

Cybersecurity:  
Practical Considerations  
and Best Practices

Continuing Legal  
Education

2023 New York Statewide  
Civil Legal Aid  
Technology Conference

• **Presenters:**

- Courtney Kanopka, Deputy Chief Information Security Officer
- Christine Sisario, Chief Information Officer
- New York State Office of Court Administration
- Division of Technology and Court Research

• **Moderator:**

- John Greiner, Esq.
- Founder and President
- Just-Tech, LLC



*"As the digital demands on the public sector have grown, so have the risks. Leaders must shift their focus to prioritize cybersecurity and defend against cyber attacks. It has never been more important to stop breaches before they happen. Security must now be at the center of every organization."*

---

## Threat Perspective: Common Risks to You and Your Environment

- Risks have increased because we are more mobile and fully dependent on tech than ever before
  - VPN, Mobile Devices, Constant Internet/Internet of Things, Social Media
- Specific Risks
  - Malware/Drive-by Malware
  - Ransomware
  - Social Media use/personal information publicly accessible
  - Email attachments/embedded URLs
  - Credential Harvesting
  - Phishing



# 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.



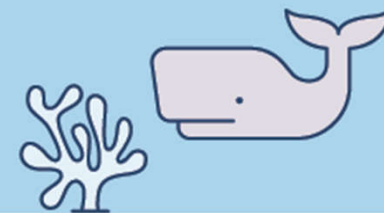
## Spear phishing

A type of phishing that targets individuals.

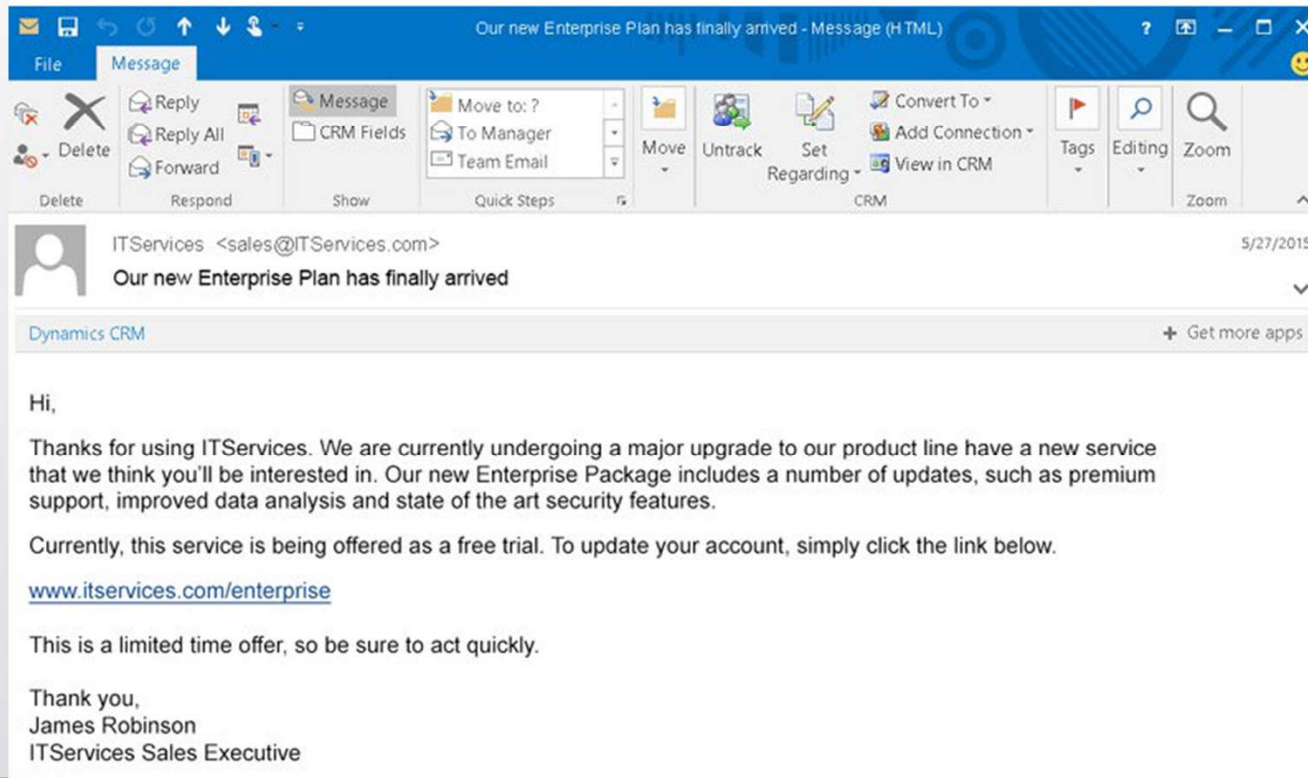


## Whaling

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



# Example General Phishing E-mail



# Example Spear Phishing E-Mail

The diagram illustrates a spear phishing email with four key components highlighted by red dashed lines and labels:

- TARGET:** Directed toward a specific person or organization. (Points to the recipient's name, Kaitlyn Taylor, in the email header.)
- IMPERSONATION:** Trying to impersonate someone or some entity that the target trusts. (Points to the sender's name, Liam Sparks, and his title, Manager, XYZ Supplies.)
- INTENT:** Email has some form of intent; they want the target to do something. (Points to the urgent subject line, "FW: Urgent: Wire Transfer", and the body text requesting a wire transfer.)
- PAYLOAD:** Email contains some form of payload to get the target to take the desired action. (Points to the attached PDF file, "invoice\_BAT\_896352.pdf", which is the malicious payload.)

The email content shown is:

Outlook Inbox

**FW: Urgent: Wire Transfer**

Liam Sparks  
to Kaitlyn Taylor <kaitlyn.taylor@abcbank.com> 10:34 PM

Hi Kaitlyn,

The attached invoice is still awaiting payment. The deadline is tomorrow and I am in an important meeting. Can you please wire over the funds as soon as you can?

Regards,

Liam  
Manager, XYZ Supplies  
t: +44 0184 667 7496

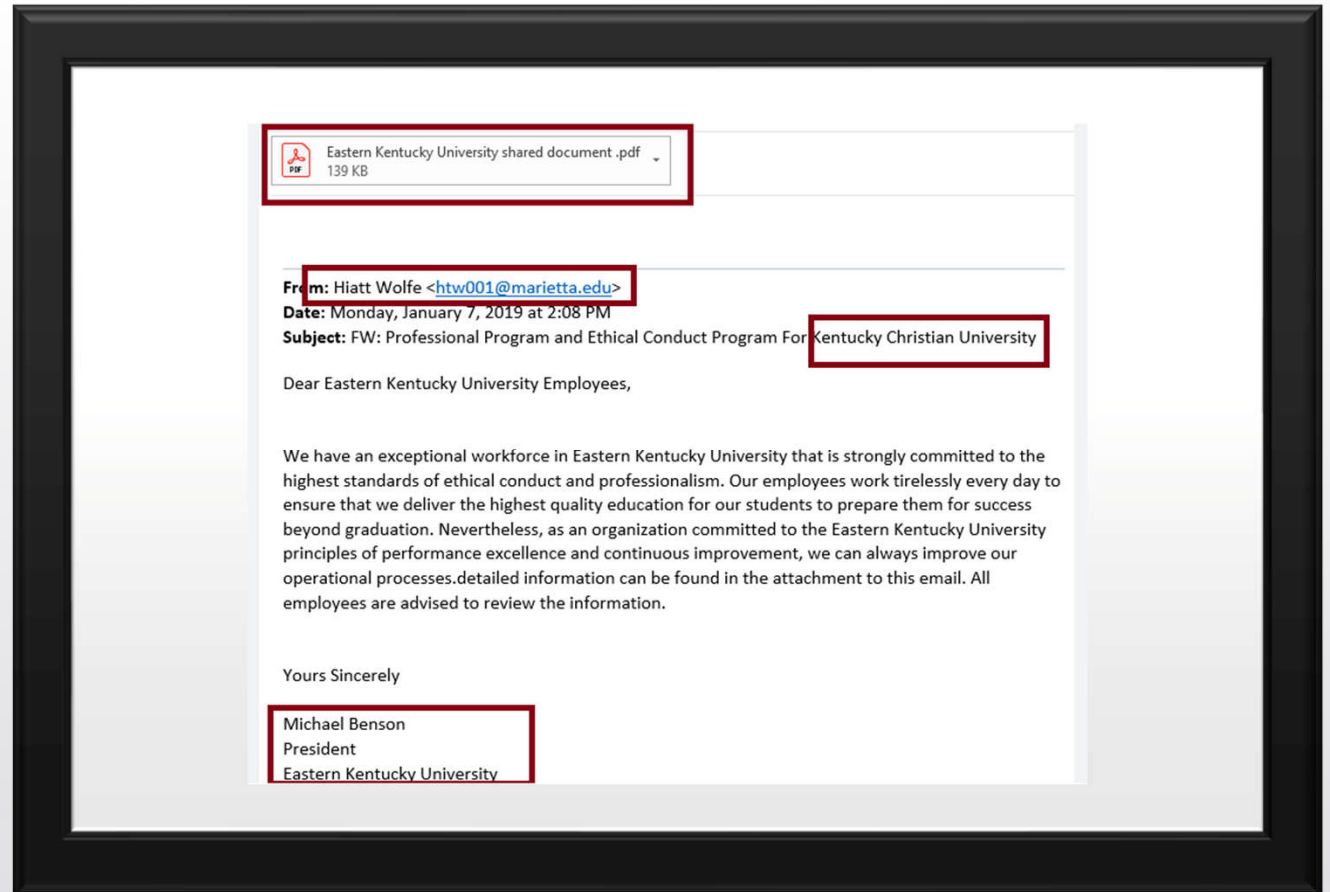
XYZ SUPPLIES

invoice\_BAT\_896352.pdf  
486 kilobytes

Download Save to OneDrive



# Example Whaling E-Mail



---

## No- and Low-Cost Options to Prevent Inadvertent Data Breaches



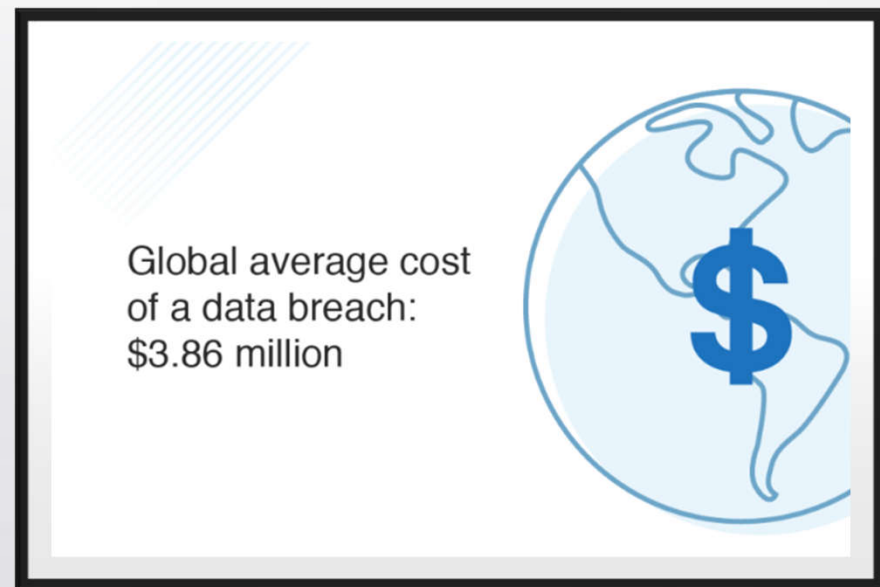
- Require cyber awareness training
- Limit internet access for your staff
  - If not needed for the job, do not grant
  - Incorporate automated blocking/Proxy
  - Review reports of use, incorporate policies
- Loss or compromise of a device
  - Data Encryption
  - Do not store files on local devices/hard drives
    - Use Cloud storage or local network storage
- 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)



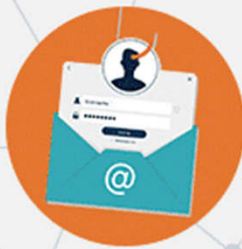
---

## No- and Low-Cost Options to Prevent Inadvertent Data Breaches, con't

- Complex Passwords
- Keep all software and operating system patches current
  - Anti-Virus and all 3<sup>rd</sup> party software
  - Seemingly minor OS updates – computers, phones, servers
- Use secure, encrypted email when sending attachments or sensitive information
- Geo-blocking
- Be careful connecting to WiFi networks, particularly those that are not password-protected
- Off-site backups of all data, such as in the cloud



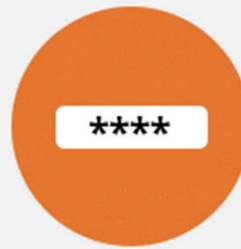
# Remote Work Considerations



**Be aware of phishing scams**



**Be careful of fake news and alerts**



**Set strong passwords or use an identity manager**



**Use Multifactor Authentication**



**Install an antivirus on all devices**



**Apply basic security features**



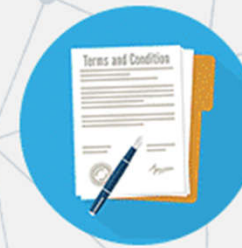
**Secure your home WiFi network**



**Use a VPN**



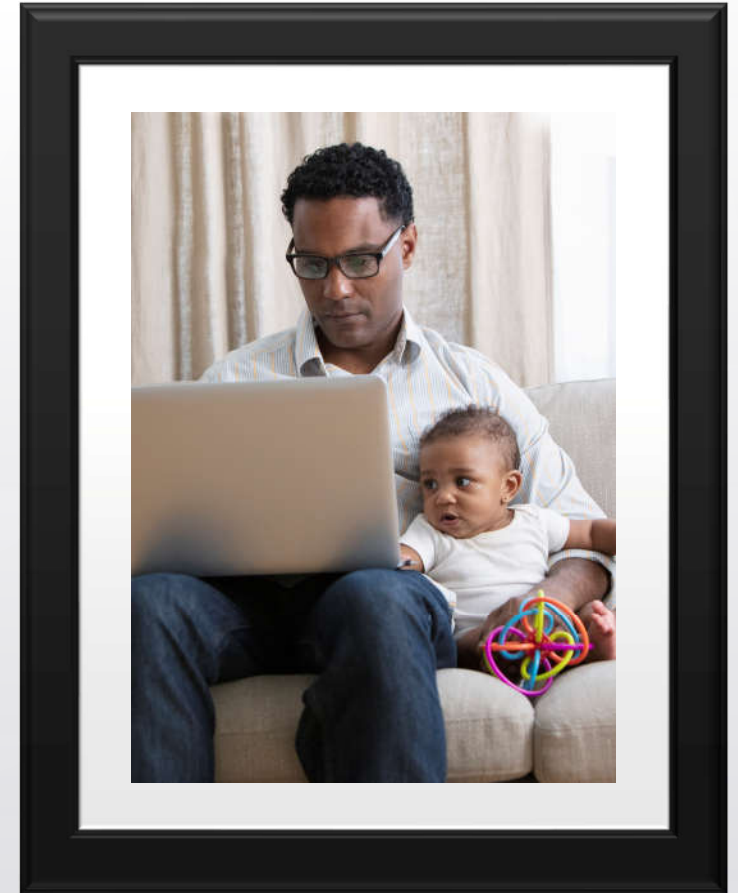
**Keep your work environment private**



**Set a Remote Work Policy**

## Remote Work: Security Measures and Policy Suggestions

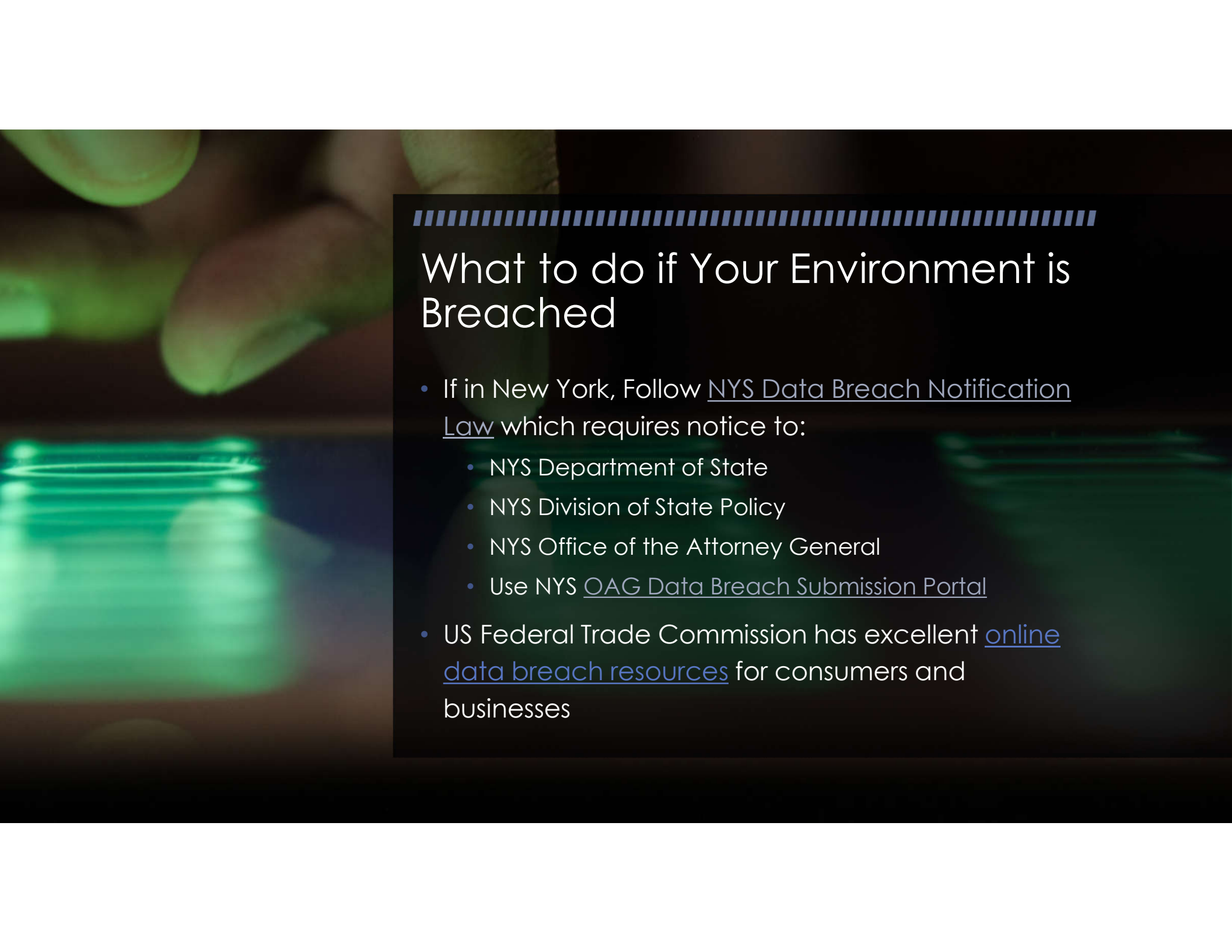
- Multi-Factor Authentication (MFA) is critical
- Prevent personal devices from connecting to your environment
  - No control over patching, other users
  - Work-issued devices are ideal
- Do not allow family members or others to use a work-issued device
- Be careful downloading apps
- Consider Mobile Device Management (MDM)
- Consider screen lock passwords, biometrics for authentication
- Only connect to work environment via secure WiFi





## Vetting Vendors and Other Third Parties

- Look at vendor policies and procedures, how they handle security threats
- Ask if their system has ever been compromised
- How is data hosted and backed up?
  - Cloud environments – Commercial vs Government Cloud, hosted in US?
- Is data encrypted at rest and in motion?
- Financial ability to recoup losses
- Compliance risk considerations / policies
  - HIPAA, CJIS, FedRAMP, StateRAMP
- Reputation, size of customer base



## What to do if Your Environment is Breached

- If in New York, Follow [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](#)
- US Federal Trade Commission has excellent [online data breach resources](#) for consumers and businesses

Q&A

