SEC 161:
Electronic Banking and Cyber Security

Dusten Kohlhorst

- Dusten Kohlhorst

 IT Director
 Ohio Treasurer Josh Mandel
 (614) 728-3940
 Dusten.Kohlhorst@tos.ohio.gov

Stacey Russell

- Fiscal Officer, Muskingum County Library System
- (740)453-0391 Ext 130
- stacey@muskingumlibrary.org

3

Muskingum County Library System

- Background information:
  - Medium Size Library serving all of Muskingum County. Annual budget of about $4.75 million with 6 locations

  - 2 Accounting staff members, 1 full time and 1 part time

Muskingum County Library System

4

ACH Fraud

What Happened?

- Tuesday, March 19ᵗʰ we ran payroll and uploaded direct deposit to our bank

- Monday, March 25, 2013 we were notified by our bank via phone that they felt we had some fraudulent activity on our account

- 3 ACH transactions that were not initiated by the Library on March 21, March 22 and March 25 totaling $144,743

- The bank immediately took steps to "recall" those transactions

What Happened?

- Library IT staff disconnected both Accounting PCs from the internet and called our Technology Consultant

- Based on the Tech Consultant's advice, Library IT staff erased & re-formatted both Accounting PCs

- Zanesville Police were called and a report was filed

- We closed our existing bank accounts and opened new ones with new log on information

- We notified staff of a possible security breach and contacted the Board of Trustees

What Happened?

- AOS was involved and information was shared with the FBI via AOS

- Our insurance carrier was notified and a claim made

- By April 25th, 2013 $54,910 was recovered

- We settled with the bank regarding the remaining loss of $89,833

Mistakes Made

- Our ACH Originator Agreement required us to notify the bank of direct deposit uploads; when we were trained by the Bank, we were told to disregard that requirement

- IT should have not erased and reformatted hard drives

- We should have pushed harder with local law enforcement

What we are doing differently

- Bank now requires us to follow the ACH Originator Agreement
- We have a stand-alone PC that is only used for online banking
- We have requested that online access be granted from only 1 IP address.
- We purchased a cybercrime policy
- We are revising our Banking RFP to include a section regarding online banking security minimums

Ransomware

- March 2017, Accounting server was not working
  - Local IT Staff investigated and accounting software provider was called to double check for any changes they might have made

  - Text File was found on the server

Hi!

If you're seeing this file, then all your FILES have been LOCKED with the most strongest military CIPHER.

All your important data - documents, photos, videos - everything in CRYPTED.

The only way to recover your files - contact us via restoreserver@yandex.com

I stored the crypted data in your hard disk.

If you want to become your data back, send me an email containing your ip adress.

Your ip adress: 66.213.91.13

Next Steps

- Called our CyberRisk Risk Policy and made a claim
  - CyberRisk Policy put us in touch with a company that specialized in breaches – the goal was to minimize liability by following the law and protect the library and any affected parties
- Report was filed with the Internet Crimes Division of the FBI

Next Steps

- New server was created for the accounting system and accounting software reinstalled – with only data from the backup

- All staff were contacted and offered a help line and credit monitoring since it could not be determined if payroll data was breached.

- Instituted on-going end-user training for all staff.

- Upgraded Malware protection

- Expanded the use of Deep Freeze to include office computers.

Cost to the library:

- Accounting was down for approximately 1 week
- Over $36,000 to the library

What do Attackers Want?

Different attackers have different motivation but here are the common purposes:

> **Money:**
> - **Money from municipal accounts**
> - **Money from your vendors**
> - **Money from your employees**
>
> **Identity:**
> - **Constituent/Employee personal information**
>   - **SSN of Employee and dependents**
>   - **Personal information to initiate identity theft**
> - **Vendor Tax ID number**
>
> **Access:**
> - **Connections to other municipalities**
>   - **Schools**
>   - **Police Department**
>   - **Public Safety**
> - **Use your computer as part of a bigger attack**
>
> **Public Embarrassment:**
> - **Defaced websites**
> - **Redirected websites**

Signs you've been compromised?

- Install of Fake Anti-Virus and Fake Messages.
- Install of unwanted browser toolbars
- Redirected browser/websites
- Frequent popups & additional browser tabs
- Installed Anti-Virus/Anti-Malware is disabled and can't be restarted
- Computer has high CPU or network usage when it should be idle
- Trusted passwords don't work anymore

How are Attacks Conducted?

Two Types of Attack:

- APT—Advanced Persistent Threat. They are attempting to compromise your specific organization. These are expensive and long term. **Rarely used against local municipalities.**

- Opportunistic Attack. You are in the wrong place at the wrong time. **MOST local attacks are Opportunistic Attacks.**

APT—Advanced Persistent Threats

- All APTs start with reconnaissance
    - Email Lists
    - Table of Organization
    - Scanning of your network
    - Review all public website
    - Review all public domain information (assigned IP addresses, contact information on GoDaddy, etc.

- Initial "Attack" is usually a soft attack
    - Spear phishing attack—an email directed specifically crafted to be viewed and sent by specific individuals:
        - An Example of this: The Executive Director sends an email to an IT engineer asking about specific firewall configurations

   NOTE:

IF you believe you are under an APT, you need to contact law enforcement. MOST municipalities do NOT have the resources to investigate and stop these sophisticated attacks.

Opportunistic Attacks

Opportunistic attacks commonly use 3 methods to break your computer:

1. Web surfing
2. Email & Clicking links in Email
3. Attaching compromised media to computer: USB drive, CD/DVD

Note:
The purpose of all attacks is to put unauthorized code on your computer which will grant the attacker access to your computer.

What should I do differently

- Don't click on email links.
- Don't fall victim to click-bait.
- If you find a USB Drive, don't plug it in.
- Limit your security rights to the minimum necessary for your daily job.
- Use Pass Phrases not passwords, >10 characters
- Different Pass Phrases for different accounts.
- Be careful on social media posting. If you're on vacation for 2 weeks, you aren't at home.
- Don't access sensitive data on public Wi-Fi

What can my organization do differently?

- Create a mandatory cyber-security education program.
- Audit user accounts
- Enforce Pass Phrases
- Limit computers & users allowed to access sensitive data (HR data, bank sites, accounting data)
- Implement debit block and only allow debit from certain organizations
- Create Incident Response Plan
- Check accounts daily for $0.01 withdrawal
- Incident Response Plan & Insurance

What technical solutions?:

- Enable automatic patching of desktops and monthly patching of servers.
- Run Anti-virus and Anti-malware software.
- Install a pop-up blocker add-on on web browsers.
- Use a 3rd party to inspect email before it's delivered to the organization.
- Create daily backups, verify they work.
- Next-Generation Firewalls—allows active inspection of web traffic for malicious code
- Dual Factor Authentication to bank sites, may be necessary to other sensitive sites.

What to do if my organization is hacked?

- IF it is a significant hack:
    - Unplug NETWORK cable from computer. Leave computer turned on.
    - Activate your Incident Response Plan
    - Notify all banks and validate balances
    - Reset all passwords (Don't use infected computer)
    - Contact law enforcement—contact info on last slide
    - Get legal/communication advice on notifying effected individuals/entities

What to do if my organization is hacked?

- IF it not a significant hack (No data loss, No financial impact)
  - Conduct through investigation, assuming a major impact until you're confident it isn't.
  - Migrate individual documents off the desktop (using backups is better)
  - Erase computer and rebuild
  - Reset all account passwords

Issues of Note:

- The IRS will NOT email you with a TAX issue

- Microsoft will NOT call you to notify you your computer has been hacked

- Urgent emails are fake emails.
  - Don't believe email links and phone numbers, look them up using Google

- Friends get compromised. DON'T believe everything they send you…and don't click on it.

Attacks ahead:

- Phishing Attack & Spear Phishing Attack
- Watering Hole Attack
- Ransomware
- Social Engineering
- Click Bait
- URL re-direct

- Zero Day Exploit
- DDOS (Distributed Denial of Service)

Watering hole attack

Ransomware In action

Click-Bait!!

DDOS Attack

URL Re-Direct Exploit

URLs point to sites that load an exploit kit
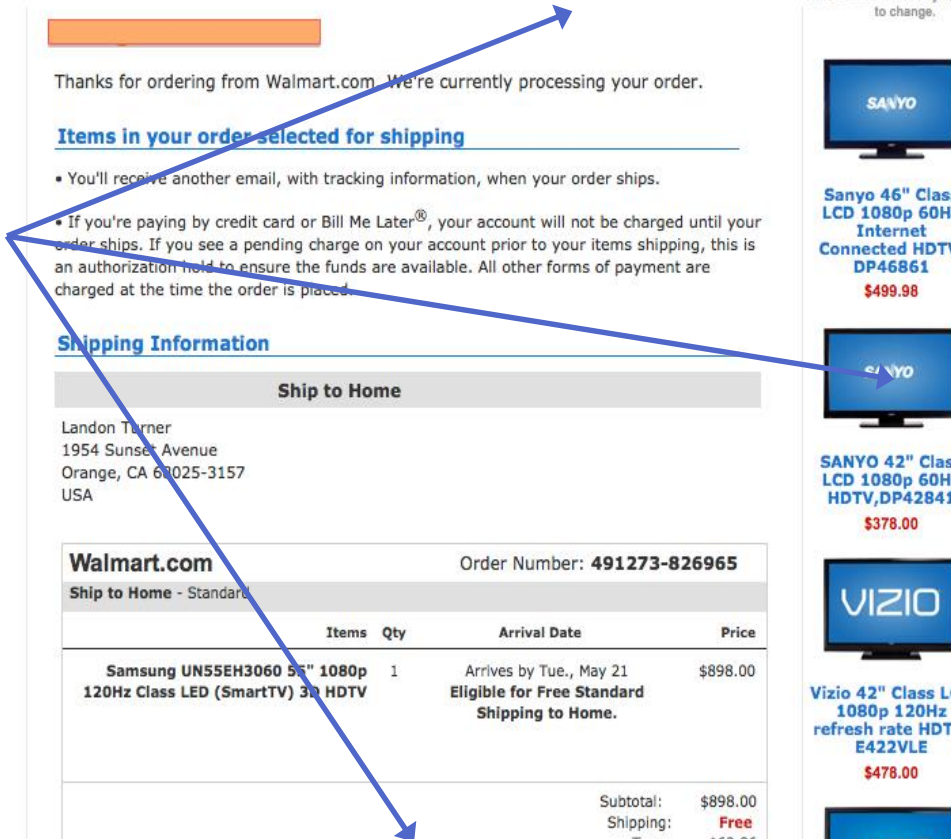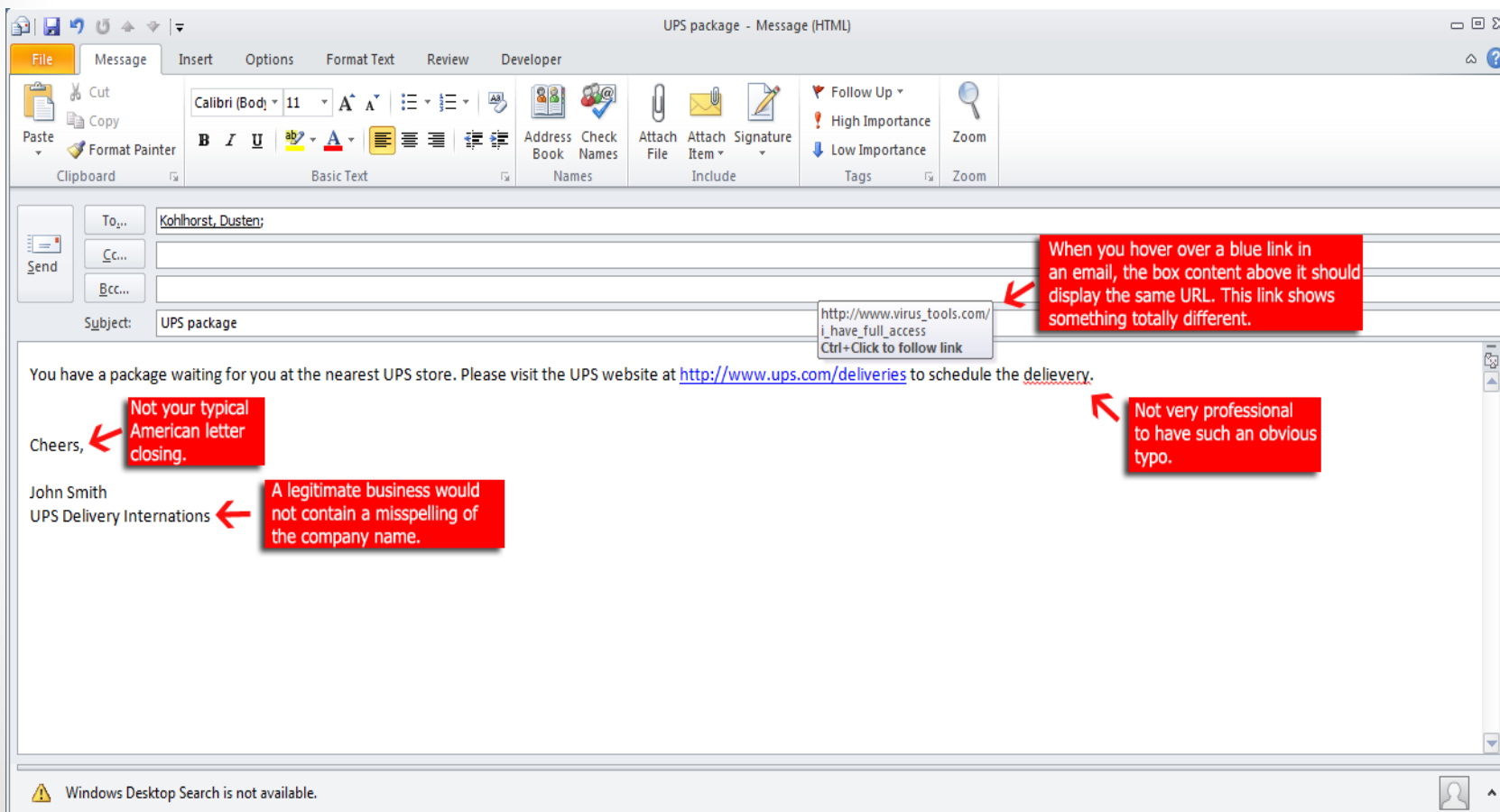
Do Not Click on Links Inside Emails

Clicking on links inside an email can give COMPLETE control of your computer to a hacker. They can have the ability to watch everything you are doing and send them a file of everything you've typed. If you get an email with imbedded links, lookup the organization's phone number and give them a call.

Security Resource

Russ Forsythe

State Chief Information Security Officer

Office of Information Security & Privacy

(614) 644-9391

State.CISCO@OIT.ohio.gov

- Intrusion Prevention
- Incident Handling & Forensics
- Vulnerability Assessment & Penetration Testing
- Information Security Training & Awareness

36

Ohio Homeland Security

Homeland Fusion Center

877-OHS-INTEL

www.privacy.ohio.gov

Ohio Strategic Analysis & Information Center

www.homelandsecurity.ohio.gov/saic.stm

Multi-State Information Sharing & Analysis Center

http://msisac.cisecurity.org

37

MyCPIM Password

CYBER