

Week 4 – Scrutinize Every Message (Oct 26)

Introduction

This week, we focus on Scrutinize Every Message.

Phishing and online scams remain common ways cybercriminals try to steal personal information, credentials, or gain access to accounts. Be cautious with unexpected emails, texts, and other messages, especially those that ask you to act urgently, provide sensitive information, open an attachment, or click a link.

Before responding or taking action, check the sender, examine links carefully, and consider whether the request makes sense. If a message appears suspicious, don't click the link or open the attachment. At CUNY, suspicious emails should be reported directly through Outlook using the Report Phish button. The button's appearance and location may vary depending on your version of Outlook.

Helpful Message Safety Tips:

- Be cautious with unexpected messages, especially those requesting personal, financial, or account information.
- Check the sender carefully and examine links before clicking.
- Be suspicious of urgency or pressure designed to make you act without thinking.
- Don't open unexpected attachments or click suspicious links.
- Verify questionable requests another way by contacting the person or organization using contact information you already know or find independently—not the information provided in the suspicious message. If you believe you clicked a suspicious link or entered your credentials on a suspicious website, contact your college IT office immediately.
- Report suspicious emails: Select the suspicious email in Outlook, click the Report Phish button, and confirm if prompted. Try to avoid forwarding suspicious emails to your campus help desk, IT staff, or colleagues for review. For step-by-step instructions, see the [Knowledge Base Article](#).

Phishing and Message Safety Resources:

- [CISA – Recognize and Report Phishing](#)
- [National Cybersecurity Alliance – What Is Phishing? How to Spot and Avoid Phishing Scams](#)

- [National Cybersecurity Alliance – Reporting Cybercrime](#)

Facts and Figures:

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

- In 2025, **phishing accounted for 40% of reported cyber incidents**.
- The five-year study found that **confidence in identifying phishing messages increased**-, even as cybercrime victimization continued to rise.

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](#).