IT Security: March 2024 Phishing Scenario Results

As part of our security awareness education program, OIT sent a simulated phishing scenario titled, *O365 FIX KIT*. The phishing scenario included the Microsoft (MS) logo to assure the recipient on the legitimacy of the request. This impersonation tactic works by exploiting Microsoft's familiarity and imposing fear by stating your emails will be blocked unless you "Follow the steps to FIX."

In a real phishing email the "FIX" is a malicious download and/or link that attempts to capture your login credentials. Brand impersonation threats provide a link to a webpage that resembles a MS login prompt for the user to enter their username and password. Upon entering your login information, the attacker now has your credentials!

Detecting a phishing email threat, like this month's scenario, is difficult when all the indicators seemingly "pass" such as no grammatical errors, MS logo matches the real logo, the contact information links lead to the real MS domain, etc. We recommend asking yourself the why question. Why is this **external to MC** sender contacting me to download a "FIX"? Pause, think, and question, especially an email that is requesting you to download items or asks for your login password!

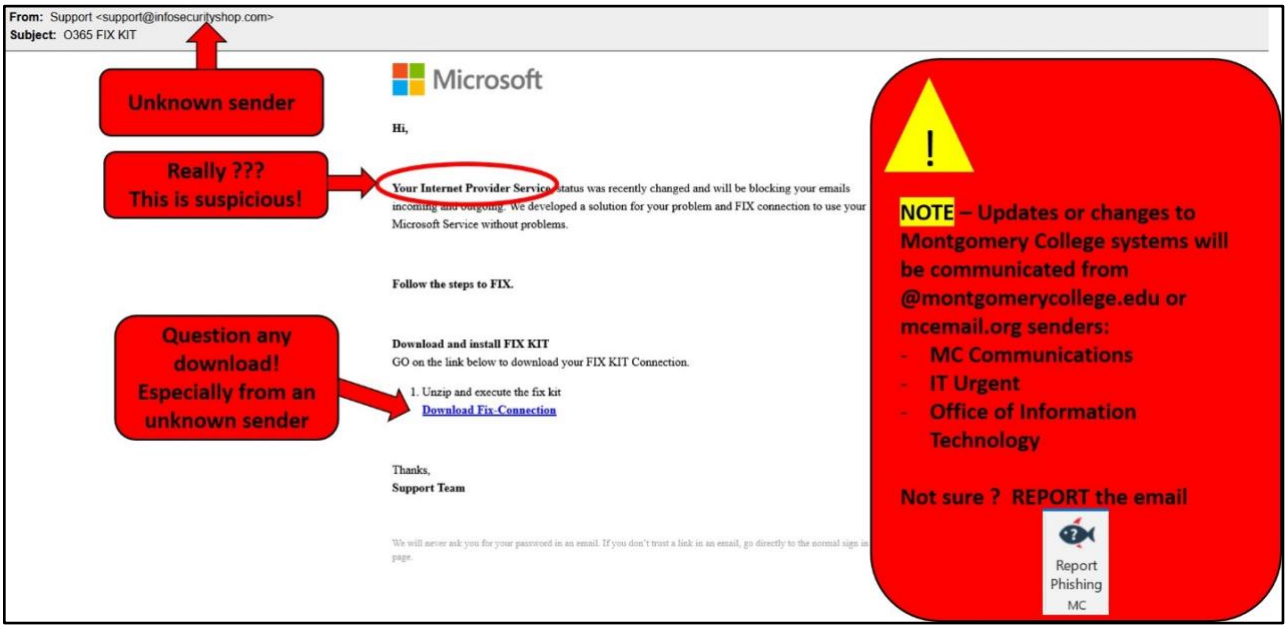
Good news:

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

Opportunities for improvement:

3 employees clicked the link within the training email. While three is a low number – one is still 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 below 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**.