Phishing Pro Tournament Scenarios – October 2024

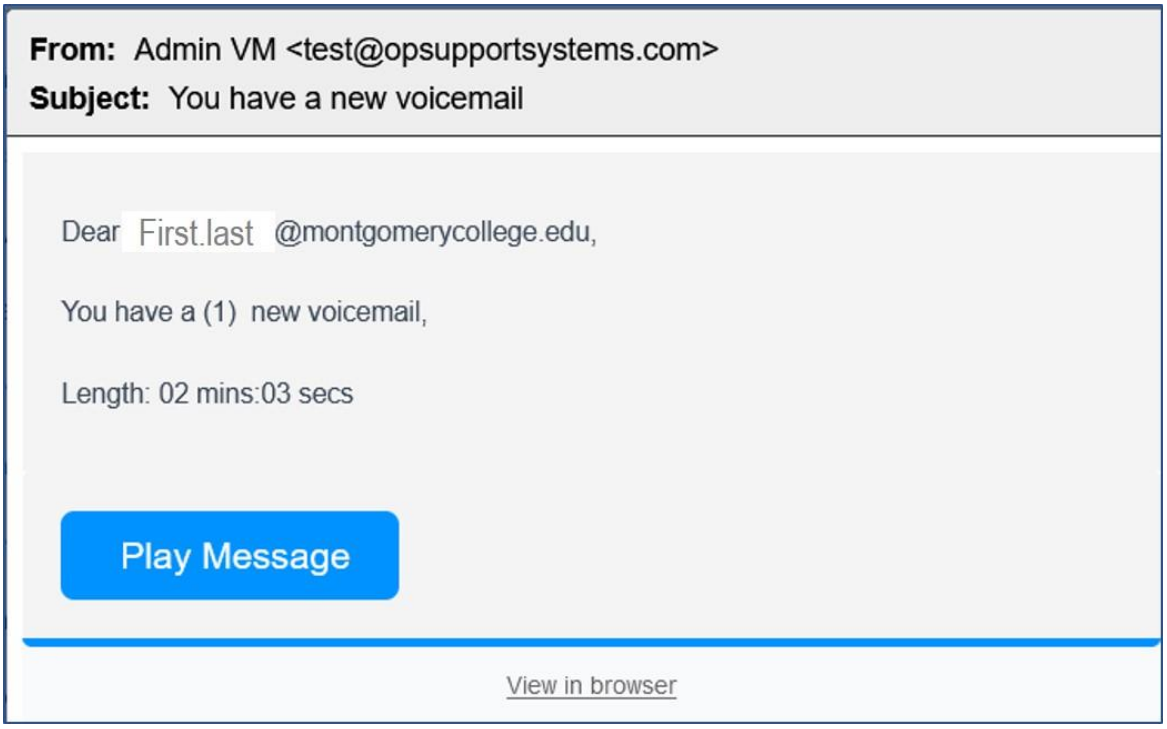
OIT launched the second annual Phishing Pro Tournament for Cybersecurity Awareness Month. This tournament was your opportunity to show off your phishing detection skills and win a prize. The tournament started October 7 and sent one simulation phishing email each day for one week. The goal was to catch all five phishing simulation emails by reporting them using the Report Phishing button **AND** to **NOT** click the link.

Remember: Clicking on links in suspicious emails may lead to potential malware infecting your system or malicious websites requesting your login credentials. Always REPORT and DO NOT click!

Learn more about each daily scenario:

Day 1 - You have a new voicemail
Reported: 933
Clicked: 629
Voicemail phishing emails are designed to be intentionally vague. Typically, there is no content on who left the voicemail and from what phone number. For your reference, legitimate MC voicemail email notification sender information and format include:

- Sender is: VirtualOfficeVoiceMails@8x8.com
- Sample subject format is:
  - VM from 123 456-7890 [City ST] to Ext. 1234 on 11/3/2024 2:30 PM for 28 sec
- MC's 8x8 voicemail notifications do **NOT** require employees to login to hear voicemail audio messages



Day 2 – Incoming Emails Rejected
Reported: 985
Clicked: 273
Employees depend heavily on email communication which is why an "email rejection" phishing email may trigger alarm. The attacker's goal is to get you to react (click) based on your emotions without thinking. Take a pause and let your brain catch up to your emotions. The sending domain is not familiar or associated with MC. Please report suspicious emails before clicking. IT Security will analyze the email and respond on their analysis.

From: Message Center <admin@webaccess-alert.com>
Subject: ®Incoming Emails Rejected

As of 10/08/2024, Office 365 was unable to deliver 5 new incoming emails to your inbox First.last @montgomerycollege.edu due to server error.

Retrieve_messages

2024®

..

Day 3- Password Check Required Immediately
Reported: 1089
Clicked: 269
This is tricky. The notice is informing you "we have updated our password policy". Emails requesting your password require extra scrutiny. Do not click the link and report the email . Legitimate updates and major system changes are communicated by the Office of Information Technology (OIT) from the IT Communications@montgomerycollege.edu sending address.

From: Information Technology <it@verifypass.pw>
Subject: Password Check Required Immediately

Dear Staff,

As part of ongoing efforts to maintain regulatory compliance we have updated our password policy and we need everyone to check their password immediately to ensure that it meets our Minimum Security Requirements.

Please click here to do that:

Check Password

Please do this right away.

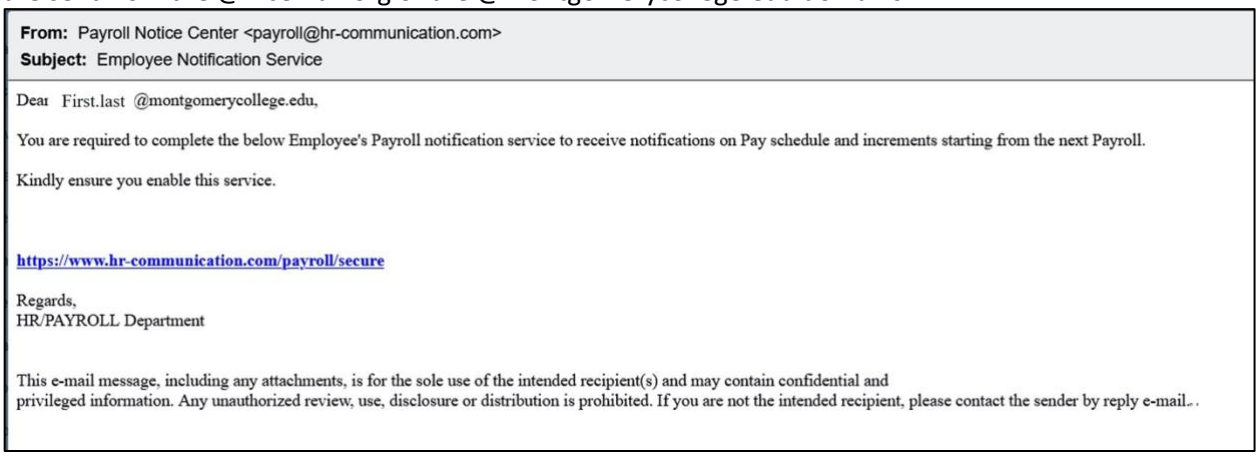
Thanks!
Information Technology
..

Day 4 – **Employee Notification Service**

Reported: 1079

Clicked: 432

Ouch, don't mess with my pay! These are especially triggering since we think failure to comply may result in a disruption to a payment. Again, slow down and re-read the email **before** clicking the link. Too many employees click the link hoping to find the answer. This is especially dangerous as the link may contain malware. Remember, legitimate Human Resources and Strategic Talent email communications are sent from the @mcemail.org or the @montgomerycollege.edu domains.



From: Payroll Notice Center <payroll@hr-communication.com>
Subject: Employee Notification Service

Dear First.last @montgomerycollege.edu,

You are required to complete the below Employee's Payroll notification service to receive notifications on Pay schedule and increments starting from the next Payroll.

Kindly ensure you enable this service.

https://www.hr-communication.com/payroll/secure

Regards,
HR/PAYROLL Department

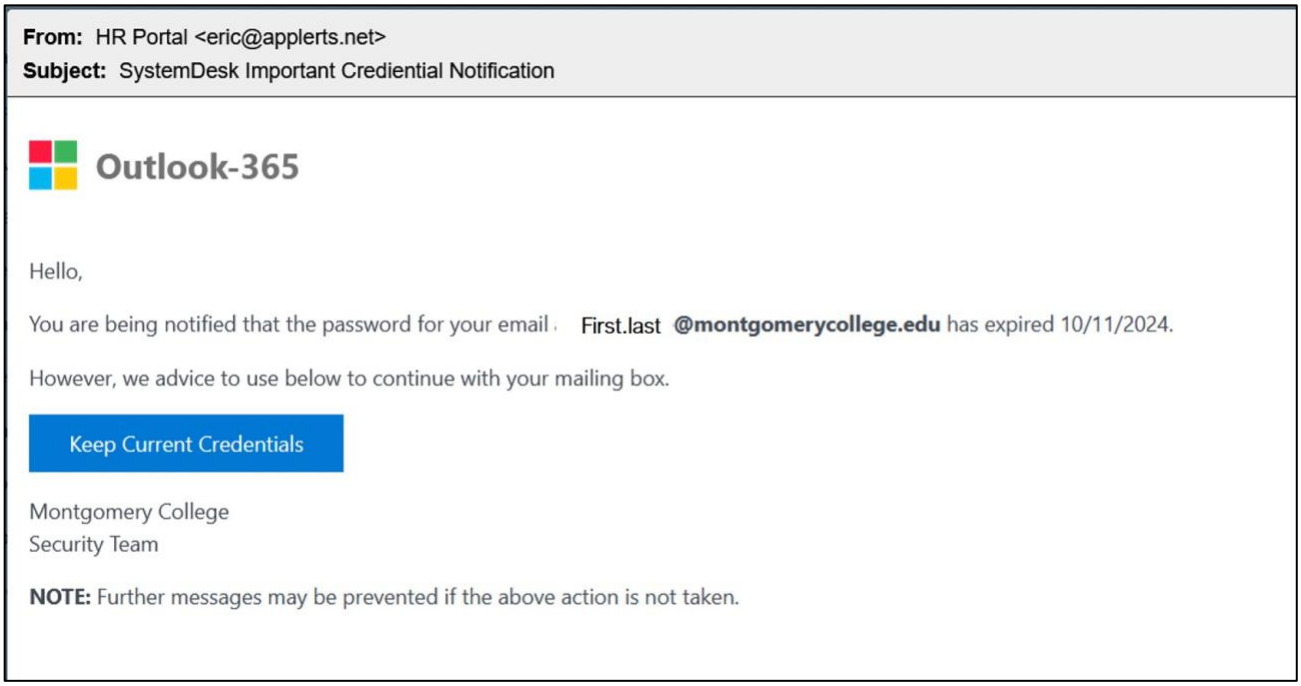
This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail..

Day 5 – SystemDesk Important Credential Notification

Reported: 1102

Clicked: 230

How often are you allowed to "keep current credentials"? Never! This phishing email sports the Microsoft logo to convince you it is a legitimate communication request. This type of email is designed to steal your login credentials. Once you click the link a login prompt is displayed for you to enter your password. MC's solution to protecting user accounts is twofold – educate employees on the threat and prevent unauthorized access with Two-Factor Authentication (2FA), Remember, only authorize 2FA login attempts you initiate. Deny unauthorized attempts using the Duo Mobile app. Montgomery College does not notify employees via email to update their password. Legitimate password updates are generated by the MyMC portal upon login and not from an email.



From: HR Portal <eric@applerts.net>
Subject: SystemDesk Important Crediential Notification

Outlook-365

Hello,

You are being notified that the password for your email First.last **@montgomerycollege.edu** has expired 10/11/2024.

However, we advice to use below to continue with your mailing box.

Keep Current Credentials

Montgomery College
Security Team

NOTE: Further messages may be prevented if the above action is not taken.