

## Introduction

October is dedicated to Cybersecurity Awareness Month, a worldwide initiative to promote safer and more secure online experiences. CUNY is proud to participate in this year's Cybersecurity Awareness Month program, in collaboration with the National Cybersecurity Alliance (NCA) and the Cybersecurity and Infrastructure Agency (CISA) of the U.S. Department of Homeland Security. Throughout October, you will receive weekly messages on four key cybersecurity behaviors:

Week 1 – **Enabling multi-factor authentication**

Week 2 – **Using strong passwords and a password manager**

Week 3 – **Updating software**

Week 4 – **Recognizing and reporting phishing attack**

This Week 1 is focused on “**Enabling Multi-Factor Authentication (MFA)**” — an important and easy way to help keep your accounts and online information secure. Already available for most online banking and retail websites and mobile applications, you should choose to enable MFA wherever and whenever it is available to you.

At CUNY, [Microsoft MFA](#) already serves as an additional layer of cybersecurity protection when accessing your Microsoft Office 365 account. You can expect the MFA protection to be extended to other CUNY applications and services in the coming months.

### **MFA Facts and Figures:**

In response to a NCA survey:

- Less than two-thirds, specifically **57%** of the respondents, had heard of MFA.
- Among those who were aware of MFA, a significant majority, around **79%**, had applied MFA to their online accounts.
- An even higher percentage, **94%**, of those who had implemented MFA continued to use it.

In response to a Duo Labs survey:

- Two-factor authentication has become more popular over the last two years, with **79%** of US/UK respondents saying they used it in 2021, compared to **53%** who used it in 2019.
- SMS text messages are the most common second factor US/UK users choose when logging into two-factor authentication accounts, at **85%**.

### **MFA Resources:**

- Check this [2factorauth](#) web page to find out which websites do or do not have multi-factor authentication available.
- Find more information on [Enabling Multi-Factor Authentication \(MFA\)](#) on the National Cybersecurity Awareness Alliance site.
- Learn the value of MFA with this [MFA Infographic](#).

### **Helpful Cybersecurity Tips:**

Training and documentation [resources](#) are available on the CUNY MFA website.

- CUNY requires that all students, faculty and employees follow these [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](#).
- CUNY students may already be enrolled by their college in CUNY's online cybersecurity awareness course through their learning management system (Blackboard). The course duration for students is 25 minutes. **Faculty and staff** can take the CUNY's online cybersecurity awareness course via the direct [link](#) or through Blackboard (learning management system) as well. The course duration for faculty & staff is 40 minutes.

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](#).