Welcome to the fourth and final week of National Cybersecurity Awareness Month. This week, our focus is on **"Recognizing and Reporting Phishing."** Phishing attacks increased by 61% in 2022, according to SlashNext. Email and text phishing attacks have become an increasingly common problem for organizations of all sizes and can be very difficult to spot. In fact, 30% of small businesses consider phishing attacks to be their top cybersecurity concern.

It's important for every individual to spot phishing's red flags and stop and think before clicking on a link or attachment in a message.

Phishing Prevention Resources:

- You can find more information in Recognize and Report Phishing Attacks on the National Cybersecurity Awareness Alliance site.
- Learn more about phishing in a Recognizing and Reporting Phishing Infographic.

Helpful Phishing Prevention Tips:

- Be wary of malicious links in messages offering a "reward" or "free gift."
- Tips for Spotting a Phish: 1) They create a sense of urgency or claim to need help. 2) They ask for your personal info. 3) They want you to download a file or click on a link.
- Do not verify your account in response to an unsolicited email or text by logging into a webpage or updating your credentials.
- If you receive a suspicious email or text, do not click on any links – even the unsubscribe link – or reply to the email.
- A phishing scheme can also install malware onto your device.
- If you are able to recognize spam or phishing emails, just delete them.
- If you suspect an email is phishing for your information, it's best to report it quickly to your IT help desk.
- Only verify account information using customer service contact and website information provided in monthly statements or original account documentation.

Phishing Facts and Figures:

In response to a NCA survey:

- **72% of respondents** reported that they checked to see whether messages were legitimate (not phishing or a scam) compared to 10% who reported not doing so.

- **Nearly half of the participants (48%)** reported phishing emails to the sender (the person or entity the cybercriminal tried to impersonate by sending the phishing email).
- **42% of the participants** said they used the reporting capability on a platform (e.g., Gmail) “very often” or “always”.

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.