Direct Deposit SCAM ALERT March 2024

On March 6, 2024, a malicious email phishing attack targeted a group of Montgomery College employees attempting to obtain their MyMC ID and password. Once employees clicked the link, the attack unfolded as follows:

- 1. A fake MyMC login page was displayed that prompted employees to enter their MyMC ID and password.
- 2. Employees were then presented with a fake Duo Two-Factor Authentication (2FA) prompt where they were asked for a Duo Mobile passcode.

The attacker used the one-time passcode to access the Duo Mobile Device Portal to add their phone to the employee's 2FA account. This granted the attacker access to the employee's MyMC ID information that was then used to access the employee's Workday account. With this access the attacker then changed the employee's direct deposit accounts in an effort to divert and steal the employee's paycheck.

THE GOOD NEWS: IT Security successfully intercepted this attack and **no** direct deposit account changes were processed.

THE BAD NEWS: Several employees clicked the link and potentially provided their personal information to the attacker. **If you clicked the link, and were not contacted by IT Security, please notify the IT Service Desk immediately** to report your encounter and receive guidance about how to protect your account.

The screenshot below is an example of the phishing attack email received by MC employees:



Wed 3/6/2024 6:37 PM

Lindee Eads <Lindee_Eads@hcpss.org>

Immediate Response Needed: COVID-19 Variant Contact Tracing Underway

To Undisclosed recipients:

Dear Member of the Montgomery College Community,

I hope this message finds you and your loved ones in good health and high spirits. However, today, I must address a matter of utmost importance regarding the safety and well-being of our community.

It is with deep regret that I must inform you of a confirmed case of a COVID-19 variant within our staff at Montgomery College. Despite the vaccination status of the majority of our staff and faculty, it is crucial to acknowledge the potential challenges posed by certain variants, even for vaccinated individuals. As a result, we are taking proactive measures to implement comprehensive contact tracing procedures to promptly identify and mitigate any potential risks.

Your immediate cooperation is essential in determining whether you have had close contact with the affected staff member. To facilitate this process, we have established a dedicated webpage for your convenience. Please click the link provided below to access detailed information regarding the staff member: [Access Staff Information]. Your prompt reporting of any interactions or contact is crucial for the well-being and safety of our community.

We understand that this news may be unsettling. However, please rest assured that our medical team is available to address any inquiries and provide guidance. You may reach them at Healthcarecenter@montgomerycollege.edu, and they will assist you promptly.

Our commitment to your well-being and to maintaining a secure working environment remains unwavering. We sincerely appreciate your cooperation, as it is vital for our collective efforts in containing the virus and ensuring the safety of everyone within our community.

As a reminder, this communication and its contents are confidential and intended solely for the recipient. We kindly request your adherence to privacy guidelines by refraining from sharing or forwarding

Your dedication to Montgomery College is deeply valued. Together, we will navigate through this challenge and emerge stronger.

Warm regards

Lindee Eads Montgomery College Health Care Center 7600 Takoma Avenue, Takoma Park, MD 20912 Phone: 240-567-5000

It is critical that we all remain vigilant staying alert and reporting suspicious or out of the ordinary emails. For example, users reported that the fake MyMC login page and Duo prompt appeared "different." Remember, **if it seems PHISHY**, **it probably is PHISHY**. Please take the time to review the sending email address, content, and nature of the request before clicking.



Please use the Report phishing button to <u>REPORT</u> suspicious emails and let IT Security analyze it for you.

As always, the IT Service Desk is available to address any technology-related questions or issues:

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

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

IT Urgent

Office of Information Technology