May Phishing Scenario Results

As part of our Security Awareness education program, OIT sent a simulated phishing scenario titled, *New myGov message*. The message indicated the recipient has a "new message" in their "myGov" inbox.

The first clue in this phishing scenario is the insinuation that you have a "myGov" account. There are legitimate government accounts that individuals may open however, this message leads the recipient to believe they have a "myGov" account. Moreover, the body of the email is vague, and the sending domain is from a .net domain and not a .gov domain.

To avoid confusion, use a password manager to keep track of all your accounts and to know which ones you created. A password manager is a vault where you store all your individual accounts with each account login username and password, and gain access to the vault with only having to remember the main password. They also offer password generation tools that create a secure password based on the criteria you input such as 15 characters in length, containing one letter and one symbol.

Most importantly, to avoid phishing email tricks such as this scenario, only use your Montgomery College email address for College business and set up personal accounts using your personal email address. This helps in identifying a phish/scam immediately because a personal government account message addressed to your College email is a red flag.

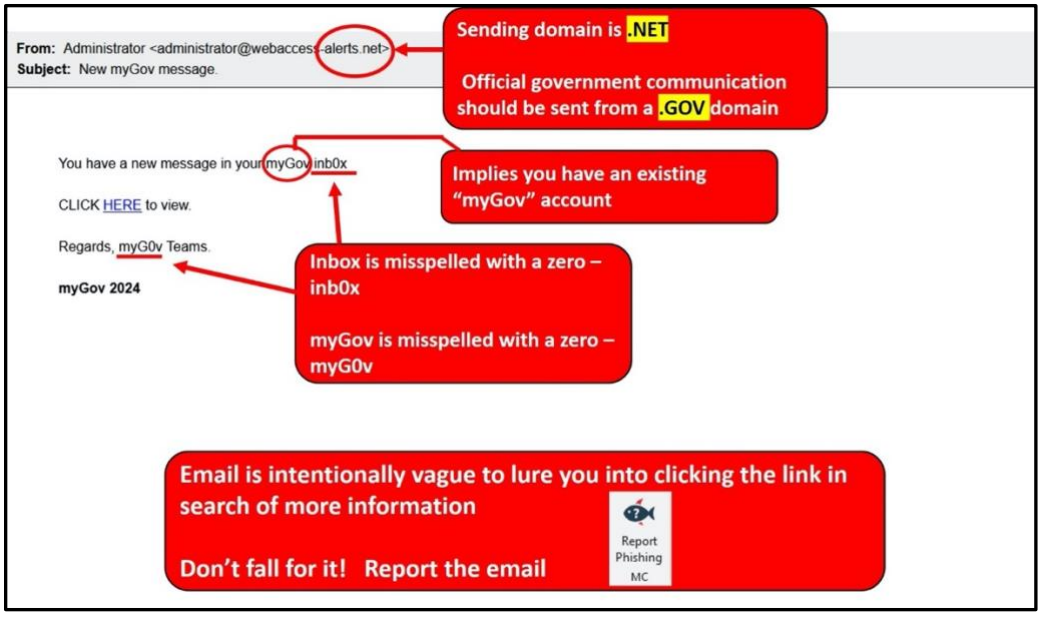
Good news:

821 employees reported the phishing scenario to the Phishtrap. Nice work MC!

Opportunities for improvement:

179 employees clicked the link within the training email. One click is one too many. 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 May phishing scenario to learn about this type of attack and ways to spot a suspicious email.



To avoid falling for these tricks remember to pause, reread the email, and if suspicious, report the email using the Report Phishing button.