

CPIM

CENTER FOR PUBLIC INVESTMENT MANAGEMENT



A PROGRAM BROUGHT TO YOU BY:

JOSH MANDEL

TREASURER OF OHIO

SEC 161: Electronic Banking and Cyber Security

Dusten Kohlhorst

- Dusten Kohlhorst

Director

Ohio Treasurer Josh Mandel

(614) 728-3940

dusten.Kohlhorst@tos.ohio.gov

Muskingum County Library System

- Background information:
 - Medium size library serving all of Muskingum County. Annual budget of about \$4.5 million with 6 locations.
 - 2 Accounting staff members – 1 full-time and 1 part-time.
 - In December of 2012, the Library signed a 3 year depository agreement with a small local community bank for active funds.

What Happened?

- Tuesday, March 19, 2013, the Library ran payroll and uploaded direct deposit to its bank.
- Monday, March 25, 2013, the Library was notified by its bank via phone that the library had some fraudulent activity on its 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.

Library's Response

- Library IT staff disconnected both Accounting PCs from the internet and called its Technology Consultant.
- Based on the Tech Consultant's advice, Library IT staff erased and re-formatted both Accounting PCs.
- Zanesville Police were called and a report was filed.
- The Library closed its existing bank accounts and opened new ones with new log on information.
- The Library notified staff of a possible security breach and contacted the Board of Trustees.

What Happened?

- Auditor of State's Office was involved and information was shared with the FBI via AOS. Ultimately, Secret Service was involved.
- The Library's insurance carrier was notified and a claim made.
- By April 25th, 2013, **\$54,910** was recovered.
- In 2014, the Library settled with the bank regarding the remaining loss of **\$89,833**.

Mistakes Made

- The Library's ACH Originator Agreement required it to notify the bank of direct deposit uploads. When the staff was trained by the Bank, they were told to disregard that requirement .
- IT staff should have not erased and reformatted hard drives.
- The Library should have pushed harder with local law enforcement.

What the Library Is Doing Differently

- Now required by Bank to follow the ACH Originator Agreement.
- Designated one stand-alone PC that is only used for online banking.
- Requested online access from only 2 IP addresses.
- Purchased a cybercrime policy.
- Revising its Banking RFP to include a section regarding online banking security minimums.



Digital Financial Security

Common Misperceptions

Common Misperception:
“I’m secure.”

Reality: NO computer attached to the internet is completely secure.

Common Misperception:
“If I had more money I could make us secure.”

Reality: Federal Agencies, as well as Fortune 100 companies have fallen victim to cyber-crime, and they have nearly unlimited budgets.

Goal: Become sufficiently secure that your data isn’t worth the effort to compromise your security.

The next couple of slides show that even unlimited recourses do NOT result in security.



Who has been compromised?

Central Intelligence Agency:

- CIA website – June 2011

Congress:

- U.S. Senate – June 2011
- Senator Bill Nelson's office – March 2009
- Representative Wolf and Foreign Affairs Committee offices – August 2006

Department of Agriculture:

- USDA DC headquarters – June 2006

Department of Commerce:

- Economic Development Administration – February 2012
- Website breach – December 2009
- Commerce Secretary – December 2007
- Bureau of Industry and Security – October

Department of Defense:

- F-35 development – February 2012
- Unmanned aerial vehicle – December 2011
- DOD – July 2011
- National Guard – December 2010
- Army – April 2010
- Unmanned aerial vehicle feeds – December 2009
- US Central Command – November 2008
- Secretary of Defense's email – June 2007
- National Defense University – May 2007
- Naval War College – November 2006

Department of Education:

- *August 2006*

Department of Energy:

- *Nuclear Security Administration – October 2011*

DOE/National Laboratories:

- *Pacific Northwest National Labs – July 2011*
- *Thomas Jefferson National Labs – July*
- *Oak Ridge National Labs – April 2011 and October 2007*

Department of Homeland Security:

- *DHS website – February 2012*
- *Homeland Security Information Network – May 2009*
- *DHS – September 2007*
- *DHS – June 2007*
- *DHS Headquarters*

Department of Interior:

- *May 2010*
- *DOI Audit – November 2009*
- *DOI – February 2002*

Department of Justice:

- *DOJ website – January 2012*

DOJ/Federal Bureau of Investigation:

- *FBI conference call – February*
- *FBI website – January 2012 and June 2011*

Department of State:

- *Bureau of East Asian Affairs – June 2006*

Department of Transportation:

- *National Highway Traffic Safety Administration – June 2010*
- *DOT website – July 2009*

DOT/Federal Aviation Administration:

- *FAA – May 2009*

Department of Treasury:

- *Treasury Dept website – July 2009*

Department of Veterans Affairs:

- *4,000 records exposed between March and December of 2011*
- *26.5M records were stolen in May 2009.*

Federal Deposit Insurance Corporation:

- *From August 2008 to July 2009*

Federal Trade Commission:

- *FTC online security website – January 2012*
- *FTC website – July 2009*

National Aeronautics and Space Administration:

- *NASA – 2011 and 2010*
- *NASA satellite – November 2011*
- *NASA's Jet Propulsion Laboratory website – May 2011*
- *Goddard Earth Observation System – May 2011*
- *International Space Station – March 2011*
- *Jet Propulsion Laboratory – 2009*
- *NASA headquarters – December 2006*
- *NASA – 2004*
- *Ames Research Center – 2004*

National Archives:

- *In April 2009, a hard drive containing SSNs of over 100,000*

Office of Personnel Management:

- *USAjobs – January 2009*

Social Security Administration:

- *36,000 people SSN were released by the SSA between May 2007 and April 2010.*

U.S. Copyright:

- *Copyright office – January 2012*

What Value Does Your Entity Have to a Hacker?

- Financial information and banking access
- Customer's personal information
- Direct connections to other government organizations
- Vendor information
- Employees' personal information
- Reputation



**Becoming
more secure
does NOT
cost a lot of
money!**

No Cost Must Do's

- ◉ **Implement Debit Block**
 - Debit block prevents withdrawals from your accounts without your knowledge. You must push payments, rather than individuals or organizations pulling payments.
- ◉ **Check your accounts DAILY**
 - Review all your accounts daily. Alert the bank if any transactions were not authorized. Pay special attention to any withdrawal under \$1.00, specifically the withdrawal of \$.01. This is a “validity test” of your account. Someone has access to your account and is testing the ability to withdrawal funds. They will be back to with withdrawal a lot more. Notify the bank and put a hold on the account immediately.

No Cost Must Do's

- **Turn on Auto-Updates for Windows computers**
 - Microsoft puts out security updates on the second Tuesday of every month (Patch Tuesday).
 - Make sure all Windows computers are set to automatically install the security updates. Also, security patches are released throughout the month depending on the severity of the vulnerability, or have an established patch schedule.
 - Have the computers set to check on a daily basis after hours.
- **Use a firewall**
 - While enterprise firewalls can cost >\$20,000 each and many can't afford that investment, Windows offers a free firewall for the Windows desktops. Turn on this feature.
 - A firewall allows only particular types of web traffic to your computer (websites, FTP, Telnet.)

Little Cost Must Do's

- ◉ **Dual factor (two factor) authentication**
 - Dual factor authentication is defined as something you know and something you have. Usually this is a username and password and a key fob that displays a number that must be entered into the banking website within 60 seconds of display. Work with your bank to implement this.
- ◉ **Anti-virus on all computers**
 - All Windows computers need to have antivirus with updated signature files. This is a critical layer of protection against inadvertently downloading viruses/malware/spyware while surfing the internet.
- ◉ **Separate network into all general public and administration computers**
 - The general public accessing websites and bringing in their own media is the highest risk for infection. Minimize the risk by separating those computers from employee computers.

Policy & Procedure Changes to Implement

- ◉ *Do not use general computers*
 - The general public computers are a prime location for a virus to infiltrate your entity. **Don't use those computers!!**
- ◉ *No wireless access for banking transactions*
 - Wireless is unsecure, even if the wireless network is password protected. It takes less than a minute to break most of these passwords. If you are doing banking, use administrative computers that are wired.
- ◉ *Use different passwords*
 - Do not use the same password for all your different access.
 - Your Facebook password needs to be different than your banking password. Password sentences, or phrases are better than a complex password. “Oct. 31st is my favorite day” is better than “31Octday.”
 - And, no password is secure if written on a sticky note attached to the monitor. 😊

Policy & Procedure Changes to Implement

- ***Use administrative computers for work only***
 - Use Administrative Computers only for work. Going to non-business sites/blogs increases the risk of getting a virus.
- ***Limit number of computers authorized to do banking***
 - Give your bank the IP address of the computer(s) authorized to do banking. All other transactions should be rejected. When implementing this, develop a business solution if your entity's network is down.
- ***Mandatory Staff Training***
 - Staff needs to be properly trained and educated on what is “suspicious” and appropriate next steps. This should be done on an annual basis and for all new employees.

Final Policy & Procedure Change

- While there are many things to consider, here are a few basic rules that should be followed:
 - Do NOT turn off the infected computer(s), and do NOT format it. Disconnect the computer from the network, the computer may have forensic data that law enforcement can use.
 - Contact the bank and let them know the situation. Suspend the account until you are comfortable no unauthorized transactions are going to take place.
 - Contact local law enforcement and Ohio Highway Patrol.
 - Be able to conduct banking business without using computers. In the event of a compromise the designated banking computers may be the ones infected. You need to be able to conduct business while these devices are being inspected.
 - Notify any other banks you have accounts with even if they are not effected. Those accounts may be compromised too.



**Develop
policies
BEFORE a
security
breach
occurs!**

Social Engineering and Phishing

- Social Engineering
 - contacting a user and convincing them to release sensitive information. “Oh, since you’re Bob from IT I’ll give you my password...”
- Phishing
 - sending a “fake email” that has the user click on an invalid link that directs the computer to a site that loads viruses and various malware.

Walmart Fake Order Confirmation

From: Walmart.com <nuptialsos@emlreq.wallmartmail.org> ☆

Subject: Thanks for your Walmart.com Order 491273-826965

To: [Redacted] ☆

Reply Forward Archive Junk Delete

5/16/13 12:49

Other Actio



[Visit Walmart.com](#) | [Help](#) | [My Account](#) | [Track My Orders](#)



Thanks for ordering from Walmart.com. We're currently processing your order.

Items in your order selected for shipping

- You'll receive another email, with tracking information, when your order ships.
- If you're paying by credit card or Bill Me Later®, your account will not be charged until your order ships. If you see a pending charge on your account prior to your items shipping, this is an authorization hold to ensure the funds are available. All other forms of payment are charged at the time the order is placed.

Shipping Information

Ship to Home

London Turner
1954 Sunset Avenue
Orange, CA 68025-3157
USA

Walmart.com

Order Number: **491273-826965**

Ship to Home - Standard

Items	Qty	Arrival Date	Price
Samsung UN55EH3060 55" 1080p 120Hz Class LED (SmartTV) 3D HDTV	1	Arrives by Tue., May 21 Eligible for Free Standard Shipping to Home.	\$898.00
Subtotal:			\$898.00
Shipping:			Free
Tax:			\$62.86

See our [Returns Policy](#) or

Walmart.com Total: **\$960.86**

Recommended for You

* Prices and availability are subject to change.



Sanyo 46" Class LCD 1080p 60Hz Internet Connected HDTV, DP46861
\$499.98



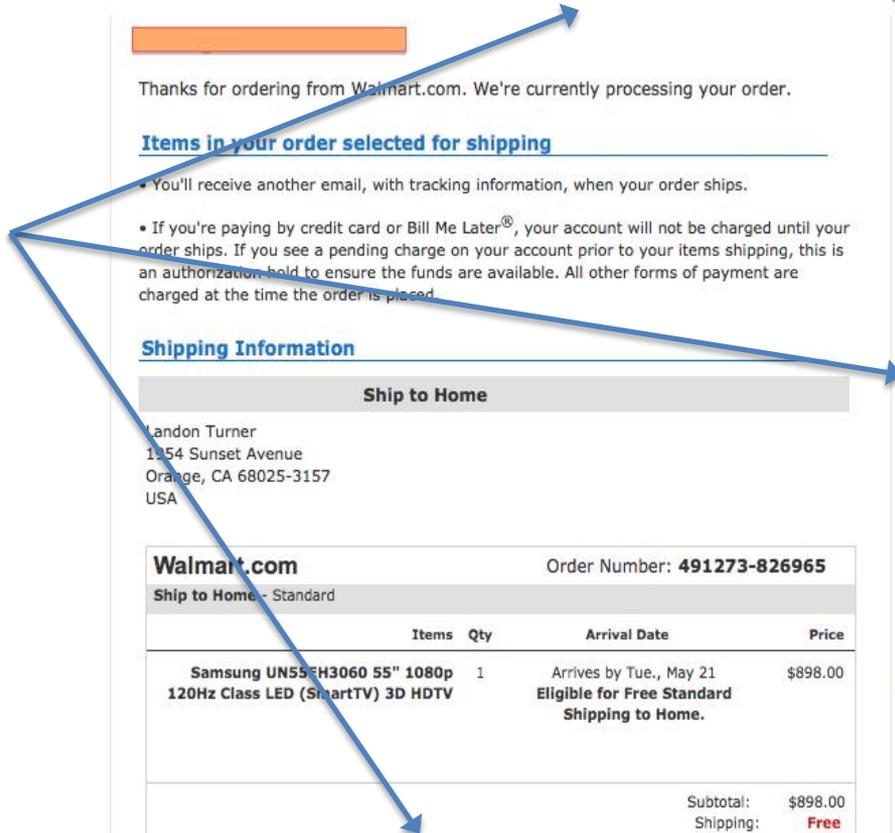
SANYO 42" Class LCD 1080p 60Hz HDTV, DP42841
\$378.00



Vizio 42" Class LCD 1080p 120Hz refresh rate HDTV, E422VLE
\$478.00



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.

The screenshot shows an email client window titled "UPS package - Message (HTML)". The interface includes a menu bar (File, Message, Insert, Options, Format Text, Review, Developer) and a ribbon with various tools like Cut, Copy, Paste, Format Painter, and text formatting options. The email header shows the recipient as "Kohlhorst, Dustin", the subject as "UPS package", and a "Send" button. The main body of the email contains the following text:

You have a package waiting for you at the nearest UPS store. Please visit the UPS website at <http://www.ups.com/deliveries> to schedule the delivery.

Cheers,

John Smith
UPS Delivery Internations

Four red callout boxes with arrows pointing to specific elements in the email:

- A box pointing to the recipient name "Kohlhorst, Dustin" contains the text: "When you hover over a blue link in an email, the box content above it should display the same URL. This link shows something totally different." (Note: The arrow points to the recipient name, but the text refers to a link.)
- A box pointing to the blue link "http://www.ups.com/deliveries" contains the text: "Not very professional to have such an obvious typo." (Note: The text refers to the misspelling of "deliveries" as "delievry").
- A box pointing to the closing "Cheers," contains the text: "Not your typical American letter closing." (Note: The text refers to the informal closing.)
- A box pointing to the sender name "UPS Delivery Internations" contains the text: "A legitimate business would not contain a misspelling of the company name." (Note: The text refers to the misspelling of "Internations" as "Internations").

At the bottom of the window, a Windows Desktop Search notification is visible: "Windows Desktop Search is not available."

Security Resource

David Brown

**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

Ohio Homeland Security

Homeland Fusion Center

877-OHS-INTEL

www.privacy.ohio.gov

**Ohio Strategic Analysis
& Information Center**

www.homelandsecurity.ohio.gov/saic.stm



**OHIO HOMELAND
SECURITY**

**Multi-State Information
Sharing & Analysis Center**

<http://msisac.cisecurity.org>



MULTI-STATE

Information Sharing & Analysis Center