Phishing in the Modern Day

Cybersecurity Awareness Month
October 2025

New York State Comptroller
THOMAS P. DiNAPOLI

Division of Local Government and School Accountability

Applied Technology Unit (ATU)
Information Systems Auditors

John Martin
Zachary Keenan

New York State Comptroller
THOMAS P. DiNAPOLI

Agenda

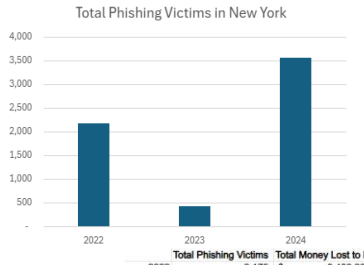
- Introduction to Phishing
- The Evolution of Phishing Attacks
- Real-World Examples
- Identifying Phishing Attempts
- Protecting Against Phishing
- Future Trends in Phishing
- Summary and Takeaways
- Cybersecurity Resources

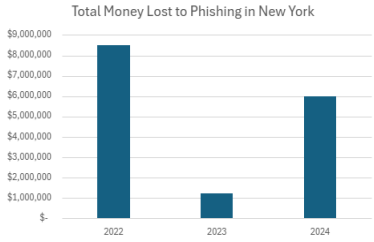
Introduction to Phishing

Phishing attacks use fake email messages or other techniques to trick a user into providing personal or sensitive information. A phishing email may provide links to a counterfeit website and request information such as name, password and account number.

The Evolution of Phishing Attacks

Early phishing relied on generic email messages and fake websites.





	Total Phishing Victims	Total Money Lost to Phishing	YOY Changes		Period change	
2022	2,175	$ 8,488,204				
2023	436	$ 1,229,605	-80%	-86%		
2024	3,557	$ 5,999,592	716%	388%	64%	-29%

Source: United States Federal Bureau of Investigation, Internet Crime Complaint Center's (IC3's) Annual State Reports, 2022-2024
https://www.ic3.gov/annualreport/reports

Modern Phishing Techniques

Business Email Compromise (BEC), also known as Email Account Compromise (EAC), is a cybercrime where threat actors impersonate legitimate business contacts to trick governments, schools and businesses into transferring funds or sensitive data.

Real-World Examples

- Email security bypass
- Road toll texts

Phishing Kits and the "Dark Web"

Phishing-as-a-Service (PhaaS) kits are known to be available to criminals on the "dark web."[1] These kits offer full phishing solutions, including templates, hosting and automation.

[1] The "dark web" is a hidden portion of the Internet, often used for its anonymity.

Artificial Intelligence (AI) and Phishing

Artificial Intelligence can be used to generate convincing emails with proper grammar and tone, allowing attackers to scale up their campaigns.

Identifying Phishing Attempts

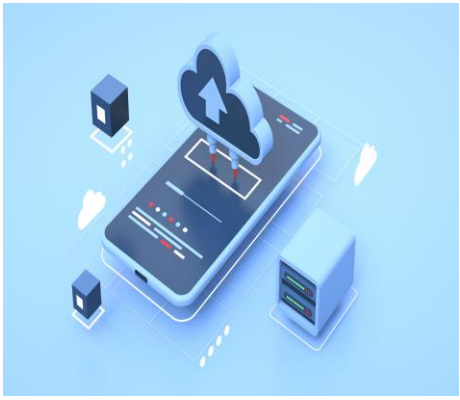
- Check sender email addresses carefully.
- Be wary of urgent and threatening language.
- Watch for improper spelling, grammar, and formatting.
- Always hover over links to verify destination locations.
- Even when the email is from someone you know, verify with them.

Protecting Against Phishing

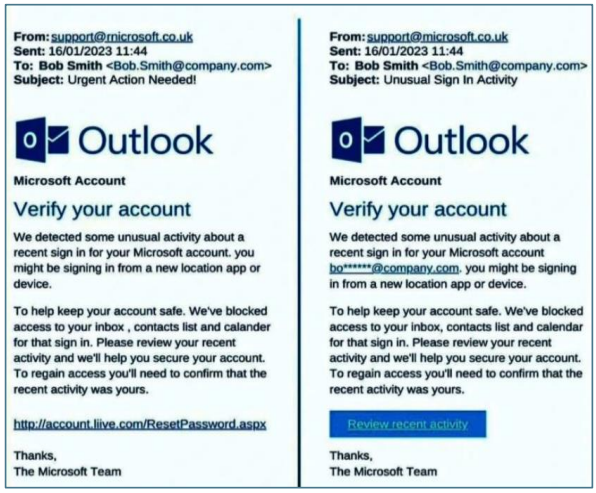
- Regular awareness training is essential.
- Implement multi-factor authentication (MFA) where possible.
- Consider leveraging enhanced protection such as email filters and anti-phishing tools.
- Establish clear procedures to report suspected phishing attempts.

Phishing on Mobile Devices

Mobile devices may hide a link's full web address, making it more difficult for users to spot phishing attempts.



Can You Spot the Phish?



From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft Team

Did You Spot the Phish?

FAKE

From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft Team

Future Trends in Phishing

- Phishing attacks will continue to become increasingly more sophisticated.
- AI-generated “deepfake” video and audio are emerging threats.
- “Internet of Things” (IoT) devices, commonly referred to as smart devices (e.g., smart boards, thermostats, light bulbs, security cameras), may become phishing targets.

Advanced and Emergent Phishing Schemes

TOADs, Vishing, Smishing, Quishing Oh My!

- Telephone-Oriented Attack Delivery (TOAD)
- Voice-Based (Vishing)
  - Calling the IT Help Desk
  - Pretending to be the IT Help Desk
- Short Message Service (SMS)-Based (Smishing)
  - Text messaging
  - MFA fatigue
- Quick-Response (QR) Code-Based (Quishing)

Telephone-Oriented Attack Delivery

TOAD

- Starts with an email purporting to represent a legitimate organization.
- Could be an unexpected invoice or credit balance, for example.
- Provides instructions to call the organization at a number used by the attacker.
- Upon calling, the attacker persuades the caller to disclose sensitive information.

Other Forms of Vishing

- Calling the IT Help Desk
  - Attackers may pretend to be an employee who lost their phone or laptop and need assistance accessing their account.
  - Relies on publicly-posted information and/or organizational knowledge (e.g., employee vacation schedules).
- Pretending to be the IT Help Desk
  - Attackers may call victims and guide them to download remote access software.
  - Software may or may not be legitimate.

Text Messaging and MFA Fatigue

Smishing

- Target personal and work cellphones
  - Attackers attempt to persuade victims to click on links to malicious websites.
- Induce MFA fatigue
  - Attackers flood victims with notifications that can become annoying.
  - Attempts to wear them down, and ultimately approve the attackers' login.
  - Often used in combination with other techniques.

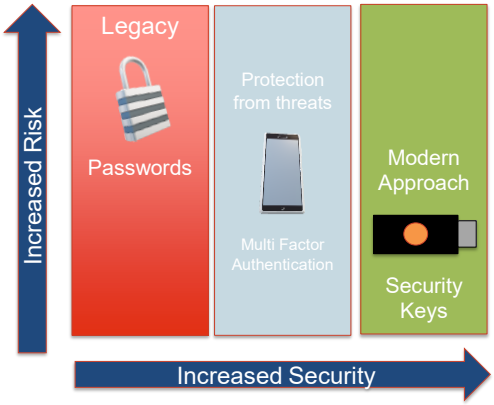
QR Code Phishing

Quishing

- Attackers may send QR codes by email or text message.
  - This may bypass some email filters.
  - It may also bypass other defenses if a user takes a picture of a QR code with their personal phone.

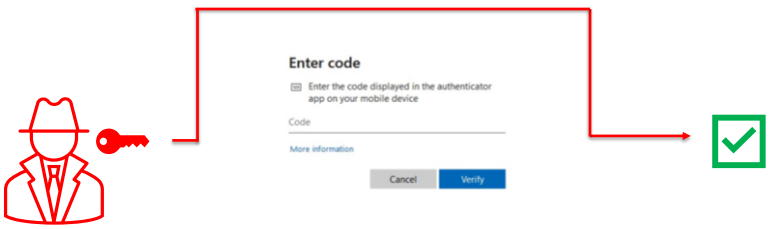
The Modern Approach to Defense

- MFA may not always be effective.
- One future strategy is through passkeys.

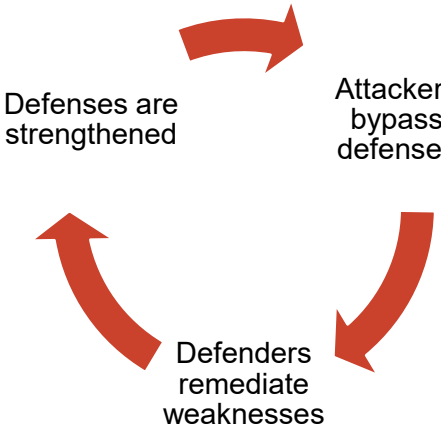


MFA Bypass Techniques

- MFA is not a silver bullet.
  - For example, attackers can steal MFA tokens (e.g., one-time passwords).
- Such bypass techniques can be mitigated with secure MFA design and implementation.



The Fight Will Continue



- **Attackers will find new ways.**
  - AI-assisted phishing
  - IT Help Desk impersonations
  - MFA fatigue and bypass
- **Defenders need to keep up.**
  - Passphrases and passkeys
  - Secure MFA design and implementation
  - Regular awareness training and vigilance

Summary and Takeaways

- Regular awareness training is essential.
- Phishing remains a dynamic and evolving threat.
- Layered defenses are key.
- Always report suspicious activities.

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 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

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

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

Additional Resources

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

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

Thank You