Subject: Phishing Results: Payroll Deposit Error

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Payroll Deposit Error*. This email was from an unknown sender and provided a link for the recipient to "sign in" to review messages. The lack of detail and the sensitive subject line are tactics attackers use to lure the recipient into responding in haste without thinking. **Don't let your curiosity outweigh the security of your MC account and data**!

This scenario is a repeat from April 2022. A comparison between April and August results show improvement however, clicking unknown links is still problematic:

	April 2022	August 2022
Reported	988	993
Clicked Link	504	316

## Did you click? In a real-world phishing attack clicking the link may have prompted you to give up your login credentials.

Please review the clues within the email to help you identify this message as suspicious:

From: Human Resources Department <hr@se Subject: Payroll Deposit Error</hr@se 	ecurefileshares.com	sending domain	
Hello Staff.Name@montgomerycollege.edu	1		
You've receive new payroll message on 08/0	3/2022.		
Please follow the instructions to review mess	sages.		
Sign in using the following e-mail address S Review Now Message encryption with Doc-droid PDF. estion ANY quest for bur login edentials	taff.Name@montgomerycollege Unknown doma https://s.securefileshares.com/25 doc/0389c8/ 1bddaee0-b517-43ea-9f91-e0f810 9c7 Click or tap to follow link.	in 13501.	Report Phishing MC Unusual and vague communications



## 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 client allows you to quickly report suspicious emails to IT Security. <u>Learn how to access the Phishing Reporter button when using Office 365 at home.</u> If you accidentally clicked on a link or attachment in a suspicious email, contact the <u>IT Service Desk</u> immediately.

Follow these additional tips to avoid phishing scams:

- Check your emotions. Do not be curious and investigate the link REPORT the email.
- Keep your MC business limited to your MC email address and use your personal email address for personal business.
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- 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 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