Introduction

This week focuses on the second cybersecurity behavior: **Turn on Multi–Factor Authentication (MFA)**. A password alone isn't enough to fully secure your online accounts. Activating MFA greatly reduces your chances of being hacked. Be sure to enable MFA on all accounts that support it, particularly for email, social media, and financial platforms.

At CUNY, Multi-Factor Authentication (MFA) already provides an essential layer of security when accessing your Microsoft Office 365 account and remotely connecting to CUNY network resources. MFA is currently being rolled out across all enterprise applications in collaboration with college IT departments to strengthen protection and ensure consistent access control. **Your participation in this initiative is fundamental to improving CUNY's overall security posture**.

By adopting MFA and staying engaged with its implementation, you help safeguard institutional data and support a safer digital environment for everyone. The University's Acceptable Use of Digital Assets and Resources policy requires that "Users [be] responsible for engaging in safe computing practices that include … using enhanced authentication features such as multi-factor authentication where available."

Helpful Cybersecurity Tips

- CUNY requires that all students, faculty, and employees follow Cybersecurity Best Practices.
- Protect yourself against secret shopper, personal assistant, and other online scams.
- Follow CUNY's Best Practices for Secure Learning, Teaching, and Working Remotely.
- When using Zoom, follow CUNY's Zoom Security Protocols.
- Take advantage of CUNY's online cybersecurity awareness course available through Brightspace:
    - Students: ~25 minutes
    - Faculty and staff: ~40 minutes

Additional Resources and Tips:

- CUNY Microsoft MFA and CUNY Login MFA resources
- MFA in 2025: Best Options Ranked

- Multi-Factor Authentication (NCA)
- Secure Our World: MFA Tip Sheet (CISA)
- Popular Sites and Services That Support MFA (Directory)
- Cybersecurity Best Practices (CISA)
- 2025–26 College of Staten Island Cybersecurity Awareness Training is now live on Brightspace

Facts and Figures:

Insights from the 2024–2025 “Oh, Behave!” Report (National Cybersecurity Alliance & CybSafe) are as follows:

- **45%** of people began using MFA after cybersecurity training – up **11%** from last year.
- **79%** of respondents are familiar with MFA, and **70%** of those who have heard of it know how to use it.
- Younger generations (Gen Z and Millennials) are the most likely to use MFA, while adoption among Baby Boomers and older generations is still lagging.
- MFA is one of the simplest and most effective ways to block unauthorized access.

Our emails and supporting information are available from the National Cyber Security Awareness Month (NCSAM) page on the CUNY web site. We also provide a growing security resources list on the CUNY Information Security pages. You may also want to visit the OUCH! website to read recent security articles or subscribe to the world’s leading, free security awareness newsletter designed for technology users.

If you have any questions about any of this information, please contact your college's Information Security Manager.