NEW YORK STATE | Homeland Security and Emergency Services

PREVENTING PHISHING ATTACKS IN NYS COUNTY GOVERNMENTS

CYBER INCIDENT RESPONSE TEAM (CIRT)

SAFEGUARDING NYS'S STATE, LOCAL, TRIBAL, & TERRITORIAL (SLTT) SYSTEMS, SERVICES, AND INFRASTRUCTURE

JANUARY 7, 2026

DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES (DHSES)

"We provide leadership, coordination, and support to prevent, protect against, prepare for, respond to, recover from, and mitigate disasters and other emergencies."

DHSES CYBER INCIDENT RESPONSE TEAM (CIRT)

Multi-Unit Collaboration Approach

- OCT Critical Infrastructure Unit
- Partnership with New York Division of Military and Naval Affairs

Identify / Prevent / Protect

- Training, exercises, workshops
- Proactive outreach

Respond / Recover / Mitigate

- Incident response and digital forensics
- Remediation assistance and guidance

WHO DOES DHSES CIRT SERVE?

- Counties - 57
- Cities - 62
- Towns - 932
- Villages - 532
- Special Districts - 11,000
- Schools/BOCES - 4,448
- Non-Executive Agencies -9
- Public Authorities - 583

WHAT IS PHISHING?

WHAT IS PHISHING?

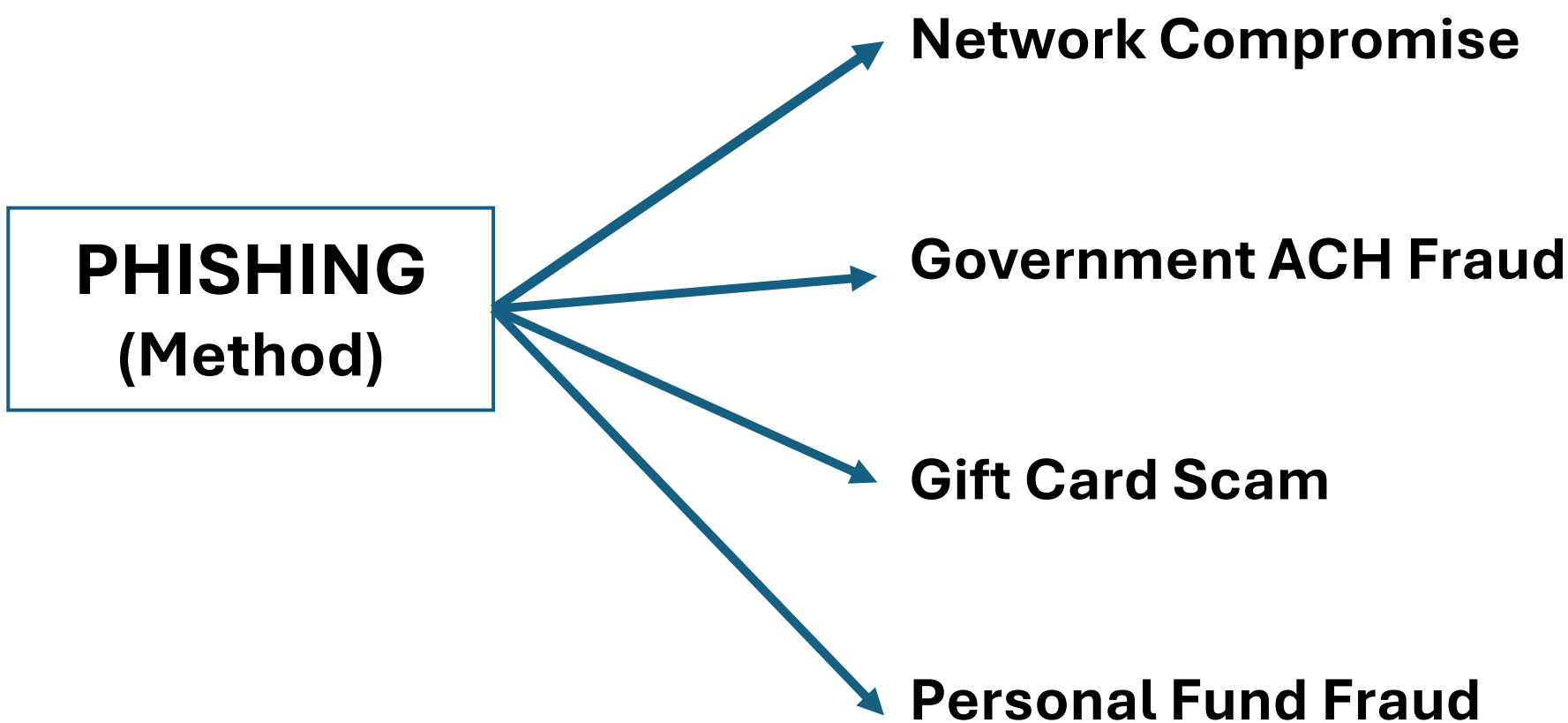
- Attackers impersonate legitimate individual or organization and interact with a target entity to get that entity to take an action (typically provide information or send money)

- Spear phishing makes the attacks highly targeted and personalized (looks like a company you know, a name you know, with information that looks familiar)

- Government is the SECOND MOST phished sector

METHOD AND OUTCOME

EXAMPLE OUTCOMES



PHISHING IN THE ERA OF AI

- Phishing and social engineering attacks up by **42%** in **2024**
- Phishing was observed in **14%** of **10,747** breaches in 2025
- Analysis of **34.6** billion cybersecurity events shows that **4.7** billion of them were phishing
- Synthetically generated content in malicious emails **doubled** over past two years
- **1,000** phishing emails can be created in **< 2** hours and for as little as **$6**

Source: Global Cybersecurity Outlook 2025

METHODS OF PHISHING

Social Engineering

- Manipulation to obtain information or to get people to perform an action which helps a perpetrator achieve their goal

Business Email Compromise

- Email scam that attempts to steal money/sensitive data

AI-Generated Phishing

- AI-generated phishing emails have higher click-through rate (54%) than likely human-written phishing emails (12%)
- Voice phishing (vishing) is up 442% between the first and second half of 2024
- Text message phishing (smishing) is increasingly used to deliver baits

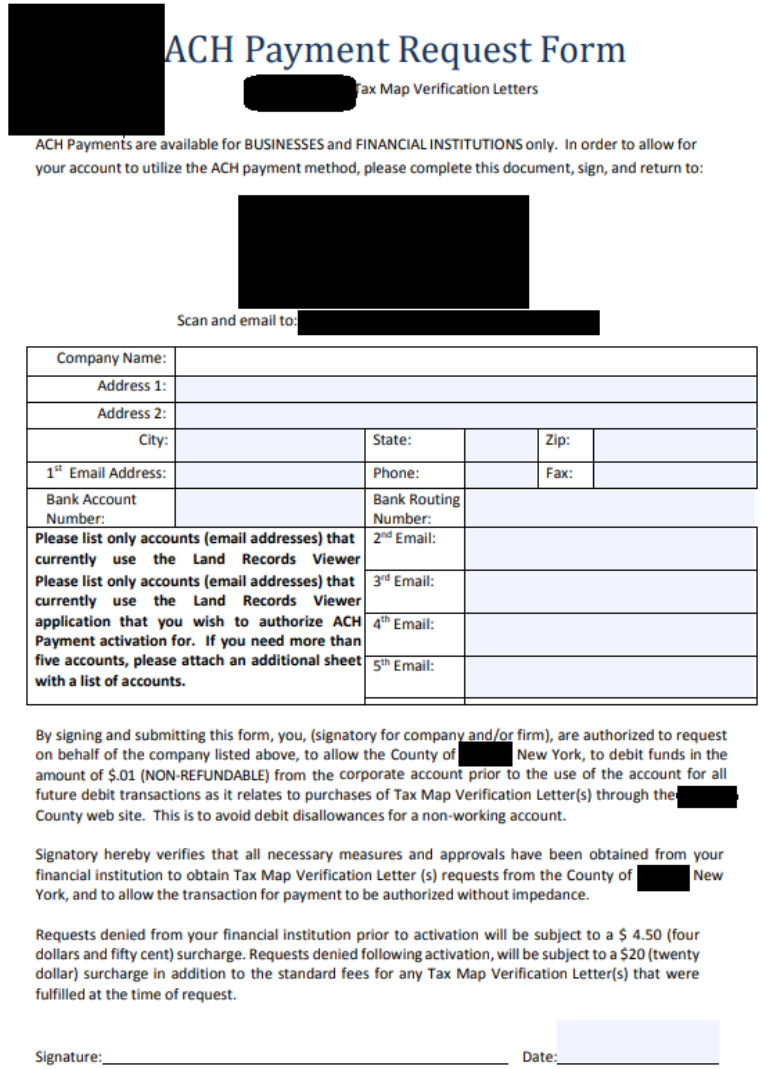
Source: The Human Factor 2025

EXAMPLE

- **Impersonation:** Hackers used publicly available information from LinkedIn to identify a current MGM employee and assume their identity
- **Social Engineering:** The attackers impersonated an employee during a call to the IT help desk, tricking the help desk into granting access to internal systems
- **Data Exfiltration:** The hackers exfiltrated sensitive client and business data, leading to a significant revenue loss and a wave of lawsuits
- **Lesson Learned:** The incident highlights the importance of employee education and security awareness to prevent such breaches

EXAMPLE

- Web forms collect your most sensitive data
- Customer credentials
- Financial records
- **44%** of organizations suffered confirmed data breaches through these forms in the past two years
- **88%** experienced at least one web form security incident in the past 24 months



[redacted] ACH Payment Request Form

[redacted]ax Map Verification Letters

ACH Payments are available for BUSINESSES and FINANCIAL INSTITUTIONS only. In order to allow for your account to utilize the ACH payment method, please complete this document, sign, and return to:

[redacted]

Scan and email to: [redacted]

Company Name:					
Address 1:					
Address 2:					
City:		State:		Zip:	
1st Email Address:		Phone:		Fax:	
Bank Account Number:		Bank Routing Number:			
Please list only accounts (email addresses) that currently use the Land Records Viewer Please list only accounts (email addresses) that currently use the Land Records Viewer application that you wish to authorize ACH Payment activation for. If you need more than five accounts, please attach an additional sheet with a list of accounts.		2nd Email:			
		3rd Email:			
		4th Email:			
		5th Email:			

By signing and submitting this form, you, (signatory for company and/or firm), are authorized to request on behalf of the company listed above, to allow the County of [redacted] New York, to debit funds in the amount of $.01 (NON-REFUNDABLE) from the corporate account prior to the use of the account for all future debit transactions as it relates to purchases of Tax Map Verification Letter(s) through the [redacted] County web site. This is to avoid debit disallowances for a non-working account.

Signatory hereby verifies that all necessary measures and approvals have been obtained from your financial institution to obtain Tax Map Verification Letter (s) requests from the County of [redacted] New York, and to allow the transaction for payment to be authorized without impedance.

Requests denied from your financial institution prior to activation will be subject to a $ 4.50 (four dollars and fifty cent) surcharge. Requests denied following activation, will be subject to a $20 (twenty dollar) surcharge in addition to the standard fees for any Tax Map Verification Letter(s) that were fulfilled at the time of request.

Signature:_____ Date:_____

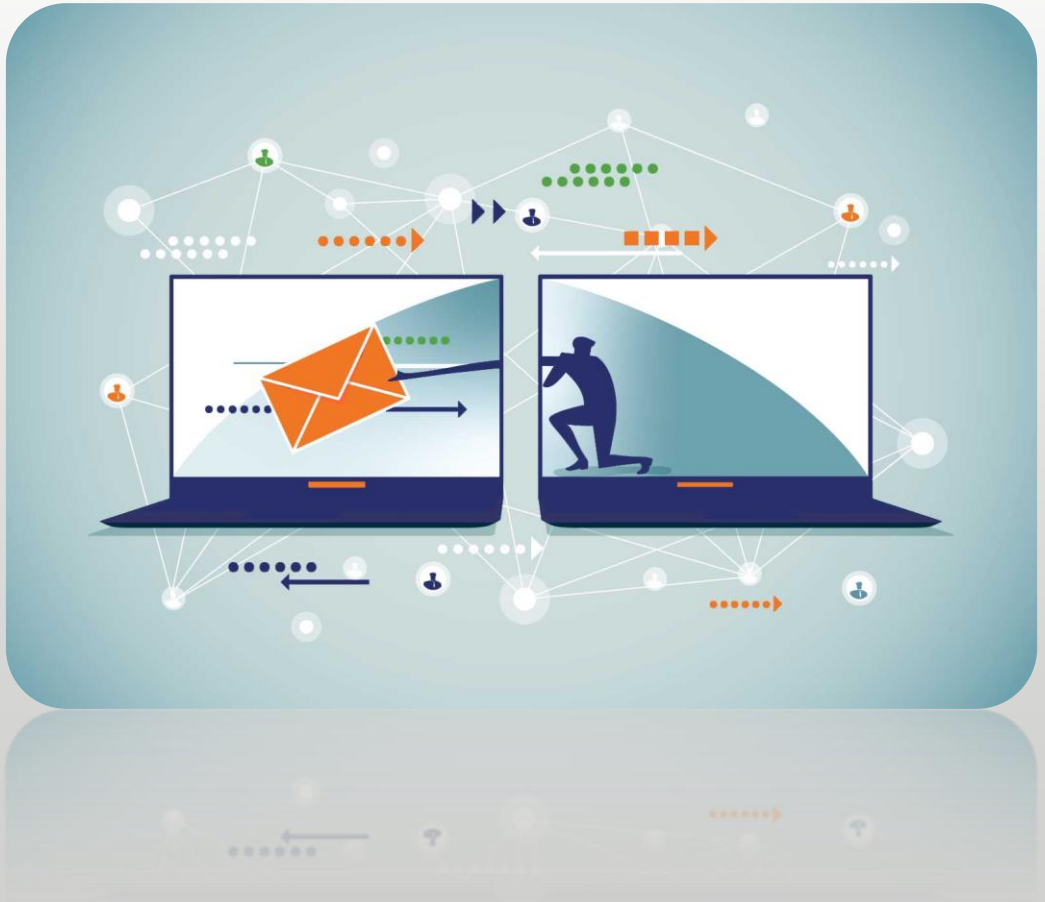
Source: 2025 Data Security and Compliance Risk Report

AI GENERATED CALLS AND VIDEOS

- **Deepfake Voice Attack, a**ttackers used AI to clone the voice of a CEO, leading to unauthorized transactions totaling approximately $18 million.
- **The Com**, a threat actor group that successfully breached several Australian banks by spoofing vendor payment approvals
- A **March attack targeting** a logistics firm used deepfake calls to authorize ransomware deployment, freezing shipments across the country

Source: Right-Hand Cybersecurity

PHISHING & ACH FRAUD



EXAMPLE

1

[Attacker]
Performs reconnaissance on victim organizations and related vendors

2

[Victim]
Attacker gains access to a trusted email account

3

[Inside Victim's Email]
Attacker monitors financial conversations and often hides real messages with inbox rules while looking for official vendor forms

4

With a look-a-like account, the **Attacker** generates malicious payment instructions then joins the conversation

5

Money is sent to the fake account before the **Victim** or anyone else notices

EXAMPLE

From: John Smith <john.smith@madeupcompany.com>
Sent: Monday, October 20, 2025 8:13 AM
To: Finance <finace@yourcompany.com>
Subject: Invoice #2025-MUC-004
Attachment: Invoice #2025-MUC-004

Hello,

Attached is invoice #2025-MUC-004 for $122,350 for the site works completed on September 28, 2025. Payment is due in 14 days.

Bank details are on the invoice PDF.

Kind regards,

John Smith
Finance Manager
Made Up Company

From: John Smith <john.smith@madeupccompany.com>
Sent: Tuesday, October 21, 2025 2:13 PM
To: Finance <finace@yourcompany.com>
Subject: Invoice #2025-MUC-004
Attachment: Invoice #2025-MUC-004

Hello,

Sorry for the short notice. Our bank account changed. Please pay the invoice immediately to the new account below to avoid late fees.

Account Number: 8675309
Routing Number: 10001110101

If you need to confirm, reply to this email.

Kind regards,

John Smith
Finance Manager
Made Up Company

WHAT ARE THE WAYS TO PROTECT?

THREE LAYERS OF SECURITY

PEOPLE

- Resist the urge to act immediately on urgent-sounding requests
- Actively look for and scrutinize suspicious email indicators
- **VERIFY** sources before taking an action (e.g., clicking links)
  - When money is involved, **VALIDATE** all transactions
- Use strong, unique, non-default passwords (>14 characters) and keep them safe
- Flag and report suspicious correspondence

PROCESS

- Have a written and enforced process for verification and validation before all ACH Transactions
- Use of technology/software only with IT department's knowledge/approval (= no shadow IT)
- Prioritize patching and audit checks if patching is automated (no updates = vulnerabilities)
- Implement a robust, automated, and regularly tested backup strategy.
  - Must include off-site and offline and have separate access credentials
- Restrict administrative privileges to a minimal number of IT personnel
  - Regularly review and audit user permissions
- Manage the third-party (vendor) risk

TECHNOLOGY

- Use phishing-resistant multi-factor authentication (MFA) on virtual private networks (VPNs)
- Invest in multiple layers of cyber protection, not just one tool
- Implement specialized spam filters can reduce the number of phishing emails
- Incorporate denylists or cyber threat intelligence feeds into firewalls rules to block known malicious sources
- Implement an endpoint detection and response (EDR) solution to monitor for and block malicious activity on end user devices
- Have a segmented network to divide your network into smaller, isolated sections

NYS DHSES
CIRT SERVICES

CIRT PROACTIVE AND RESPONSIVE CYBERSECURITY SERVICES

- Cyber Incident Response and Digital Forensics
- Cybersecurity Risk Assessments (Rapid and Full)
- Phishing and Training Exercises
- Tabletop Exercises
- Capability Workshops
- Penetration Testing
- Cybersecurity Grant Program
- Statewide Cyber Shared Service Program

All DHSES CIRT services are provided at no cost to non-executive agencies, local governments and public authorities.

CIRT PHISHING AND TRAINING EXERCISE PROCESS

- Simulated phishing attacks that help assess end user training
- Training modules issued to workforce
- Reports and metrics provided to customer

Goals:

- Help local governments train and educate their users
- Prevent compromises and infections

Want Phishing Training Services?
CIRT@DHSES.NY.GOV

CIRT PHISHING AND TRAINING EXERCISE PROCESS

Simulated phishing campaign that accounts for the organizational mission

- Campaign are custom designed to test user's susceptibility to account compromise and clicking potentially malicious links
- Often runs over three weeks (week 1 – first phishing campaign, week 2-training, week 3 – second phishing campaign)

Training modules

- Includes topics such as introduction to phishing, avoiding dangerous links, data entry phishing, security on mobile devices, etc.
- Completion progress is tracked

- To **REQUEST DHSES CIRT ASSISTANCE** for a cyber incident, CALL1-844- OCT-CIRT (1-844-628-2478)
- To **REPORT** a cyber incident, ransom payment, or a ransom payment explanation, visit https://www.dhses.ny.gov/cybersecurity-incident-and-ransom-payment-reporting
- To **ASK A QUESTION** about cyber reporting, email cyber.reporting@dhses.ny.gov
- To **REQUEST DHSES CIRT SERVICES** (phishing training, rapid risk assessments, pentests, tabletop exercises, cyber capability workshops) email CIRT@dhses.ny.gov.

Federal Internet Crime Complaint Center

https://www.ic3.gov/

NEW YORK STATE | Homeland Security and Emergency Services

PREVENTING PHISHING ATTACKS IN NYS COUNTY GOVERNMENTS

CYBER INCIDENT RESPONSE TEAM (CIRT)

SAFEGUARDING NYS'S STATE, LOCAL, TRIBAL, & TERRITORIAL (SLTT) SYSTEMS, SERVICES, AND INFRASTRUCTURE

JANUARY 7, 2026