Bonus Week: Understanding Phishing and Social Engineering

As Cybersecurity Awareness Month concludes, we're sharing bonus content that highlights phishing and social engineering – two prevalent tactics used by attackers to manipulate individuals into disclosing sensitive information or engaging with malicious links. Stay informed and vigilant.

What Is Phishing?

Phishing is a type of cyberattack where attackers impersonate trusted entities: such as university officials, IT support, or even fellow researchers; just to trick you into revealing sensitive information or clicking malicious links.

Common signs of phishing emails:

- **Urgent or threatening language** – Such as "Your account will be suspended!"
- **Unexpected attachments or links**
- **Requests for login credentials or financial information**
- **Unusual formatting and, nowadays with AI, too-perfect grammar** – no typos, no contractions, overly polished. Humans rarely write like that.
- **Tone mismatch** – does the email sound slightly off – too formal or too casual for the sender?
- **Vague urgency** – phrases like "Need this processed quickly" without context or clarity are common AI patterns.
- **No follow-up path** – no phone number, reply thread, or calendar invite. AI can't (yet) simulate full business context well.
- **Unusual attachment names** – e.g. *invoice_urgent_45b.pdf* or *transfer_auth_final.docx*.
- **Subtle hallucinations** – an AI might refer to a meeting that never happened or assign someone the wrong job title.
- **Odd time-of-day patterns** – was it sent at 3:17 a.m.? That's a sign of automation.
- **Overuse of synonyms** – instead of "Please review," you might see "Kindly assess and evaluate at your earliest."
- **Signature inconsistencies** – if Mike usually signs "-Mike" but this one says "Michael Wright, MSc, CISSP," something's off.
- **Unusual language density** – AI email often feels overly formal or verbose without emotion or shortcuts.

What Is Social Engineering?

Social engineering goes beyond email. It also involves manipulating people into giving up confidential information via phone calls, text messages, or in-person tactics. Examples:

- A caller pretending to be from IT asking for your password
- Someone posing as a visiting scholar requesting access or tailgating at the entrance
- A message claiming to be from a journal editor asking for payment

How You Can Stay Safe

- **Think Before You Click:** Hover over links to verify URLs. Don't open attachments from unknown senders.
- **Verify Requests:** If someone asks for sensitive info, confirm their identity through official channels.
- **Report Suspicious Activity:** Use the "Report Phishing" button below. *Do not forward the suspicious email.*
- **Use Strong Passwords:** Enable multi-factor authentication (MFA) wherever possible.
- **Stay Informed:** Take CUNY Cybersecurity Training.

Additional Resources and Tips

- Recognize and Report Phishing – Secure Our World (CISA)
- Phishing: How To Spot and Avoid It (Stay Safe Online)
- Cybersecurity Best Practices (CISA)
- 2025–26 College of Staten Island Cybersecurity Awareness Training is now live on Brightspace

Facts and Figures

- **52%** of people reported experiencing phishing attempts in the past year – up 2% from 2023.
- **69%** feel confident identifying phishing attempts, though many still fall victim.
- **51%** of Americans actively report cybercrimes, particularly phishing.
- **33%** began recognizing more phishing attempts after receiving cybersecurity training.
- **Younger generations (Gen Z and Millennials)** are targeted more frequently due to higher online activity.

Spread the Word

Cybersecurity is a shared responsibility. Please share this message with your colleagues and students. Together, we can build a safer academic environment.

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.