WBASNY
WOMEN'S BAR ASSOCIATION of the STATE OF NEW YORK

Presents

Cybersecurity Overview: Identifying and Protecting Against Risks

October 14, 2025
1:00 pm - 2:00 pm

Presenters: Courtney Kanopka, M.S.C.S.
Lisa Noroian, Esq.

CYBERSECURITY OVERVIEW: Identifying and Protecting Against Risks (October 14, 2025)

PRESENTERS:

COURTNEY KANOPKA – CHIEF INFORMATION SECURITY OFFICER

NEW YORK STATE OFFICE OF COURT ADMINISTRATION

DIVISION OF TECHNOLOGY AND COURT RESEARCH

Common Risks to You and Your Environment

Risks have increased because we are more mobile and fully dependent on tech than ever before

- Mobile Devices, Constant Internet/Internet of Things

Specific Risks

- Social Media use/personal information publicly accessible
- Email attachments/embedded URLs
- Phishing
- Personal USBs
- Ransomware, Malware/Drive-by Malware
- Credential Harvesting
- 3rd party VPNs

Current Cyber Threat Landscape

Opportunistic

Ransomware most impactful

Phishing/Spear Phishing (Credential Harvesting)

Malspam (emails with malware attachments or links)

Exploitation of exposed or vulnerable ports and services

Nation-States Threat Actors

Disruptive operations (e.g., DDoS)

Destructive operations (e.g., Wipers)

Supply chain compromises (e.g., SolarWinds)

Information Gathering

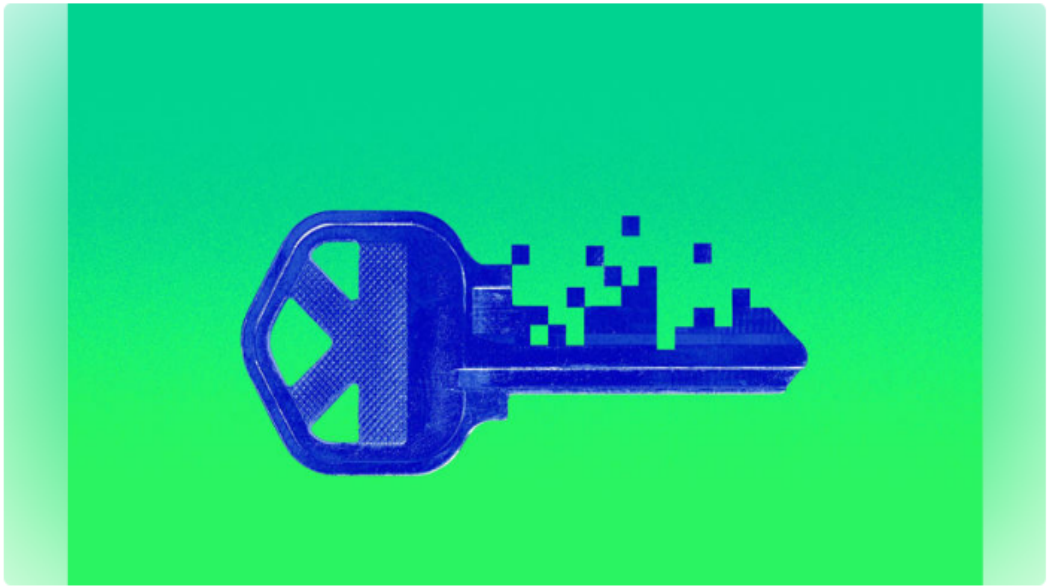
3rd Party VPNs Used for NYS Cyberattack (China)

US arrests man allegedly behind enormous botnet that enabled cyberattacks and fraud

Story by Lauren Feiner • 1w • 2 min read

MARKETS TODAY ...

INX ▼ -0.08% DJI ▼ -0.20% COMP ▲ +0.08%



3rd Party VPNs Used for NYS Cyberattack (China)

> It's a scheme that "reads like it's ripped from a screenplay," according to one Commerce Department official. Thirty-five-year-old Chinese national YunHe Wang allegedly helped run an international botnet that deployed VPN programs to infect more than 19 million IP addresses around the world.

After distributing malware through programs such as MaskVPN and DewVPN, Wang allegedly operated the botnet and sold access to the compromised IP addresses, according to the Department of Justice. The department says his customers then went on to commit their own crimes under the concealment of the proxied addresses.

The botnet, known as 911 S5, "facilitated cyber-attacks, large-scale fraud, child exploitation, harassment, bomb threats, and export violations," according to a statement from Attorney General Merrick Garland. The US worked with international partners to dismantle the operation, which infected computers in almost 200 countries, according to Federal Bureau of Investigation Director Christopher Wray.

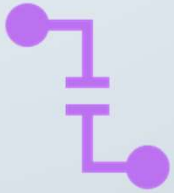
Gaining Initial Access

Compromised Credentials to gain initial access

Credential harvesting (fake Microsoft website)

Brute Force attempts

Compromised Passwords



Problematic against services like 3rd party private Virtual Private Networks (VPNs)

Threat actors authenticate like normal users to access enterprise resources

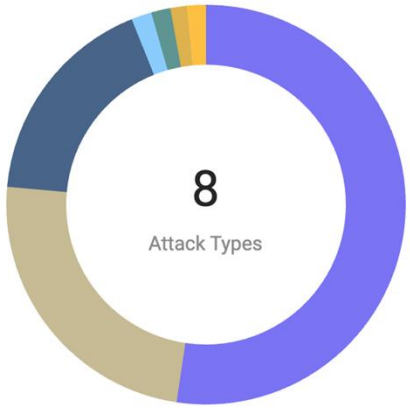
Email Daily Averages: NYS Courts Example

Inbound Email Messages	**380,000**	
Phishing/Malware/ Spam Blocked by Automation	40,000	12%
Phishing/Malware/ Spam Undetected	400	1%

Email Attack Trends Last 30 Days

Trending Attacks ⓘ

Over the entire 90-day period, Abnormal detected Phishing: Credential as the most common attack type for your organization. For reference, the most common attack type in the previous 90-day period was Phishing: Credential.



Attack Types	Attack Count ⓘ	vs. Previous Period ⓘ
Phishing: Credential Attacker tricks victim into giving away their online credentials to unauthorized parties	10303 (52%)	+2098 +26%
Other Non-categorized attacks	4736 (24%)	-832 -15%
Scam Advance fee fraud and similar scams	3444 (18%)	-453 -12%
Malware Attacker attempts to deliver malicious payload	323 (2%)	+41 +15%
Social Engineering (BEC) Attacker impersonates employee to establish rapport with victim recipient and convince victim to engage in actions such as changing direct deposit information, paying fake invoice, buying gift cards, or performing another task	308 (2%)	-152 -33%
Invoice/Payment Fraud (BEC) Attacker impersonates a vendor, partner or well-known brand and asks recipient for fake invoice/payment	261 (1%)	+64 +32%
Internal-to-Internal Attacks (Email Account Takeover) Attacker compromises an employee's account and delivers other internal employees fake invoices, credential phishing, and other malicious content	2 (0%)	-2 -50%
Spam Untargeted and unsolicited communications	301 (2%)	+200 +198%

Phishing incidents

Phishing

- Uses ongoing crises or World events
- Spear Phishing, Vishing, Smishing, etc
- Business email compromises (BEC)

Cyber threat actors are always adapting

- Use of QR codes to bypass email phishing protections and email security tools
- Use of OneNote files starting in 2023

Phishing vs. spear phishing vs. whaling

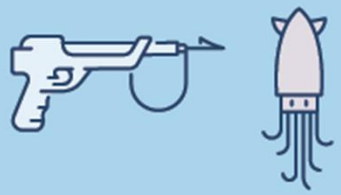
Whaling is a specific type of spear phishing, and spear phishing is a specific type of phishing. Learn the differences below.

Phishing

A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

Spear phishing

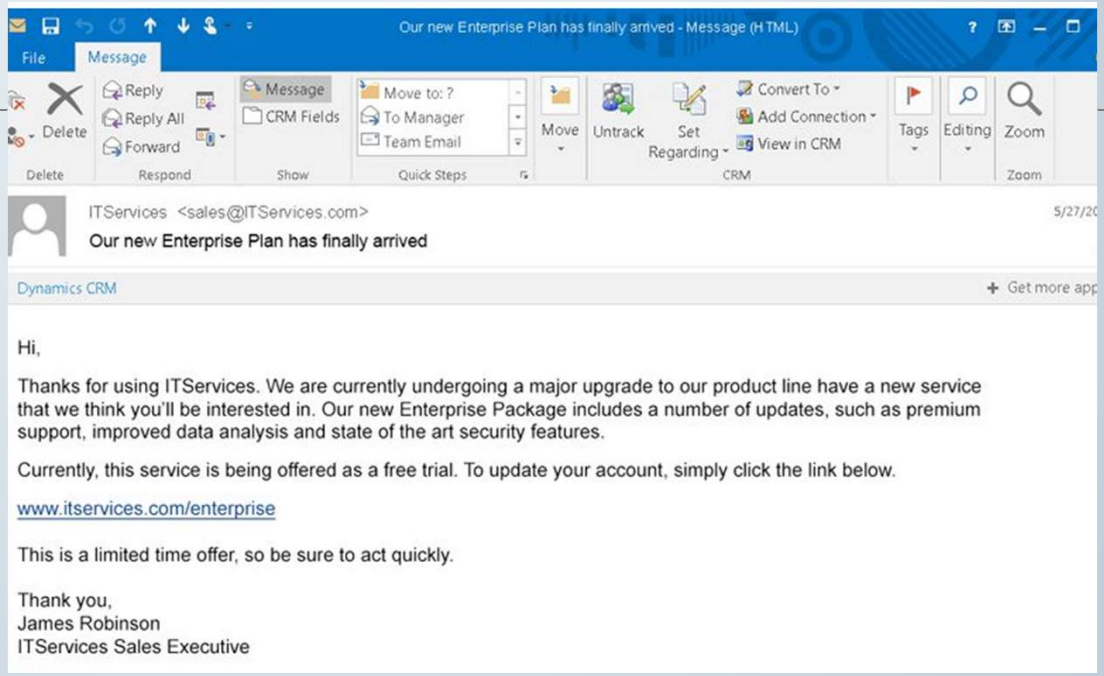
A type of phishing that targets individuals.



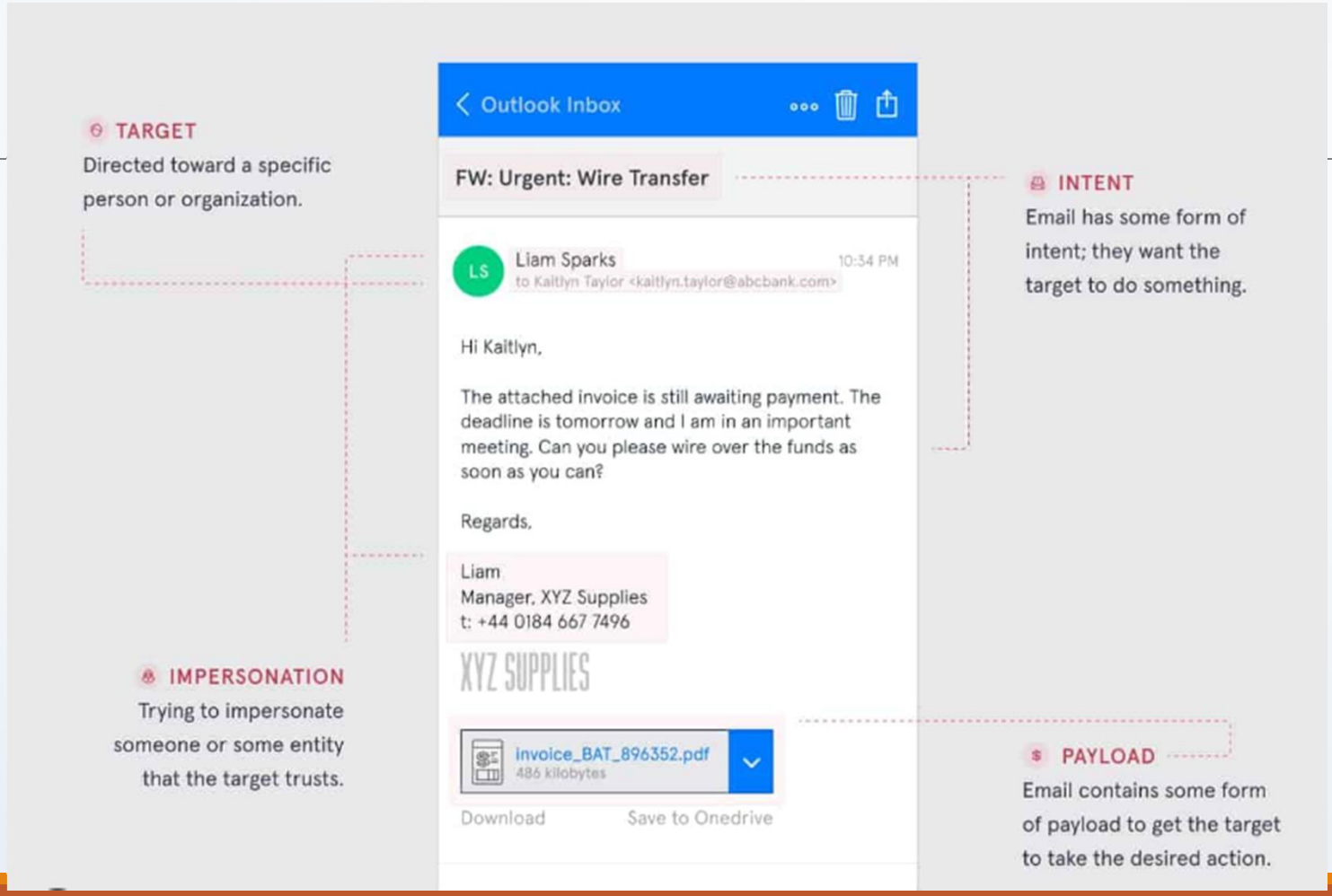
Whaling

A form of spear phishing that targets high-ranking victims within a company.

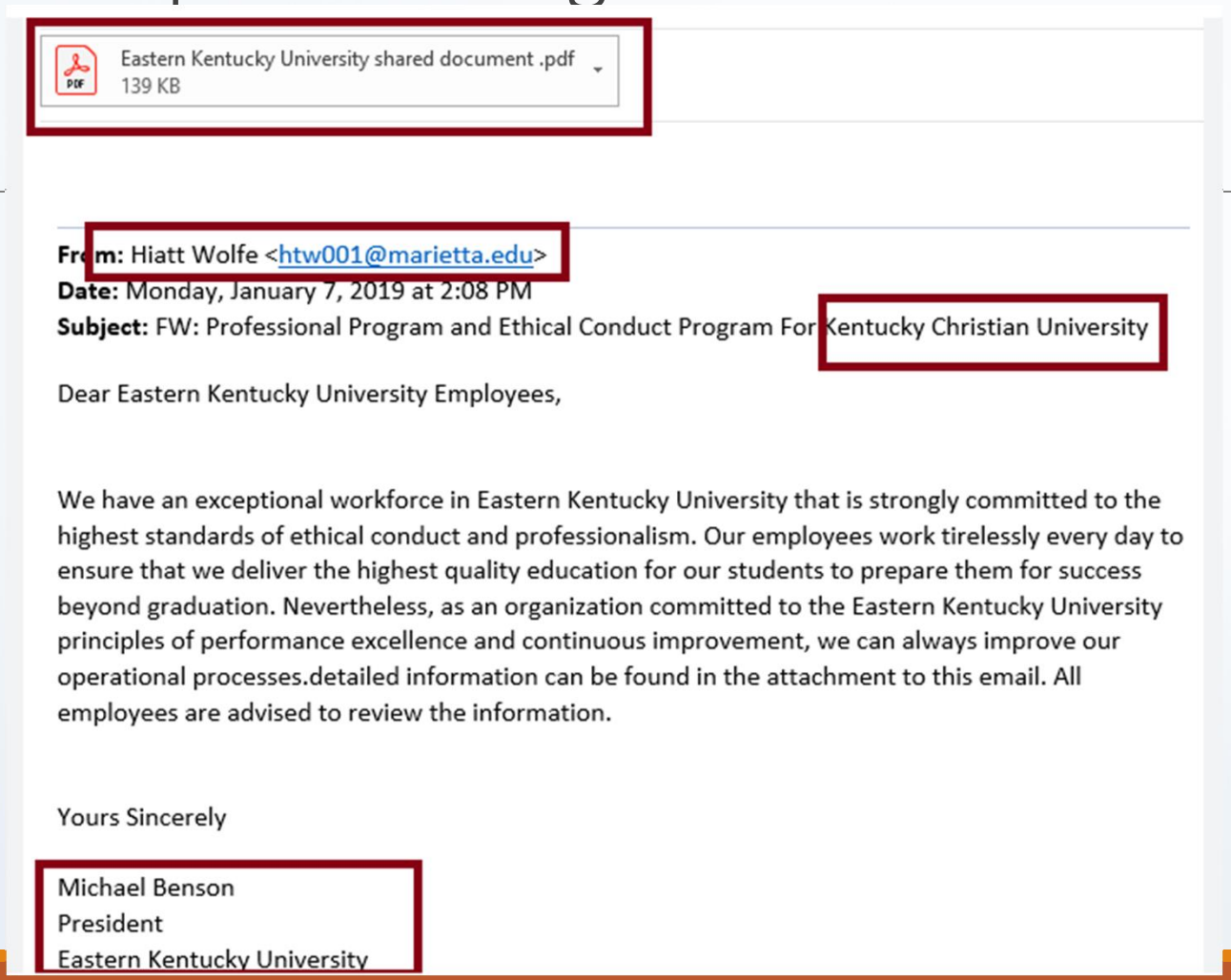
Example: General Phishing E-mail



Example: Spear Phishing E-Mail



Example: Whaling E-Mail



Eastern Kentucky University shared document .pdf
139 KB

From: Hiatt Wolfe <htw001@marietta.edu>
Date: Monday, January 7, 2019 at 2:08 PM
Subject: FW: Professional Program and Ethical Conduct Program For Kentucky Christian University

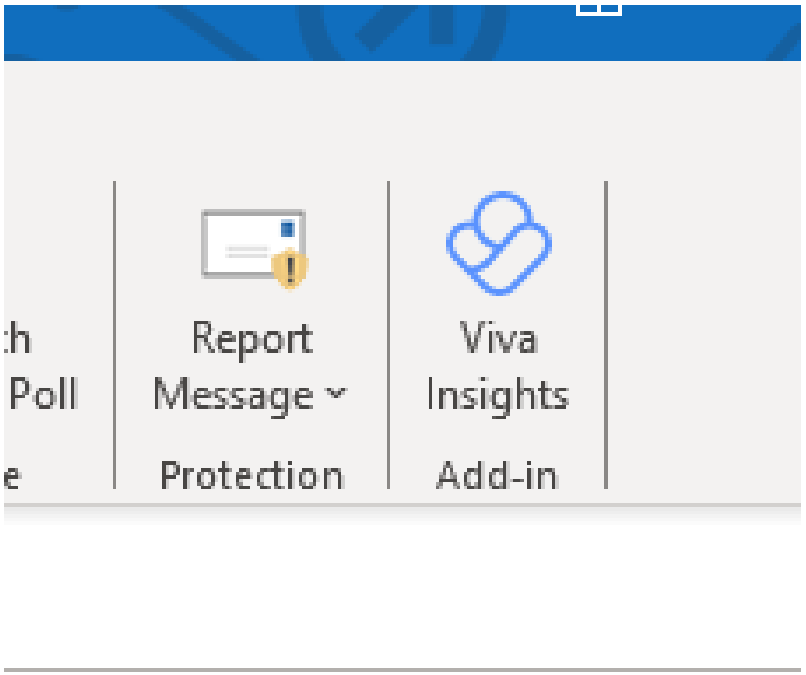
Dear Eastern Kentucky University Employees,

We have an exceptional workforce in Eastern Kentucky University that is strongly committed to the highest standards of ethical conduct and professionalism. Our employees work tirelessly every day to ensure that we deliver the highest quality education for our students to prepare them for success beyond graduation. Nevertheless, as an organization committed to the Eastern Kentucky University principles of performance excellence and continuous improvement, we can always improve our operational processes.detailed information can be found in the attachment to this email. All employees are advised to review the information.

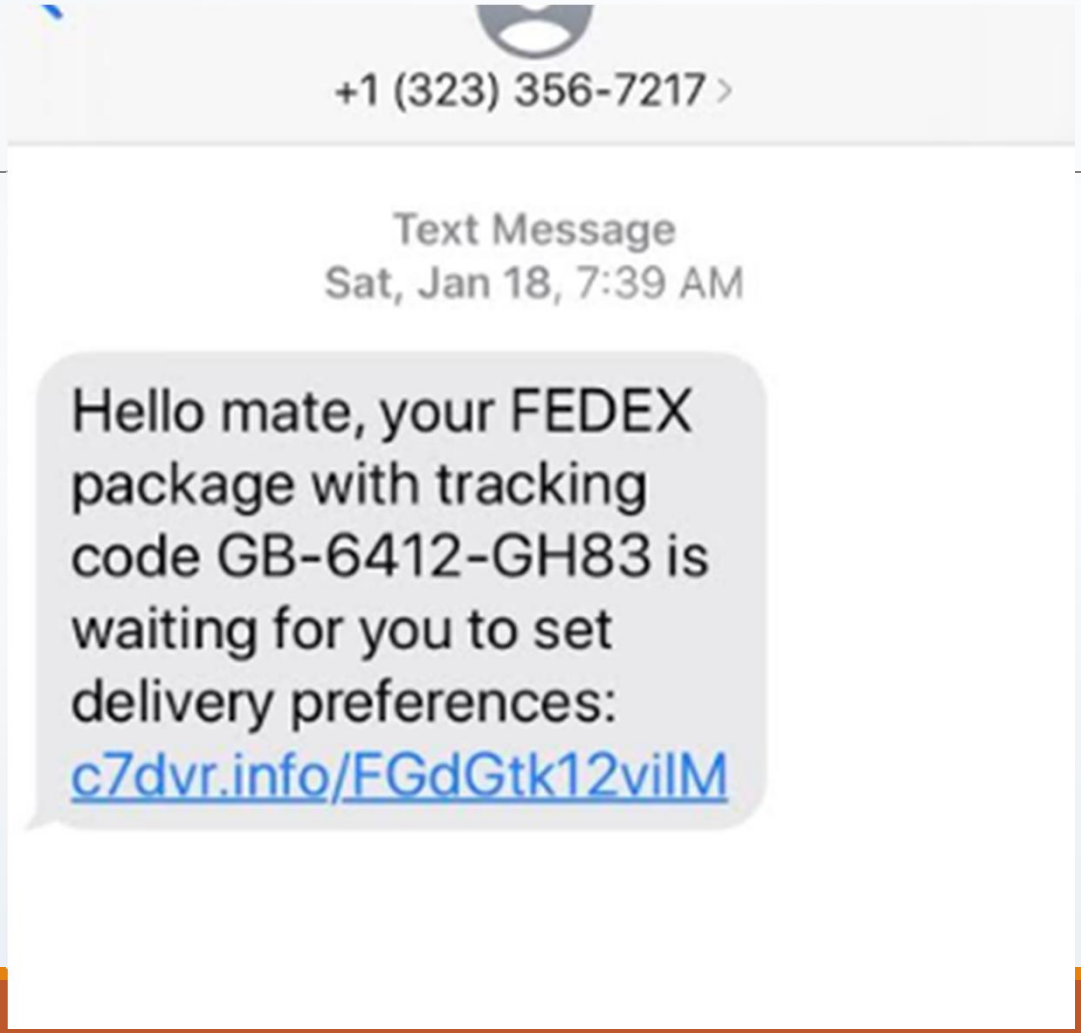
Yours Sincerely

Michael Benson
President
Eastern Kentucky University

How to report A Suspicious Message in Outlook



Example: Smishing Message (SMS)



AI Generating Malicious emails

Subject: You have an issue with your billings info
From: Support <support@teeela.zendesk.com>
To: [redacted]
Reply-to: Support <support+id550989@teeela.zendesk.com>
Date: Aug 11, 2023, 7:03pm ET

N

UPDATE REQUIRED ACCOUNT IS ON HOLD

Dear Customer,

We hope you have been enjoying your Netflix experience so far! As a valued member of the Netflix community we wanted to remind you that your current subscription is coming to an end soon. To avoid any disruption in your streaming experience, we kindly request that you renew your subscription promptly.

To renew your subscription, simply follow these easy steps:
1. Log in to your Netflix account here.
2. Choose your preffered plan and enter your payment details.

Once you have completed the renewal process, you can continue enjoying your favorite movies and TV shows without interruption. Remember that with Netflix, you have access to an ever-growing library of content, including exclusive originals, award-winning movies, and popular TV series from around the world. Plus, you can watch on multiple devices and switch plans or cancel at anytime.

If you need any assistance or have questions about your subscription, our Customer Support team is available 24/7 to help. You can reach us through the live chat on our website, or you can call us at 1-800-123-4567.
Thank you for choosing Netflix as your streaming partner. We've dedicated to making your viewing experience better every day, and we hope you continue to enjoy the world of entertainment we offer.

Dear Customer,

We hope you have been enjoying your Netflix experience so far! As a valued member of the Netflix community we wanted to remind you that your current subscription is coming to an end soon. To avoid any disruption in your streaming experience, we kindly request that you renew your subscription promptly.

To renew your subscription, simply follow these easy steps:
1. Log in to your Netflix account here.
2. Choose your preffered plan and enter your payment details.

Once you have completed the renewal process, you can continue enjoying your favorite movies and TV shows without interruption. Remember that with Netflix, you have access to an ever-growing library of content, including exclusive originals, award-winning movies, and popular TV series from around the world. Plus, you can watch on multiple devices and switch plans or cancel at anytime.

If you need any assistance or have questions about your subscription, our Customer Support team is available 24/7 to help. You can reach us through the live chat on our website, or you can call us at 1-800-123-4567.
Thank you for choosing Netflix as your streaming partner. We're dedicated to making your viewing experience better every day, and we hope you continue to enjoy the world of entertainment we offer.

Recent Major Data Breaches Impacting NYS

SIGNIFICANT US DATA BREACHES

- **January 2021: U.S. Courts System put out a statement acknowledging** that its Case Management/Electronic Case Files system, had been compromised as part of the massive breach. As a result, procedures for filing highly sensitive documents were changed so that they could only be handed in via paper documents, a secure electronic device or through a secure computer system. Investigation by the Justice Department.

- **February 2023: U.S. Marshals System** was victim of a ransomware attack. The affected system contained "law enforcement sensitive information, including returns from legal process, administrative information and personally identifiable information pertaining to subjects of U.S.M.S. investigations, third parties and certain U.S.M.S. employees."

- **August 2023**: **Gadsden County Florida Court System**. Law enforcement investigating a data breach involving Gadsden County court records. 2nd Judicial circuit said that initial assessments show some of the records contained "personal identifying information." In the process of investigating and remediating.

Preventing Inadvertent Data Breaches

Limit internet access for your staff

- If not needed for the job, do not grant
- Incorporate automated blocking/Proxy
- Review reports of use, incorporate policies

Loss or compromise of a device

- Data Encryption
- Do not store files on local devices/hard drives
  - Use Cloud storage or local network storage
- Do not leave mobile devices unattended

Protect Personal Identifiable Information (PII)

- Review storage and access in case management systems – audit, limit access, permissions by role
- If it must be sent, use secure email, other sharing options (cloud sharing with permissions)

Keep in mind physical security (locked server, locked devices, cameras, paper)

Require cyber awareness training

* Stay informed and up to date about threats, schemes, etc.

Check out, for example: FBI's Internet Crime Complaint Center www.ic3.gov; and Federal Trade Commission www.ftc.gov

* Keep your computer, software, browser, plug ins, antivirus software all up to date.

* Maintain different passwords especially for accounts that contain private, confidential, or more sensitive information.

* Be careful before clicking links or attachments.

Data Breach Laws

All 50 States, as well as the US Territories, have their own data breach statutes that governs what is considered a data breach, and response and reporting obligations in the event of a breach.

Examples – **Information Security Breach and Notification Act** N.Y. Gen. Bus. Law § 899-aa (state and businesses/organizations); NY STATE TECH § 208 (state entities, not the Judiciary)

- Requirement to disclose any breach to any resident of NYS whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization ("Breach of Security").

NY Shield Act.

ADDITIONAL DUTIES OF ATTORNEYS

STATUTES

ETHICAL RULES AND GUIDELINES

ETHICS OPINIONS

Steps to take:

1. Data security policy at your firm
2. Train staff on mitigating risks
3. Use strong passwords
4. Encrypt, encrypt, encrypt
5. Secure your communications
6. Consider access control
7. Conduct regular reviews
8. Vet vendors carefully
9. Plan for the worst
10. Bump up your law firm's mobile security

(from Clio in ABA, Law Technology Today (2024))

NYS Attorney General – law firm fined (March 2023)

In an investigation, NY Attorney General secured $200,000 in penalties from a law firm that represented New York City area hospitals due to data security failures. The law firm violated state law and HIPAA for failure to adhere to advanced data security practices as they maintained sensitive private information of patients (dates of birth, social security numbers, health insurance information, medical history/treatment) and/or health treatment information. An attacker exploited a weakness in the law firm's Microsoft Exchange email server. The firm had not timely applied patches, which were released by Microsoft several months earlier.

NYS Attorney General Enforcement Examples

Wegmans (2022)

- Number of affected individuals: Over 3 million (830,000 New York residents)
- AG allegations: failure to secure cloud storage, secure user passwords, regularly conduct security testing of cloud assets, maintain long-term logs of cloud assets and maintaining information derived from customer driver's licenses without reasonable business purpose
- Settlement: $400,000 & must adopt new security measures

- **Carnival Cruise Line (2022)**
  - Number of affected individuals: 6,575 New York residents
  - Investigation: multistate investigation into Carnival's email security practices and compliance with state breach notification statutes
  - Settlement: $1.25 million (New York received $44,000) & must adopt new security measures

- **Sports Warehouse, Inc. (2023):**
  - Number of affected individuals: 136,000 New York residents
  - AG allegations: failure to adopt reasonable practices to protect personal information; specifically, failure to encrypt private information on its servers and adopt appropriate deletion practices
  - Settlement: $300,000

Cyberattack Incident Checklist handled by OCA Tech

Verify incident with impacted organization

Determine if any users have access to our systems and/or we have any data exchange(s) in place. If so:

- **Immediately disable all user access**
- **Immediately disable all data exchanges**

Immediate internal notification to technical team, DCAJ, impacted court/office, OCA Executive Director

Meet with IT leaders of impacted organization, keep in regular contact

Provide disabled usernames, exchanges to impacted organization

Provide "Data Breach Remediation Report Requirements" to impacted organization. Upon resolution:

- **Impacted entity must send validated 3rd party report, confirming incident is remediated**
- **Password resets on all accounts**
- **Re-enable data exchanges**
- **Notify appropriate court oversight offices**
- **Finalize internal incident report**

What to do if your environment is breached

In New York, Organizations Must Follow the NYS Data Breach Notification Law which requires notice to:

- **NYS Department of State**
- **NYS Division of State Policy**
- **NYS Office of the Attorney General**
- **Use NYS OAG Data Breach Submission Portal**

Questions ?

RESOURCES:

FBI's Internet Crime Complaint Center
www.ic3.gov

The Internet Crime Complaint Center (IC3) is the central hub for reporting cyber-enabled crime. It is run by the FBI. For more information about the IC3 and its mission, see About Us.

Brochures - Internet Crime Complaint Center (IC3)

2024_IC3Report.pdf

IC3's Home page Warning:

"SCAMMERS ARE IMPERSONATING THE IC3

The IC3 does not work with any non-law enforcement entity, such as law firms or crypto services, to recuperate lost funds or investigate cases. The IC3 will never directly contact you for information or money. Please see this PSA for more information.

If you are approached by someone impersonating or claiming to work with IC3 or find a website impersonating the IC3, please file a complaint with the information. Be sure to include the website link in your complaint."
S IC3

FEDERAL TRADE COMMISSION
www.ftc.gov

Cybersecurity for Small Business | Federal Trade Commission

Scams | Consumer Advice

FTC also has warning: **" Scammers Are Impersonating the FTC**

The FTC will never threaten you, say you must transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone. That's a scam.

Report it at ReportFraud.ftc.gov"

ATTORNEY CLE Requirements:

Continuing Legal Education Cybersecurity and Data Privacy Requirement Rules (§ 1500.2).

Attorneys must complete training in "Cybersecurity, Privacy and Data Protection-Ethics," or "Cybersecurity, Privacy and Data Protection-General."

Ethics category focuses on lawyers' ethical responsibilities regarding electronic data and communication, and includes understanding ethical obligations, protecting confidential and privileged client information, addressing risks (i.e.: data breaches, cyberattacks, inadvertent disclosures). Attorneys are also required to supervise employees, vendors, and third parties to ensure compliance with these ethical standards. Client counseling on data protection policies, client consent regarding electronic data storage, addressing privacy implications. Unauthorized disclosure of confidential information (i.e.: social media, other electronic means).

General category pertains to the practice of law, can include technological aspects of protecting client and law office electronic data and communication; cybersecurity features of technology used; network, hardware, software and mobile device security; preventing, mitigating, and responding to cybersecurity threats, (i.e.: cyberattacks and data breaches); vetting and assessing vendors and other third parties relating to policies, protocols and practices; applicable laws relating to cybersecurity (including data breach laws) and data privacy; law office cybersecurity, privacy and data protection protocols and policies.

A Selection of Ethics Opinions

ABA Formal Opinion 483 Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Duty of Competence Model Rule 1.1 – a lawyer shall provide competent representation to a client, maintain requisite knowledge and skill. This includes understanding technologies (attorneys and staff).

Attorney obligation to take reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

What kind of data breach? When “material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer’s ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.” (Formal Opinion 483)

Under Model Rules 5.1 and 5.3, lawyers and law firm must have measures in place ensuring all lawyers and staff in the firm will conform to the Rules of Professional Conduct.

Breach of client information: 1) is suspected or detected, pursuant to Rule 1.1, the lawyer must “act reasonably and promptly to stop the breach and mitigate damage resulting from the breach.” (Formal Opinion 483) and 2) must use reasonable efforts to determine what occurred during the breach.

Duty of confidentiality: reasonable efforts (factors are not exclusive): “the sensitivity of the information…the likelihood of disclosure if additional safeguards are not employed…the cost of employing additional safeguards…the difficulty of implementing the safeguards, and… the extent to which the safeguards adversely affect the lawyer’s ability to represent clients.” (Formal Opinion 483).

There are also ethical duties pertaining to providing notice of a breach (which may be different for current and for former clients).

Selected NYSBA Ethics Opinions

Opinion 842 (September 10, 2010) discusses the use of online systems to store client confidential information. It advises attorneys to take reasonable steps to ensure that the online storage provider has effective security measures in place and to periodically reconfirm that the provider's security measures remain effective given advances in technology.

Opinion 1019 (August 8, 2014), addresses confidentiality and remote access firm’s electronic files.

Opinion 1240 (April 11, 2022) addresses the ethical implications of sharing client contact information stored on a smartphone with third-party applications. It emphasizes that attorneys must ensure that no human being will view confidential client information and that the information will not be sold or transferred to additional third parties without the client's consent.

NYC Bar Association Ethics Opinion 2024-3 (July 18, 2024) Ethical Obligations Relating to a Cybersecurity Incident.

References Rules 1.1, 1.3, 1.4, 1.6, 1.7(a)(2), 1.9, 1.15, 1.18, 4.1, 5.1, 5.3, 8.4. Discussion includes but not limited to: lawyers' obligation of technological competence (Rules 1.1, 1.3, 1.6) to safeguard client confidential data and information; statutory, regulatory, or contractual obligations to notify clients and others; in addition ethical obligation under Rule 1.4 to promptly notify current clients when a cybersecurity incident occurs that cybersecurity incident occurs that is a "material development" in a representation, and allow client to make an informed decision regarding the representation if likely unable to meet material obligations to client; cyber-extortion, ransoms, dealing with law enforcement and Rules 1.6, 1.9 and 1.18, and Rule 1.7 new or continuing representation if a breach occurred (conflicts).

A Selection of New York Statutes

1. **New York Health Information Privacy Act**

Working alongside HIPAA, the purpose of this act is to "create a legal framework for residents to reclaim and retain control of their healthcare information." This Act aims to achieve its stated purpose by requiring all regulated entities, service providers and other third parties to safeguard the security, confidentiality, and integrity of regulated health information, and by giving residents rights similar to individuals' rights provided by HIPAA.

2.**The NYS Information Security Breach and Notification Act** -

Comprised of State Technology Law §208 (state entities) and General Business Law §899-aa.

- Entities or businesses owning or licensing computerized data containing private information must notify affected New York residents of breaches.
- Businesses must also notify the NYS Attorney General, Division of State Police, and Department of State – Division of Consumer Protection.
- State entities are subject to separate notification requirements.

899-aa information, click here: infosecbreach.pdf

3.**Stop Hacks and Improve Electronic Data Security Act – Shield Act** - signed into law July 2019, amended in 2024). It amended New York's 2005 Information Security Breach and Notification Act to strengthen and expand New York's data security laws (in definitions of data breach and scope of protective measures organizations to take). SHIELD Act | New York State Attorney General

The website explains the significance of the law, definitions of private information covered, information about safeguards required to be taken (reasonable administrative, technical AND physical safeguards), obligations of a business if a breach occurs, penalties and exceptions.

THANK YOU - to Alexander Slizewski, Esq., Lewis Brisbois, One Riverfront Plaza, Suite 800, Newark, NJ 07102, for contributions to the materials.

Kathy Hochul
Governor

NEW YORK STATE OF OPPORTUNITY.
Division of Consumer Protection

Rossana Rosado
Secretary of State

A Division of the New York Department of State

Advocating for and Empowering New York Consumers

Consumer Assistance Hotline: 1-800-697-1220 / https://dos.ny.gov

FACTSHEET FOR BUSINESS

NYS Information Security Breach and Notification Act

N.Y. Gen. Bus. Law. Section 899-aa

What types of information are covered by the law?

Computerized personal information that contains a combination of name, Social Security number, driver's license number, account number, or credit and debit card number.

When is the law triggered?

When a person has acquired computerized data containing personal information without valid authorization.

How does my business determine that information has been aquired without valid authorization?

Your business should look for any one of the following: (1) that information is in the physical possession and control of an unauthorized person such as a lost or stolen computer or other device; (2) evidence of unauthorized download or copied information; (3) evidence of unauthorized use of the information.

Good faith acquisition of personal information for a business purpose does not trigger provision of the law so long as the information is not used or subject to unauthorized disclosure.

When does my business need to disclose a data breach?

The disclosure must be made in the most expedient time possible and without unreasonable delay upon determination of a data breach. However, law enforcement may require that you delay notification of a data breach if they believe that its disclosure will impede a criminal investigation.

How does my business disclose that there has been a data breach to New York residents?

Notification can be made by any one of the following methods: written, electronic (but only with consent of the person you are notifying) or by telephone.

A business could also use substitute notice, if it can demonstrate to the New York State Attorney General that the cost of providing notice would exceed $250,000 or that the affected class of people to be notified exceeds 500,000 persons. You may also use substitute notice if you do not have sufficient contact information for those who have been affected.

Substitute notice consists of all of the following: e-mail, conspicuous posting on your website, and notification to major statewide media.

(Continued)

What information must be contained in the notice to New York residents?

Notice shall contain a description of the types of information believed to have been acquired by a person without valid authorization and your contact information so that affected New York State residents may contact you about the data breach.

When does my business need to notify the credit reporting agencies?

If there are more than 5,000 New York residents affected by the security beach at one time, your business must also notify consumer reporting agencies as to the timing, content and distribution of the notices.

Which New York State entities need to be informed?

If New York residents are affected, then your business is required to inform:

1. The New York State Office of the Attorney General;
2. New York State Division of State Police; and,
3. The New York Department of State's Division of Consumer Protection.

New York State
Office of the Attorney General
SECURITY BREACH NOTIFICATION
Consumer Frauds &
Protection Bureau
120 Broadway - 3rd Floor
New York, NY 10271
Fax: 212-416-6003
E-mail: breach.security@ag.ny.gov

New York State
Division of State Police
New York State Intelligence Center
SECURITY BREACH NOTIFICATION
31 Tech Valley Drive, Second Floor
East Greenbush, NY 12061
Fax: 518-786-9398
E-mail: risk@nysic.ny.gov

New York
Department of State
Division of Consumer Protection
SECURITY BREACH NOTIFICATION
One Commerce Plaza
99 Washington Ave., Suite 640
Albany, NY 12231
Fax: 518-473-9055
E-mail:
security_breach_notification@dos.ny.gov

To download the NYS Information Security Breach and Notification Act Reporting form, please visit:
https://its.ny.gov/eiso/breach-notification