

Week 3 – Keep Software Updated

Introduction

This week, we focus on **Keep Software Updated**.

Keeping your software updated is an important part of protecting your devices and information. Updates often include security patches that address newly discovered vulnerabilities. CUNY's Cybersecurity Best Practices recommends installing software updates as they are released, including Microsoft and Apple software security updates, and maintaining up-to-date antivirus and antimalware software.

Don't put off important updates. Keeping your operating system, applications, web browsers, and security software current helps protect both your personal information and University data.

Helpful Software Update Tips:

- Turn on automatic updates whenever possible.
- Install updates promptly instead of repeatedly selecting “Remind me later.”
- Keep your operating system, applications, web browsers, and security software current.
- Download software and updates only from trusted sources, such as official vendor websites or app stores. Avoid clicking on unexpected or suspicious pop-ups that claim your software needs to be updated.

Software Update Resources:

- [CISA - Understanding Patches and Software Updates](#)
- [National Cybersecurity Alliance - Why You Should Update Software for Security and How to Do It](#)

- [CISA – Secure Our World](#)
- [CISA – Secure Our World Cybersecurity Awareness Month Resources](#)

Facts and Figures:

Insights from the Oh Behave! Cybersecurity Attitudes and Behaviors Report: 2021–2025 (National Cybersecurity Alliance & CybSafe) are as follows:

- The percentage of respondents who reported **always installing software updates declined from 44% in 2021 to 31% in 2025.**
- The five-year study found that routine cybersecurity maintenance habits, including installing software updates, **weakened over time despite increased cybersecurity awareness.**

Helpful Cybersecurity Tips:

- [CUNY Cybersecurity Best Practices](#)
- [Secret Shopper, Personal Assistant, and Other Online Scams](#)
- [CUNY Information Security Resources](#)
- [CUNY Security Awareness](#)

Our emails and supporting information are available from the [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 its 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](#)