

Cybersecurity for Local Governments and Schools: A 2-Part Live Webinar Series



New York State Comptroller
THOMAS P. DINAPOLI



1

Part 1 – Effective Cybersecurity Awareness Training



New York State Comptroller
THOMAS P. DINAPOLI



2

Division of Local Government and School Accountability (LGSA)

Applied Technology Unit (ATU)
Information Systems Auditor

Courtney Knight

3

Part 1 Agenda

- **Who, What, When, Where and Why?**
- Assessing Training Effectiveness
- Enhanced Cybersecurity Knowledge
- Cybersecurity Concepts and Terminology
- Measuring Cybersecurity Knowledge
- The Knowing-Doing Gap
- Cybersecurity Aware Practices
- Indicators of Effective Cybersecurity Awareness
- Measuring Cybersecurity Practices
- Part 2 Preview
- Cybersecurity Resources

New York State Comptroller
THOMAS P. DI NAPOLI

4

Who?

Cybersecurity awareness is essential for anyone who uses or accesses a local government's or school's technology, including:

- Officials and employees with access to data containing personal, private or sensitive information.
- Information technology (IT) system administrators.
- Third-party representatives providing services that involve IT system use or access.



New York State Comptroller
THOMAS P. DINAPOLI



5

What?

Valuable cybersecurity awareness topics include:

- Common cyberattack techniques (e.g., phishing, ransomware)
- Pertinent, evolving cybersecurity risks, threats and best practices (e.g., password standards, email security, public Internet risks)
- Incident reporting procedures

New York State Comptroller
THOMAS P. DINAPOLI

6

When?

Cybersecurity awareness training should occur:

- Initially upon onboarding/granting access, and
- At least annually thereafter, with
- Periodic updates ongoing.

New York State Comptroller
THOMAS P. DINAPOLI

7

Where?

- Cybersecurity awareness training can be provided live, in-person and/or virtually.
- Alternatively, training can be offered on-demand, through an online training platform.
- Awareness activities can also be informal, such as through games and trivia incorporated into regular staff development days or team-building events.

New York State Comptroller
THOMAS P. DINAPOLI

8

Why?



- Cybersecurity awareness training is required to comply with New York State laws and regulations, and is often needed to qualify for cyber insurance policies.
- **Effective training is crucial to help prevent inadvertent data breaches, to protect IT systems from unauthorized access and use, and to recognize and properly report cybersecurity incidents that may occur.**

New York State Comptroller
THOMAS P. DINAPOLI

9

Assessing Training Effectiveness

Assessments should evaluate participant awareness before and after training, and could measure for:

- Enhancements in familiarity and understanding of cybersecurity concepts and terminology.
- Reinforcement of practices that help safeguard IT systems and data.
- Redirection from practices that may expose IT systems and data to cybersecurity risks and threats.



New York State Comptroller
THOMAS P. DINAPOLI

10

Enhanced Cybersecurity Knowledge

While it may not be necessary for all IT system users to know the technical details, it is important to be familiar with, recognize and understand the potential impacts of key cybersecurity concepts and terminology, such as the **common phases of a cyberattack**.



New York State Comptroller
THOMAS P. DINAPOLI

11

Common Phases of a Cyberattack

- Initial Access
- Gained Foothold
- Proliferation and Escalation
- Command and Control
- Objective Achievement



New York State Comptroller
THOMAS P. DINAPOLI

12

Cybersecurity Concepts and Terminology

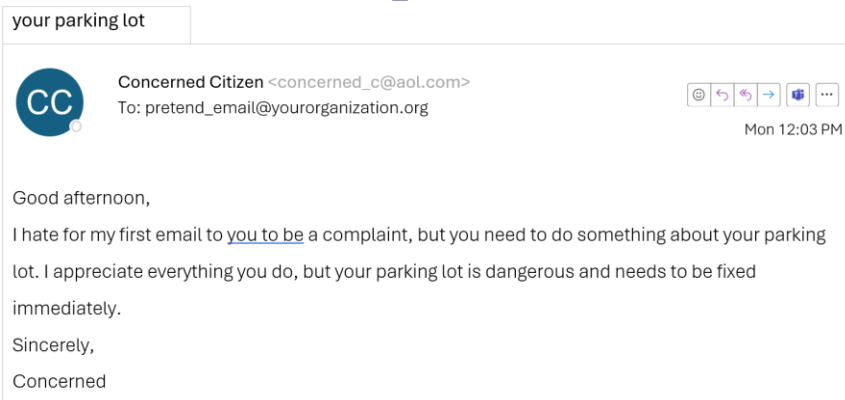
Cybersecurity awareness training content should be periodically updated to evolve along with the dynamic cyber threat landscape:

- For example, phishing emails may no longer contain obvious spelling mistakes as attackers leverage artificial intelligence (AI).



13

Phishing Example



Pictured on screen: A representation of a potential phishing email.
This is a representation for demonstration purposes, and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

14

Phishing Example

Free Wifi for your Organization!



Totally Real Internet Service Provider <real@trisp.org>

To: pretend_email@yourorganization.org

Cc: other_pretend_email@yourorganization.org



Mon 10:11 AM



Free Wifi for You!.docx
909 KB

Hello! We're very excited to announce that we are offering free wifi to organizations like yours!

Simply fill out the attached file and we'll get back to you with our free offer!

Warmest regards,

Totally Real Internet Service Provider

Pictured on screen: A representation of a potential phishing email.
This is a representation for demonstration purposes, and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

15

Phishing Example

John Smith Shared a Document



John Smith

To: pretend_email@yourorganization.org



Mon 10:05 AM



John Smith invited you to view a file

Here's the document that John Smith shared with you. "Budget 2024"

Pictured on screen: A representation of a potential phishing email.
This is a representation for demonstration purposes, and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

16

Other Common Cyberattack Techniques

Other than phishing, common cyberattack techniques include:

- **Credential Abuse:** Malicious actors buy and sell compromised credentials (i.e., usernames and passwords) on the “dark web” (a hidden portion of the Internet often used for its anonymity). The credentials may have been compromised in breaches of online shopping, gaming, or other non-work websites or applications.
- **Vulnerability Exploitation:** Many cyberattack techniques are categorized under this umbrella term. Vulnerability exploitation has been rapidly increasing as attackers leverage AI.

Source: Verizon, 2026 Data Breach Investigations Report

<https://www.verizon.com/business/resources/reports/2026-dbir-data-breach-investigations-report.pdf>

New York State Comptroller
THOMAS P. DINAPOLI

17

Types of Vulnerability Exploitation

- Password Spraying
- Falsified Login Portals
- Malicious Browser Extensions
- Ransomware

New York State Comptroller
THOMAS P. DINAPOLI

18

Password Spraying

A type of brute force attack where an attacker uses well-known and compromised passwords to attempt to gain access to specific user accounts in a network.

```
S C:\script\spray> Invoke-MSOLSpray -UserList .userlist.txt -Password ####
*) There are 40 total users to spray.
*) No spraying Microsoft Online.
*) Current date and time: 06/26/2026 10:41:22
*) SUCCESS! User1@domain OnMicrosoft.com : Password ####
*) SUCCESS! User2@domain OnMicrosoft.com : Password ####
*) SUCCESS! User3@domain OnMicrosoft.com : Password ####
```

Pictured on screen: A representation of a password spraying attack.
This is a representation for demonstration purposes, and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

19

Falsified Login Portals

Can you spot the difference?

An attack where a malicious actor makes a recreation of an entity's login portal, attempting to trick the entity's IT system users to login to the falsified portal.

Real Login Screen

<https://real-organization-login.com>



Organization Name Here

Falsified Login Screen

<https://real-organizatization-login.com>



Organization Name Here

Pictured on screen: Representations of a real and falsified login portal.
This is a representation for demonstration purposes, and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

20

Falsified Login Portals

An attack where a malicious actor makes a recreation of an entity's login portal, attempting to trick the entity's IT system users to login to the falsified portal.

Real Login Screen

<https://real-organization-login.com>



Organization Name Here

NetID

Password

Falsified Login Screen

[https://real-orga

nz

ation-login.com](https://real-orga<h1>nz</h1>ation-login.com)



Organization Name Here

NetID

Password

Pictured on screen: Representations of a real and falsified login portal.

This is a representation for demonstration purposes, and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

21

Malicious Browser Extensions

A type of attack where a malicious actor creates a seemingly useful browser extension, such as a PDF reader, and markets it to people on a legitimate browser extension store. Behind the scenes, the malicious extension gains control of your browser and can exfiltrate your data.



Absolutely Real PDF File Reader

[Install the plugin](#)

★★★★★ 5 | 14 reviews | 0 Favorites

Tool Introduction: Edit .PDF documents with our one-of-a-kind, definitely-not-malware app!

Update time: June 26, 2026

Pictured on screen: A representation of a malicious browser extension in a browser's app store.

This representation is for demonstration purposes and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

22

Ransomware

A type of malicious software (malware) that disrupts access to technology and, in some instances, threatens to disclose confidential or otherwise sensitive data to the public unless a ransom payment is made.



Pictured on screen: A representation of a ransomware alert message.

This is a representation for demonstration purposes, and is not real.

New York State Comptroller
THOMAS P. DINAPOLI

23

Measuring Knowledge Enhancements

- A popular way to measure training effectiveness is through attendee surveys. However, training effectiveness should not be measured based only on how well attendees *liked* the training.
- There may be fun and unique ways to measure and reinforce cybersecurity knowledge enhancements (e.g., quizzes, trivia).

New York State Comptroller
THOMAS P. DINAPOLI

24

The Knowing-Doing Gap

While most people know they shouldn't click on suspicious links in emails, phishing continues to be a successful attack method.

Source: Verizon, 2026 Data Breach Investigations Report
<https://www.verizon.com/business/resources/reports/2026-dbir-data-breach-investigations-report.pdf>

- This is referred to as the Knowing-Doing Gap.



25

Cybersecurity Awareness Practices

Effective cybersecurity awareness training should include, in addition to cybersecurity knowledge, best practices for helping to safeguard IT systems and data, such as:

- Checking if personal information has been compromised.
- Verifying computers' operating systems and applications are current and vendor-supported.
- Reporting, through expected procedures, when something unexpected occurs on a computer.

New York State Comptroller
THOMAS P. DINAPOLI

26

Indicators of Effective Cybersecurity Awareness

Effective cybersecurity awareness could look like:

- Using long, unique passwords and changing them immediately upon suspicion of compromise.
- Applying computer updates in a timely manner.
- Not interacting with phishing emails.
- Reporting suspicious computer events through proper procedures.

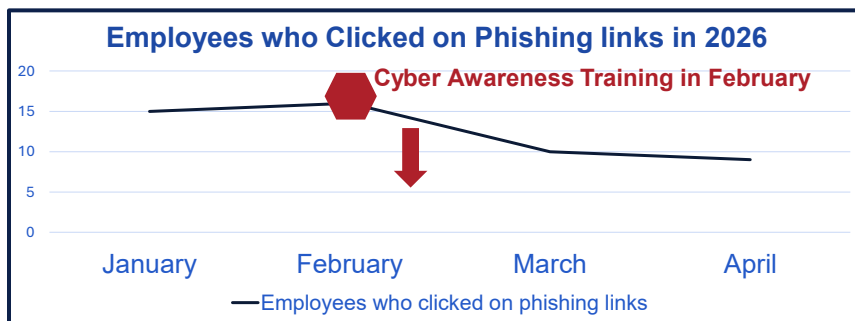


New York State Comptroller
THOMAS P. DINAPOLI

27

Measuring Cybersecurity Practices

Effective cybersecurity awareness training could lead to a decrease in IT system users who interact with phishing emails.



New York State Comptroller
THOMAS P. DINAPOLI

28

Cybersecurity Governance

- A local government's or school's governing board and chief executive officer should ensure a culture and tone that encourages cybersecurity awareness.
- **Don't wait for a cybersecurity incident or audit** to assess your IT system users' cybersecurity awareness. You can start today.
 - * Work with your IT department or service provider to establish and schedule periodic reports of IT system activity that can indicate cybersecurity awareness or improvement needs (e.g., counts of clicked email links, password changes or incidents reported).
 - * You may benefit from following a structured assessment tool, such as **LGSA's IT Governance Security Self-Assessment**.

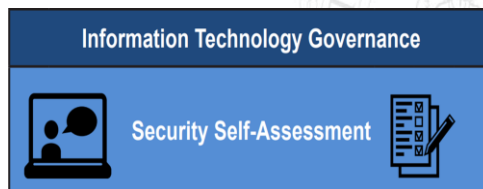
New York State Comptroller
THOMAS P. DINAPOLI

29

Information Technology Governance Local Government Management Guide

<https://www.osc.ny.gov/files/local-government/publications/pdf/it-governance-self-assessment-form.pdf>

<https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf>



New York State Comptroller
THOMAS P. DINAPOLI

30

New York Local Government and School Cybersecurity: A Cyber Profile

<https://www.osc.ny.gov/files/local-government/publications/pdf/nys-local-gov-school-cyber-profile.pdf>



New York State Comptroller
THOMAS P. DINAPOLI

31

Part 2 Preview

Cybersecurity Standards: A Case Study

- Part 2 of this webinar series will walk through a cybersecurity standards case study, demonstrating how an IT system administrator could select and use one of the many industry-vetted standards as a baseline when configuring, implementing and periodically evaluating an IT system's position in successfully defending against today's cybersecurity threats.
- IT system administrators generally need to evaluate, update and configure settings before a newly implemented IT system can be used securely. A variety of cybersecurity standards have been published and are available to help IT system administrators navigate this often-arduous task.

New York State Comptroller
THOMAS P. DINAPOLI

32

LGSA Resources

LGSA Cybersecurity Resources

Audit Reports	https://www.osc.state.ny.us/local-government/audits
Training	https://www.osc.state.ny.us/local-government/academy
Publications	https://www.osc.state.ny.us/local-government/publications
LGSA Help Line	localgov@osc.ny.gov or (866) 321-8503 or (518)-408-4934
ATU Cybersecurity Team	Muni-Cyber@osc.ny.gov or (518) 738-2639

New York State Comptroller
THOMAS P. DINAPOLI

33

Additional Resources

Additional Cybersecurity Resources

Center for Internet Security (CIS)	https://www.cisecurity.org/
Multi-State Information Sharing and Analysis Center (MS-ISAC)	https://www.cisecurity.org/ms-isac
NYS Division of Homeland Security and Emergency Services (DHSES)	https://www.dhSES.ny.gov/cyber-incident-response-team
NYS Office of Information Technology Services (ITS)	https://www.its.ny.gov/
NYS Police Computer Crime Unit (CCU)	https://troopers.ny.gov/computer-crimes

New York State Comptroller
THOMAS P. DINAPOLI

34

Additional Resources

Additional Cybersecurity Resources (continued)

United States Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/
United States Department of Justice (DOJ) Cybercrime	https://www.justice.gov/criminal-ccips
United States Federal Bureau of Investigation (FBI)	https://www.fbi.gov/investigate/cyber
United States National Institute of Standards and Technology (NIST)	https://www.nist.gov/cybersecurity

New York State Comptroller
THOMAS P. DiNAPOLI

35

Questions?

Contact Us

- LGSA Applied Technology Unit Cybersecurity Team
 - Muni-Cyber@osc.ny.gov
 - (518) 738-2639
- LGSA Help Line
 - 1-866-321-8503 or
 - 518-408-4934

New York State Comptroller
THOMAS P. DiNAPOLI



36

Thank you.



New York State Comptroller
THOMAS P. DINAPOLI

