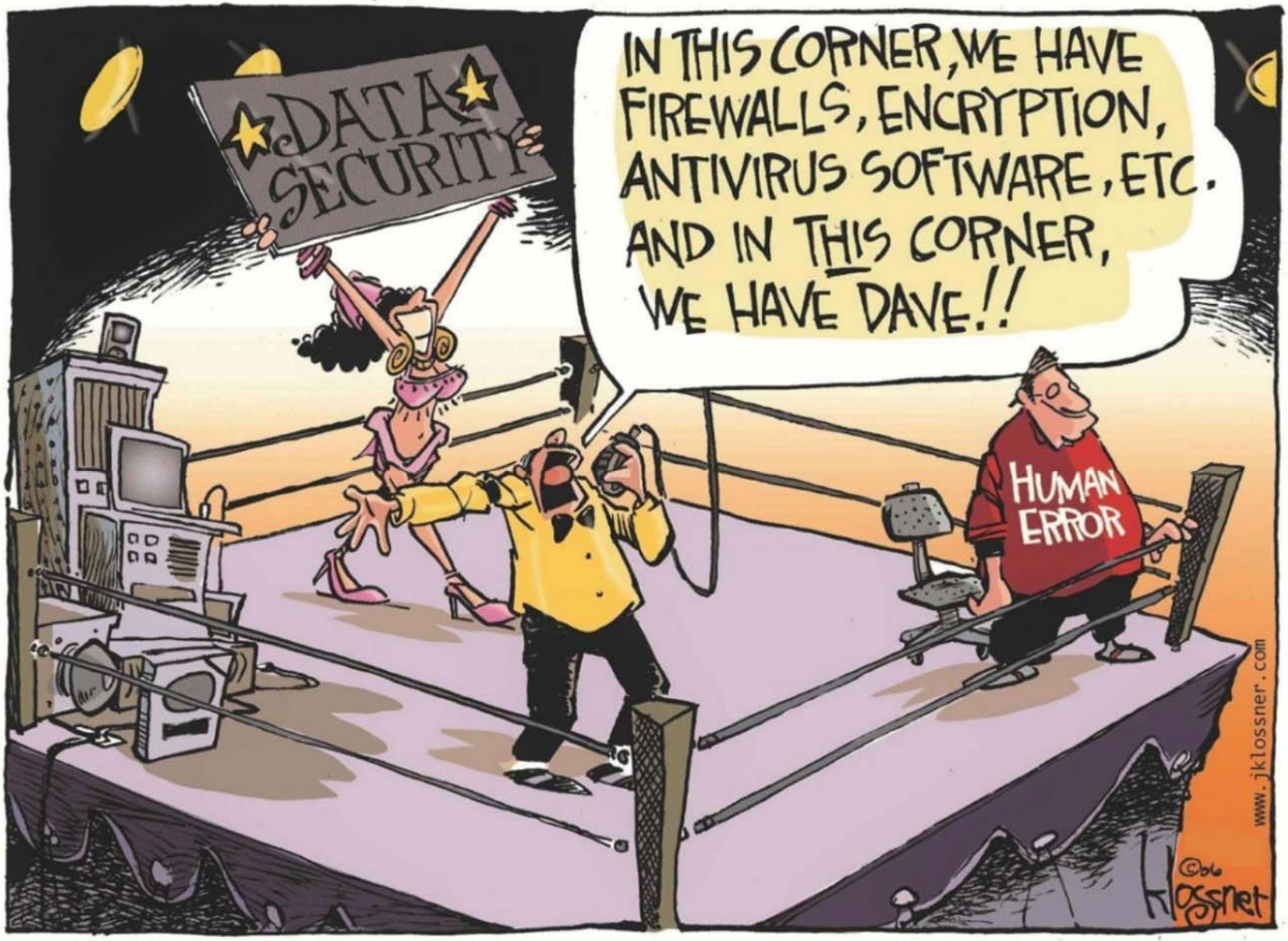
Fraud Awareness Overview

October – 2018
County Treasurers Association of Ohio

Chuck Peirano, Senior Vice President
Chief Fraud and Security Officer


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©blo
Klossner

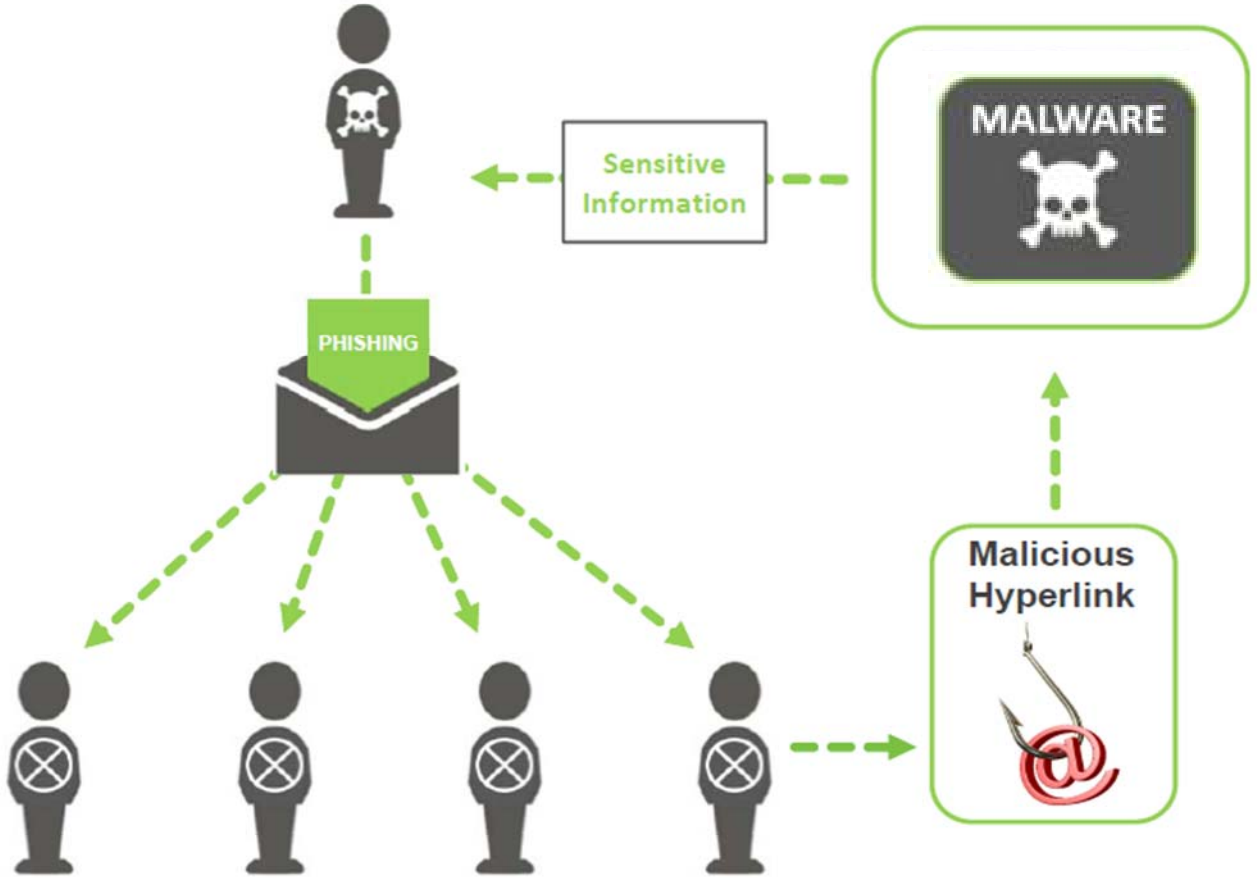
Why is it Important to Remain Vigilant?

- Fraud does not discriminate – it occurs everywhere, and no organization is immune
- Fraud tactics are becoming more sophisticated every day
- Fraudsters are reliant on the actions of their targets
- Fraud is ubiquitous in today's business environment and the threat continues to grow
- We can not rely on our customers to have adequate protection

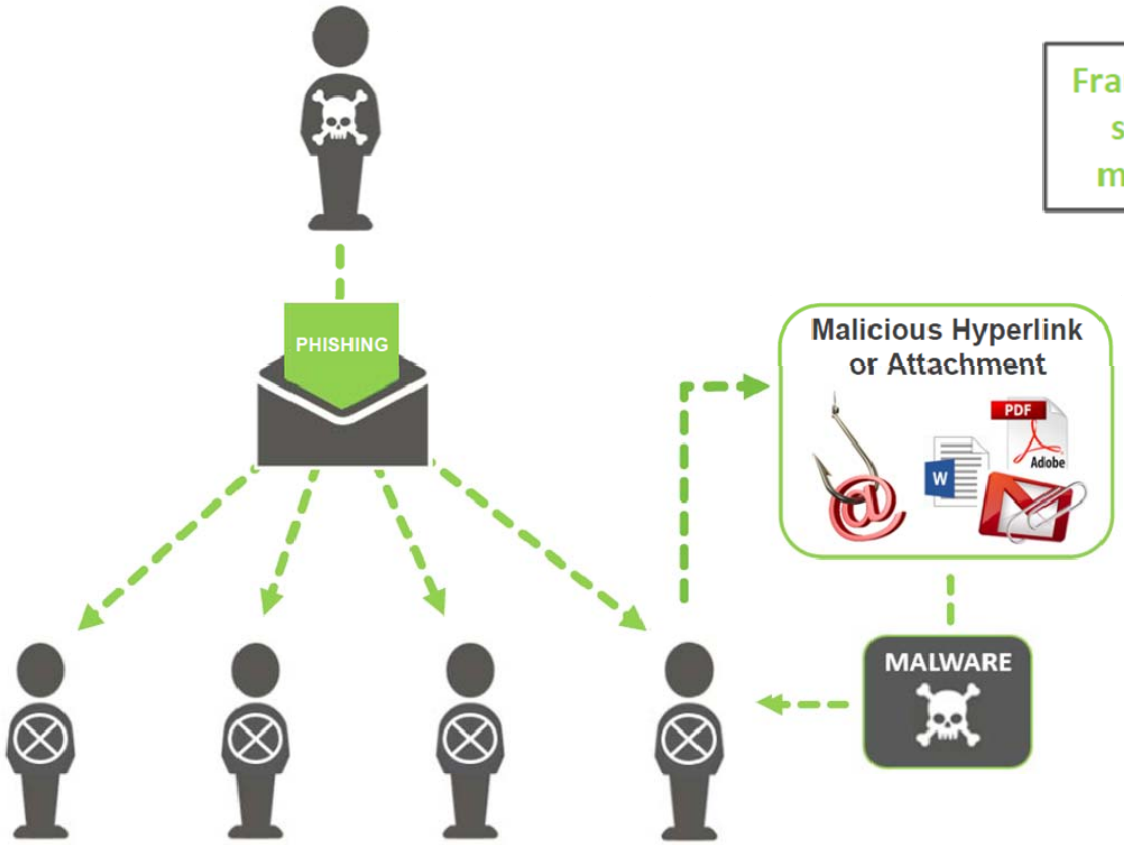
What is Phishing?

- Phishing attacks are typically perpetrated through the use of emails that appear to be sent from a legitimate source.
- Through deception, recipients of these emails are directed to **click on links** that send them to websites or **open attachments** within the email.
- Goal
  - Financial gain
  - Obtain sensitive information
- How is it done
  - Spoof Websites
  - Malware
  - Spoof email

Phishing – Using Spoof Websites



Phishing – Installing Malware



Fraudster uses malware to obtain sensitive information and/or manipulate the target's device

How Does BEC Work

BEC is a multi-component stealth exercise, mixing technology and the human factor.

Four stages:

1. **Profiling**: Surveillance of a target organization. The miscreant needs to gain understanding of how the organization runs and does business.

2. **Staging**: Information gathered provides insights on hierarchy and money movers.

3. **Execution**: Payload Malware or Spoofing

4. **Exit**: Request funds be sent

Malware - Example Scenario

1. Fraudster uses spear phishing tactics to compromise the email of a company's CEO.

2. Access to the CEO's email is acquired, and the fraudster reviews all available info (calendar, email history, language/signature/templates used, who executes monetary transactions, etc.)

3. A request is sent to the employee responsible for moving funds.

4. The employee confirms the request via email with the fraudster, who they believe to be the CEO.

5. The employee, believing the request to be legitimate, initiates the fraudulent payment.

6. Money exits to mule.

Spoofing BEC

Another multi-component stealth exercise, mixing technology and the human factor.

Three stages:

1. **Profiling**: Surveillance of a target organization. The miscreant needs to gain understanding of how the organization runs and does business

2. **Staging**: Information gathered provides insights on hierarchy and money movers

3. **Exit**: Request funds be sent

Spoofed Email - Example Scenario

1. Fraudster establishes an email similar to the real naming convention.

	Real Email
• Chuck.CXO@anycompany.com	
• Chuck.CXO@aanycompany.com	Chuck.CXO@aanycompany.com
• Chuck.CX0@anycompany.com	Chuck.CX0@anycompany.com
• Chuck.CXO@any_company.com	Chuck.CXO@any_company.com

2. Email sent to target requesting payment of invoice

3. Money exits to mule


STOP
THINK
ACT

Red Flags

The best way to stop a BEC fraud is to evaluate every request for money or sensitive data. Some examples of red flags are below:

1. Reply to email address does not match the from email address
2. The email address does not match known email formatting
3. Email may contain several spelling and grammatical errors and/or language not typically used by the alleged sender
4. Request that are of an urgent or rushed nature
5. Email sender is unavailable to talk, i.e., Meeting, Traveling, Vacation
6. Urgent or confidential request for payment
7. Move money request to new account numbers or routing numbers
8. Move money request to new account
9. Request for payments to a personal account or a new subsidiary of the company
10. Request for payments of unusual amounts, i.e., especially large or atypical
11. Request for payment without justification
12. Request to send money to areas not atypical, i.e., International, Country

Technical Steps

1. **Always** follow established written documentation of process and protocols
2. Understand your responsibilities & liabilities
3. Wire request via email are not allowed unless approved by established protocols
4. Treat all emails with caution
5. Never call a phone number provided in an email or text
6. Ensure phone numbers and contact information has not changed within the last thirty days (30)
7. Never take a move money request over the phone unless approved by established protocols
8. When in doubt stop and ask your manager for advise

Smishing & Vishing

What is SMISHING? This tactic involves the perpetrator sending an SMS (text) message to the target's smartphone containing a hyperlink that either installs malicious software onto their device or sends them to a website designed to obtain confidential information. In some instances, a phone number will be provided for the target to call, at which point they will be prompted to divulge sensitive information by an individual or an automated system.

- Messages appear to be from a valid source, often posing to be from a bank notifying the target that their account has been blocked – target directed to follow the bad link to unsuspend
- Mobile malware can harvest the data from your cell phone and transmit it back to the fraudster - including contacts (phone & email) and bank information
- Forward suspect text messages to 7726 (SPAM) to have the number blocked by your carrier

What is VISHING? This tactic is the telephone equivalent of phishing and uses phone calls to scam the victim into surrendering sensitive information. The fraudster will leave a voicemail in some instances, citing the urgency of a prompt response.

- These calls are designed to generate fear and evoke an immediate response (i.e. your card account will be closed immediately if you do not call back)
- When connected to an individual, they are often aggressive and will push for information without providing any themselves
- When in doubt, call the entity in question directly at a verified or publicly published phone number

Q & A

Appendix

Protect Your Business

Fraud Mitigation Checklist

Huntington is committed to assisting our clients in mitigating the risks associated with payment and online fraudulent activity. As part of that commitment, we have compiled a checklist of practices that may help you reduce the potential for payment and online fraudulent activity.

Issuing Checks, Initiating ACH / Wire

❑**Regularly review** your list of authorized personnel accessing your bank accounts, especially those with check issuance, ACH initiation, wire initiation, and approval access.

❑For consistency and increased transparency to errors and/or fraud, **implement and utilize**:

- Check Positive Pay, with teller line protection and payee positive pay
- ACH Positive Pay
- Wire-transfer templates

❑Adopt **dual-authorization** protocols and/or **callback procedures**:

- For all electronic funds transfers
- To decision suspect/exception check items

❑**Establish transfer limits** for all wire transactions

❑**Diligently monitor** your account for all non-standard check, ACH, and wire transaction activity

❑Do not deviate from these standard safeguards or your processing procedures.

Huntington

Protect Your Business

Fraud Mitigation Checklist (continued)

Card Acceptance

❑**Implement** tokenization and encryption security for terminal or web-based transactions.

❑**Adopt and utilize** EMV card capabilities.

❑**Establish** PCI DSS compliance and annually **complete** PCI DSS Self-Assessments to identify gaps.

Conducting Online Business

❑**Strengthen your network** by establishing a secure firewall, VPN connectivity and installing/maintaining anti-virus and anti-spyware solutions.

❑**Restrict or block access** to:

- Removable media devices (i.e. CDs, DVDs, or USB devices)
- Email attachments in formats commonly used to spread malicious programs (i.e. VBS, .BAT, .SCR, .EXE, .PIF)
- Social networking sites

❑**Train all employees** about cybercrime, common fraud schemes, keeping password credentials secure, and the importance of following online security protocol.

❑Evaluate a **cyber liability insurance policy** to provide first and third party coverage for damages when private, personal, and financial information are compromised due to a data breach or network intrusion.

Protect Your Business

Email Security

As with all security measures, the best offense is a good defense. Proactively protect your business and employees by knowing how email scams work.

Check

- ❑**Be suspicious of requests for secrecy or urgency**, and emails that request you use Reply, not Forward.
- ❑**Establish a company domain for company email** instead of using open source services such as Gmail. Register domains that are slightly different than the actual company domain and might be used by fraudsters to spoof company emails.
- ❑**Look carefully for small changes in email address** that mimic legitimate email addresses. For example: ".co" vs. ".com", "abc-company.com" vs. "abc_company.com", or "hijkl.com" vs. "hljkl.com"
- ❑**Flag email coming from domains that don't match the company domain** by programming your email system to add "-e" to the end of all external senders' email addresses.
- ❑**Turn webmail off if you don't need web access to email**, as it provides another attack point for criminals. If you must provide web access to email, limit accessibility by implementing VPN or another security control.
- ❑**Check for sudden changes to business practices** if the request is coming from a vendor. Were earlier invoices mailed and the new invoice emailed? Did a current business contact ask to be contacted via their personal email address when all previous official correspondence used a company email address?
- ❑**Check to see if the request is consistent** with how earlier requests have been requested. How often does the CIO or CFO directly request a wire payment? Do they typically submit requests when traveling (these attacks often are timed when the executive is out-of-office)? Have earlier requests included the phrases "code to admin expenses" or "urgent wire transfer," which have been reported by victims in fraudulent email requests.

Protect Your Business

Email Security (continued)

Confirm

- **Use an alternate mechanism to verify the identity** of the person requesting the funds transfer. If the request is an email, then call and speak to the person using a known phone number to get a verbal confirmation. If the request is via phone call or fax, then use email to confirm using an email address known to be correct. Or Forward the email (instead of using Reply) and type in a known email address. Don't reply to the email or use the phone number in the email.

- **Ask the sender to reconfirm the request.** While many people may be hesitant to question what appears to be a legitimate email from their boss or the CIO, consider which would be worse in light of how common this scam is: asking the CIO or CFO to reconfirm the request, or having the money stolen.

- **Implement dual approvals for financial transactions.** If you don't have written procedures, develop them. Avoid having the two parties responsible for dual approvals be in a supervisor/subordinate relationship as it could undermine the effectiveness of the process. Once they're in place, be sure to always follow established procedures.

- **Use a purchase order model** for wire transfers to ensure that all payments have an order reference number that can be verified before approval.

- **Develop a special policy to confirm requests** for employees that frequently travel and are authorized to request funds transfers, develop a special way to confirm requests. Perhaps develop a coding method that isn't documented within the network (in case of an intrusion search).

Protect Your Business

Email Security (continued)

Coach

❑**Spread the word.** Coach your employees about email fraud and the warning signs. Alert receptionists, admins, and others not to provide executives' travel schedules to unknown callers. Be suspicious and diligent, and encourage employees to ask questions.

❑**Be careful about what is posted to social media and company websites**, especially reporting structure and out-of-office details. Criminals have been known to launch these attacks when they know the CEO or CFO is traveling and therefore not easily available to confirm the request.

❑**Slow down**. Fraudsters gain an advantage by pressuring employees to take action quickly without confirmation of all the facts. Be suspicious of requests to take action quickly.

❑**Trust your financial institution.** If they question a payment, it's worth the time to cooperate with them to confirm the transaction is legitimate.

❑**Create an open culture** where employees feel free to challenge the need for information.

What to do if fraud happens to you

- ❑ Gather as much information and documentation as you can about the incident.
- ❑ Report the incident to the financial institution
- ❑ File a police report, if you think it's the best thing to do for your company
- ❑ Contact the Federal Trade Commission at 877.FTC.HELP or ftc.gov

There is no guarantee that you will get any money back in the event of fraudulent activity that results in a monetary loss.