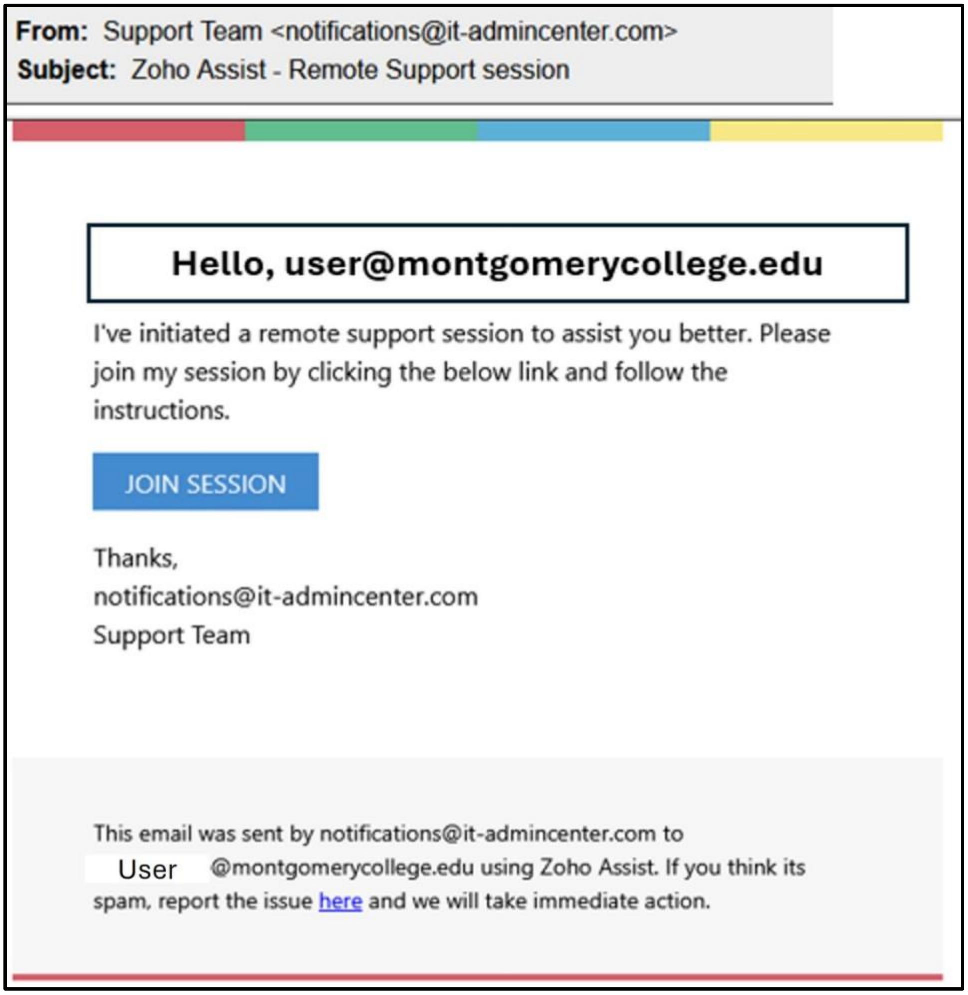
Thanks,
Office of Information Technology

Email delivery, or delivery failure, phishing emails are successful in prompting an emotional response from you. The goal is to get you to react without careful review of the email content. To provide the reader with additional confidence the scenario included the MC logo and the sending display name, “Office of Information Technology”. This type of threat often times includes a link that leads to a prompt for your login credentials.

Scenario Three: Zoho Assist – Remote Support session

Reported: 1084

Clicked: 35



From: Support Team <notifications@it-admincenter.com>

Subject: Zoho Assist - Remote Support session

Hello, user@montgomerycollege.edu

I've initiated a remote support session to assist you better. Please join my session by clicking the below link and follow the instructions.

Thanks,
notifications@it-admincenter.com
Support Team

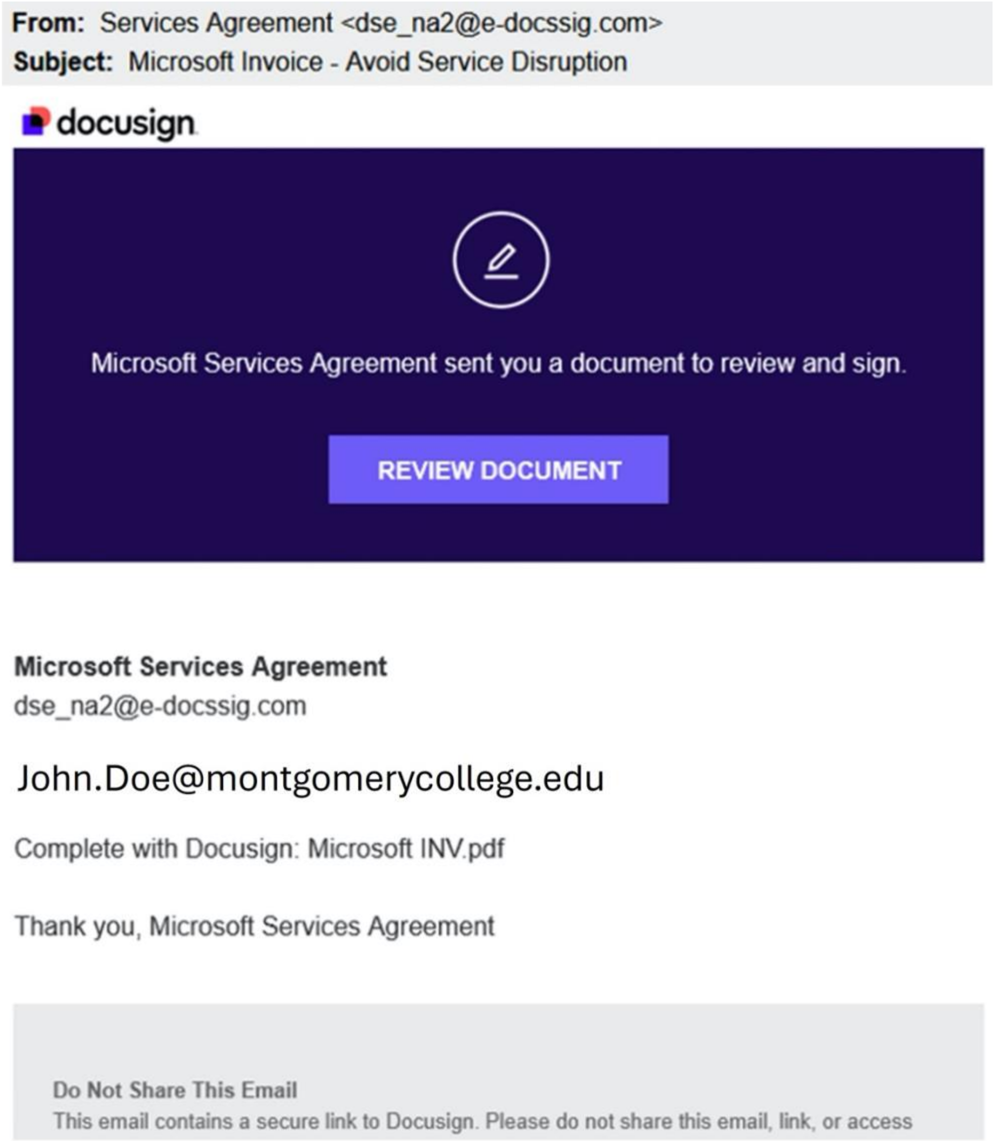
This email was sent by notifications@it-admincenter.com to User @montgomerycollege.edu using Zoho Assist. If you think its spam, report the issue here and we will take immediate action.

This scenario is a commonly used "tech support scam" email that attackers use to scare you into believing there is a virus or other problem with your computer. They include a link or phone number for you to call support and request you allow them remote access to your system under the guise of providing assistance. Once the attacker has remote access, they manipulate the system views and windows to appear there is a technical problem, and offer to fix the problem for a fee. The legitimate IT Service Desk support phone number is 240-567-7222. Any other phone number is not MC related. Contact the IT Service Desk for any MC device or related support issue. The IT Service Desk does not request remote access via email. Do not click on links from unknown senders.

Scenario Four: Microsoft Invoice – Avoid Service Disruption

Reported: 984

Clicked: 76 of these clicked, 23 entered their login credentials



From: Services Agreement <dse_na2@e-docssig.com>
Subject: Microsoft Invoice - Avoid Service Disruption

Microsoft Services Agreement sent you a document to review and sign.

Microsoft Services Agreement
dse_na2@e-docssig.com

John.Doe@montgomerycollege.edu

Complete with Docusign: Microsoft INV.pdf

Thank you, Microsoft Services Agreement

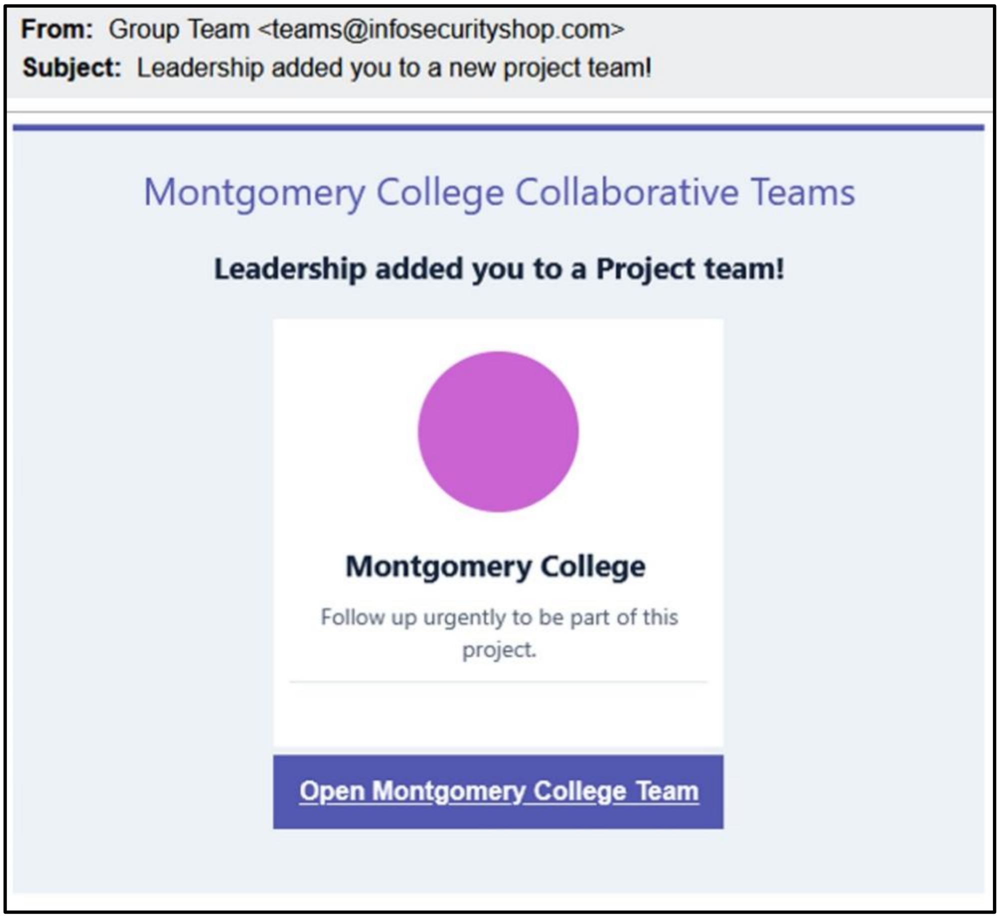
Do Not Share This Email
This email contains a secure link to Docusign. Please do not share this email, link, or access

This phishing scam used the name of a legitimate digital signing service, Docusign. However, they misspelled *Docusig.com* in hopes you would not notice. The first and easiest clue to spot this type of threat is you should know in advance about an email requiring your digital signature. If you are expecting an email that requires your signature (or review) you should establish with the sending party beforehand who will be sending the email and when. Establish a process with the other party to safely respond. An unexpected email of this type should be reported – do not click or trust unknown senders.

Scenario Five: Leadership added you to a new project team!

Reported: 785

Clicked: 305



From: Group Team <teams@infosecurityshop.com>

Subject: Leadership added you to a new project team!

Montgomery College Collaborative Teams

Leadership added you to a Project team!

Montgomery College

Follow up urgently to be part of this project.

The last scenario in this series mimics a Microsoft Teams notification. Notice the email does not identify the name of the person who added you to the Team. The email shows “Leadership” added you, and the notice directs you to “Follow up urgently…”. Messages requiring you to respond urgently should be given your extra attention. As a project manager or department lead, communicate with your colleagues on what medium you will be using ahead of time to avoid confusion or the potential for your team members falling for a phish. An email such as this raises too many questions and should be reported.