

## 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:

The image shows a screenshot of a simulated phishing email. The email header includes a sender profile for 'Support' with a logo and the address 'support@infosecurityshop.com'. A red callout box points to this address with the text 'Not a Microsoft domain'. The email body features the Microsoft logo and the text 'Hi,'. A red callout box points to the Microsoft logo with the text 'Contact the IT Service Desk for questionable requests'. Below the greeting, the email text states: 'Your Internet Provider Service, status was recently changed and will be blocking your emails incoming and outgoing. We developed a solution for your problem and FIX connection to use your Microsoft Service without problems.' A red callout box points to this text with the text 'Only trust notices from Montgomery College Office of Information Technology' and 'MC OIT is the only source to manage device and system updates'. The email then says 'Follow the steps to FIX.' and 'Download and install FIX KIT GO on the link below to download your FIX KIT Connection.' A list of instructions follows: '1. Unzip and execute the fix kit' with a blue link 'Download Fix-Connection'. A red callout box points to this link with the text 'DO NOT trust unknown link destination'. The email ends with 'Thanks, Support Team'.

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](mailto:itservicedesk@montgomerycollege.edu)

by web chat on [OIT's web page](#)

by phone at 240-567-7222