June Phishing Scenario Results

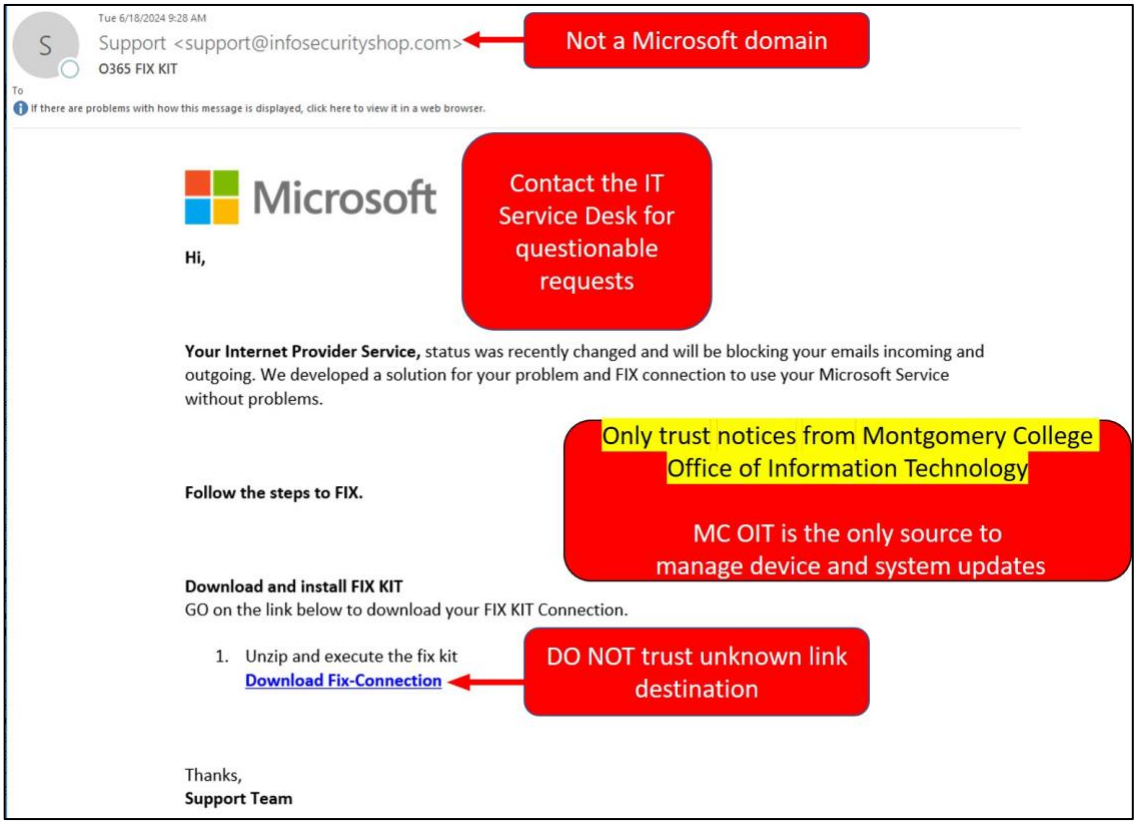
As part of our Security Awareness education program, the Office of Information Technology (OIT) sent a simulated phishing scenario titled, *O365 FIX KIT*. The phishing scenario notified the recipient that their "Internet Provider Service" changed and as a consequence, emails would be blocked. To fix the problem the email provided a download link instructing the user to "Unzip and execute" the fix kit.

Urgency and fear are the most commonly used phishing tactics. To further convince their target, they use authentic-looking logos, in this case, Microsoft. Utilize best practices to pause, reread the content, and do not respond (click) when urgency and fear are present. Do not download and install executables on to your device unless instructed by OIT. **Montgomery College OIT is the only source for managing updates to MC devices.**

Good news:
861 employees reported the phishing scenario to the Phishtrap. Keep up the good work!

Opportunities for improvement:
49 employees clicked the link within the training email. Did you know that even ONE click puts the entire MC network at risk.

In a real-world phishing attack clicking the download may have installed malware or ransomware. View the red flags in the June 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.

Kindly direct technology-related questions or issues to the IT Service Desk:

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