Phishing

Cybersecurity Awareness Month
October 2022

New York State Comptroller
THOMAS P. DiNAPOLI

1

Division of Local Government and School Accountability

Applied Technology Unit
Ariel Bethencourt

New York State Comptroller
THOMAS P. DiNAPOLI

2

Phishing

- When a cybercriminal poses as a legitimate party in the hopes of:
  - Getting individuals to engage with malicious content or links;
  - Users unknowingly providing personal or sensitive information;
  - Installing malware on computers or mobile devices;
  - Initiating ransomware.

New York State Comptroller
THOMAS P. DiNAPOLI

3

How to Spot a Phishing Attempt

- Contains an offer that's too good to be true
- Language that's urgent, alarming or threatening
- Poorly crafted writing with misspellings and bad grammar
- Requests to send personal information

How to Spot a Phishing Attempt (continued)

- Urgency to click on an unfamiliar hyperlink or attachment
- Sending email address doesn't match the company or municipality it's supposedly coming from

How to Report a Phishing Attempt

- Report incident to your IT manager or security officer.
- Block sending address.
- Report email as a phishing attempt directly in the email platform.

Help Mitigate Phishing Risks

Best practices

- Provide Security Awareness Training and include phishing topics to help advise and inform regarding phishing-related risks, identification tips and actions to take if users suspect they have been phished (See our Week 1 Webinar, *Cybersecurity Foundations*).

New York State Comptroller
THOMAS P. DiNAPOLI

7

Help Mitigate Phishing Risks
(continued)

- Provide periodic updates to all users regarding current and emerging cybersecurity threat trends, including phishing schemes.
- Employ the principle of least privilege and restrict user access to only the resources that are necessary to accomplish their assigned duties.

New York State Comptroller
THOMAS P. DiNAPOLI

8

Help Mitigate Phishing Risks
(continued)

- Enable Multifactor Authentication (MFA) where possible (See our Week 3 webinar, *Multifactor Authentication*).
- Implement strong password practices (see our Week 4 webinar, *Passwords*) including, but not limited to:
  - Monitor for password and account compromise;
  - If a compromise is suspected or detected, require an immediate password change.

New York State Comptroller
THOMAS P. DiNAPOLI

9

Help Mitigate Phishing Risks
(continued)

- Install software updates and patches in a timely manner (see our Week 2 webinar, *Software Management*).

Additional LGSA Resources

Visit our website for additional cybersecurity resources:

- Publications
  - https://www.osc.state.ny.us/local-government/publications
- Training
  - https://www.osc.state.ny.us/local-government/academy

Additional LGSA Resources
(continued)

Visit our website for additional cybersecurity resources:

- Audits
  - https://www.osc.state.ny.us/local-government/audits

Other Resources

- Center for Internet Security (CIS)
  - https://www.cisecurity.org/
- Cybersecurity and Infrastructure Security Agency (CISA)
  - https://www.cisa.gov/
- Federal Bureau of Investigation (FBI)
  - https://www.fbi.gov/investigate/cyber

New York State Comptroller THOMAS P. DiNAPOLI

13

Other Resources (continued)

- National Institute of Information Technology Services (NIST)
  - https://www.nist.gov/cybersecurity
- New York State
  - Office of Information Technology Services
    - https://www.its.ny.gov
  - Division of Homeland Security and Emergency Services
    - https://www.dhses.ny.gov/cyber-incident-response-team

New York State Comptroller THOMAS P. DiNAPOLI

14

Questions?

Contact us

- LGSA Applied Technology Unit's Cyber Team
  - LGSACyberTeam@osc.ny.gov
- LGSA Help Line
  - 1-866-321-8503 or
  - 518-408-4934

New York State Comptroller THOMAS P. DiNAPOLI

15

Thank You!

New York State Comptroller
THOMAS P. DiNAPOLI

16