Cybercrime: It's not a question of if, but when. Is your data safe?

Presented by:
Nicole Beckwith
Fraud Investigator/Digital Forensic Examiner

DAVE YOST
Ohio Auditor of State

www.ohioauditor.gov

Threat Overview

- In 2015 Ohio ranked #10 in the nation for cybercrime**
- In 2016 Ohio ranked #9 in the nation for cybercrime***
- The hardest hit age group are those over 60 ***
- In 2016 more than 4.2 billion records were exposed*
- In over 4149 data breaches*
- By 2019 cybercrime is expected to reach $2 TRILLION in loss*

*Verizon 2016 Data Breach Investigations Report

** 2015 FBI cybercrime report

***2016 FBI cybercrime report

Cybercrime in Ohio

DAVE YOST
Ohio Auditor of State

www.ohioauditor.gov

Victims of Cybercrime

- Montgomery County, Miami Valley Regional Planning Commission – Ransomware
- Clinton County, Vernon Township – Ransomware
- Morrow County, Peru Township – Ransomware
- Columbiana County, Court System – Ransomware
- Licking County – Ransomware
- Madison County – Agricultural Society – Vishing
- Delaware County – Big Walnut Schools – Phishing
- Athens County – Trimble Local Schools – Phishing
- Many, Many More……

Agenda

- Threats Overview
- Ransomware
- Social Engineering
  - Vishing
  - Smishing
  - Phishing
- Important Contact Information

Top 5 Hackers

- Who are they?
- Why do they attack the little guys?
- Why governments?

Malware

A blanket term covering any form of intrusive software such as:

- Trojans
- Worms
- Spyware
- Adware
- Bots
- Viruses
- Keyloggers
- Ransomware

Ransomware


WARNING!
YOUR COMPUTER MAY BE INFECTED:
System Detected (2) Potentially Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-Download. Your Personal & Financial Information MAY NOT BE SAFE.
To Remove Viruses, Call Tech Support Online Now:
1(888) 643-9730
(High Priority Virus Removal Call Line)
Your IP Address: 198.199.92.121 | Generated on 03-15-2014 | Priority: Urgent

Police Department Loses Digital Evidence Dating Back to 2009 in Ransomware Attack

DAVID BISSON

JAN 27, 2017 | LATEST SECURITY NEWS

SECURITY NEWS

AddThis

A police department based in Texas has lost digital evidence and other files dating back to 2009 as a result of a ransomware attack.

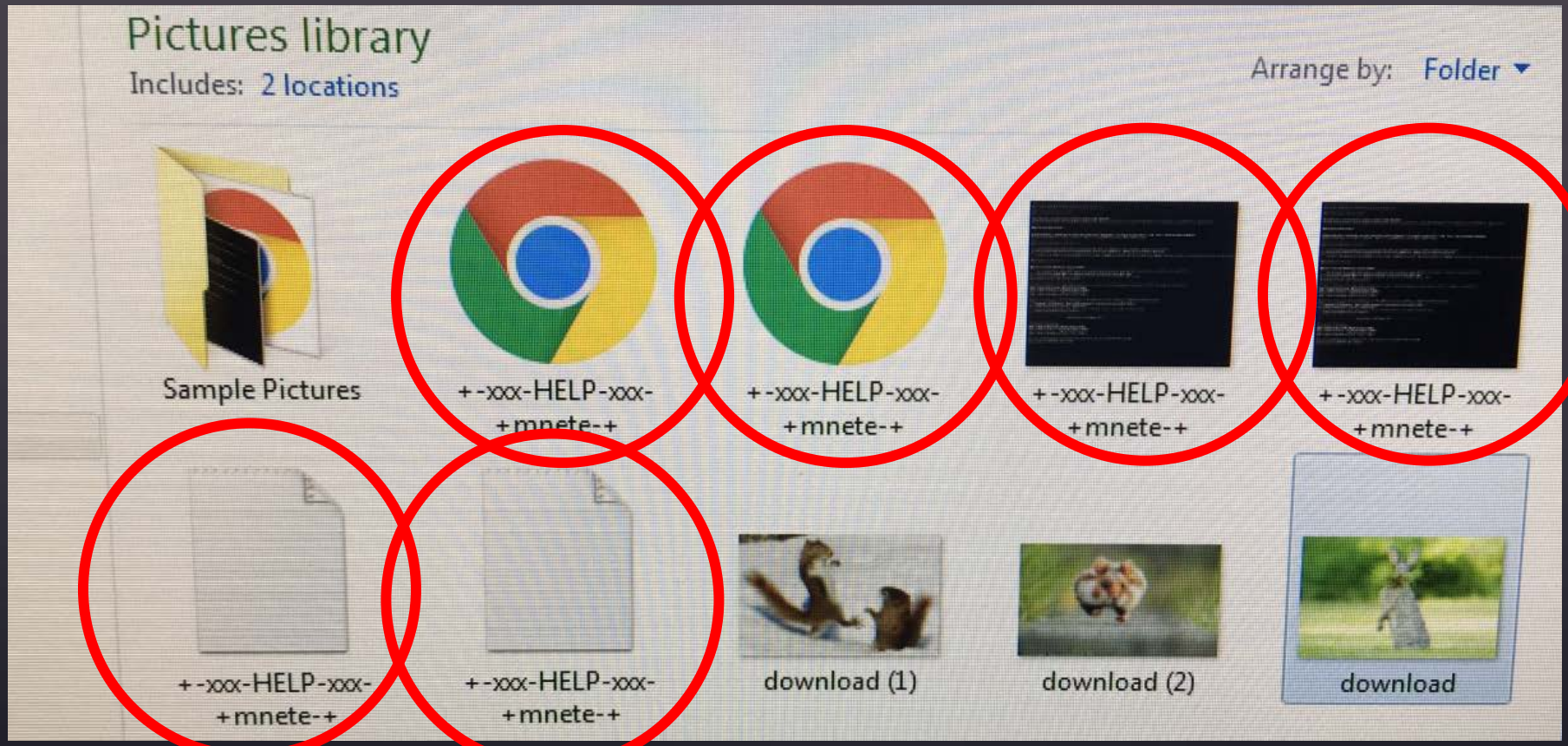
On 25 January 2017, the Cockrell Hill Police Department issued a press release in which it reveals a computer virus had recently affected one of its servers:

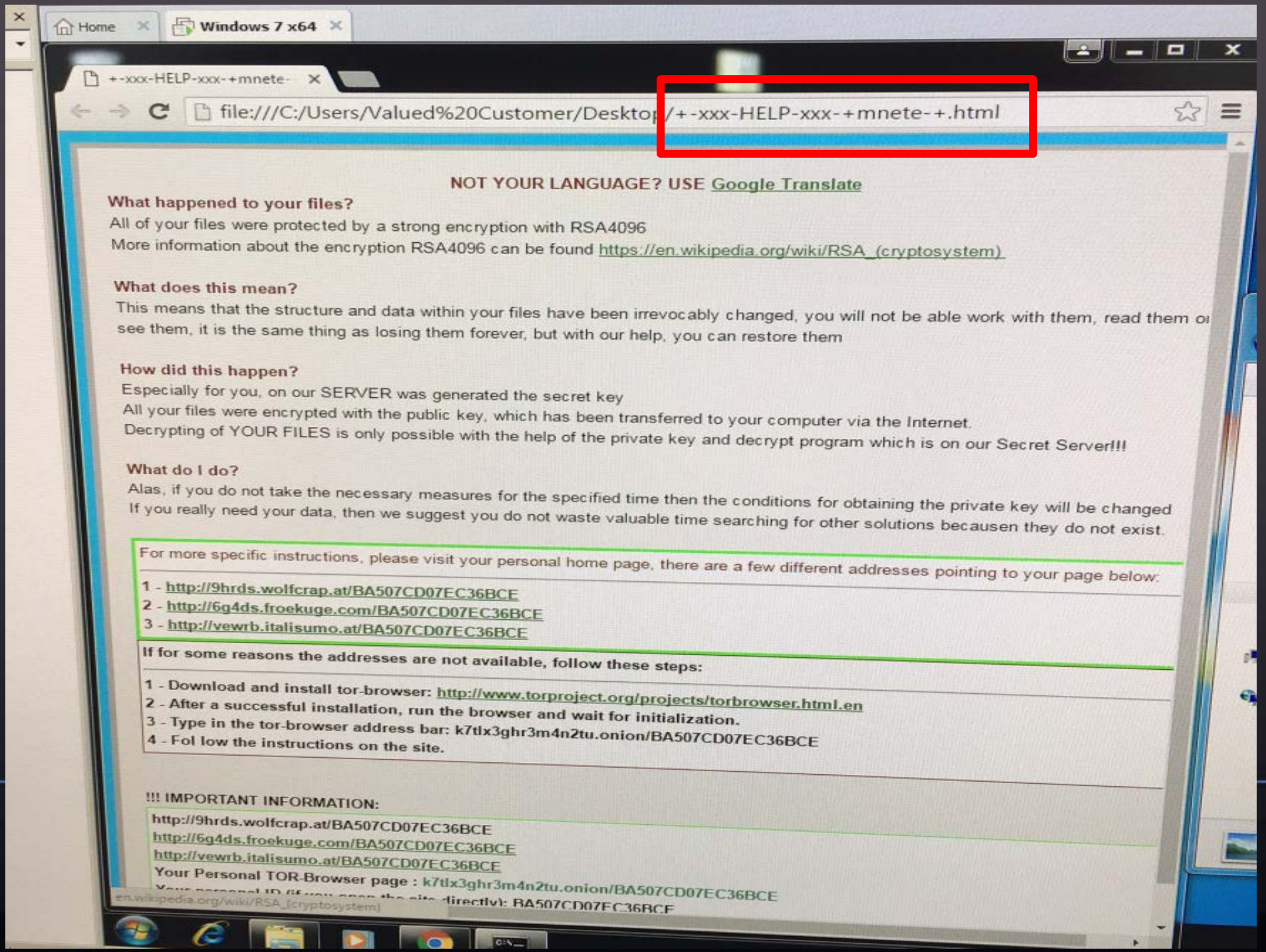
Ransomware

- A form of malware that targets your critical data and systems for the purpose of extortion.
- The ransomware encrypts files and requires a key to decrypt them.
- A timeframe is set and specific instructions are given to purchase the key.

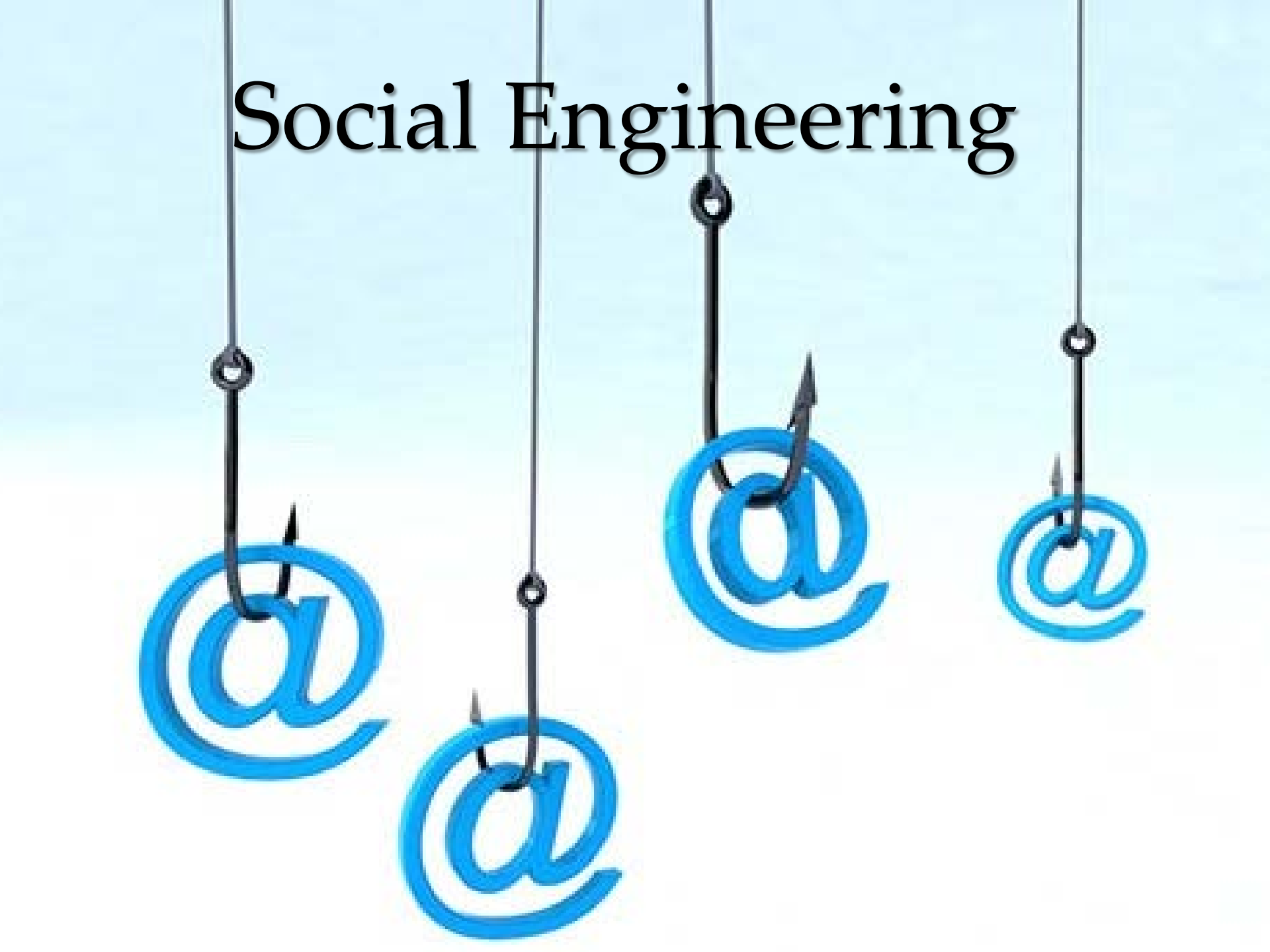
DAVE YOST
Ohio Auditor of State

Ransomware


Pictures library
Includes: 2 locations
Arrange by: Folder
Sample Pictures
+-xxx-HELP-xxx-+mnete-+
+-xxx-HELP-xxx-+mnete-+
+-xxx-HELP-xxx-+mnete-+
+-xxx-HELP-xxx-+mnete-+
+-xxx-HELP-xxx-+mnete-+
+-xxx-HELP-xxx-+mnete-+
download (1)
download (2)
download


Home
Windows 7 x64
+-xxx-HELP-xxx-+mnete-
file:///C:/Users/Valued%20Customer/Desktop/+-xxx-HELP-xxx-+mnete-+.html
NOT YOUR LANGUAGE? USE Google Translate
What happened to your files?
All of your files were protected by a strong encryption with RSA4096
More information about the encryption RSA4096 can be found https://en.wikipedia.org/wiki/RSA_(cryptosystem)
What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read them or
see them, it is the same thing as losing them forever, but with our help, you can restore them
How did this happen?
Especially for you, on our SERVER was generated the secret key
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!!
What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed
If you really need your data, then we suggest you do not waste valuable time searching for other solutions becausen they do not exist.
For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1 - http://9hrds.wolfcrap.at/BA507CD07EC36BCE
2 - http://6g4ds.froekuge.com/BA507CD07EC36BCE
3 - http://vewrb.italisumo.at/BA507CD07EC36BCE
If for some reasons the addresses are not available, follow these steps:
1 - Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2 - After a successful installation, run the browser and wait for initialization.
3 - Type in the tor-browser address bar: k7tlx3ghr3m4n2tu.onion/BA507CD07EC36BCE
4 - Fol low the instructions on the site.
!!! IMPORTANT INFORMATION:
http://9hrds.wolfcrap.at/BA507CD07EC36BCE
http://6g4ds.froekuge.com/BA507CD07EC36BCE
http://vewrb.italisumo.at/BA507CD07EC36BCE
Your Personal TOR-Browser page : k7tlx3ghr3m4n2tu.onion/BA507CD07EC36BCE
directly): BA507CD07EC36BCE
en.wikipedia.org/wiki/RSA_(cryptosystem)

Social Engineering



The Human Element

DAVE YOST
Ohio Auditor of State

www.ohioauditor.gov

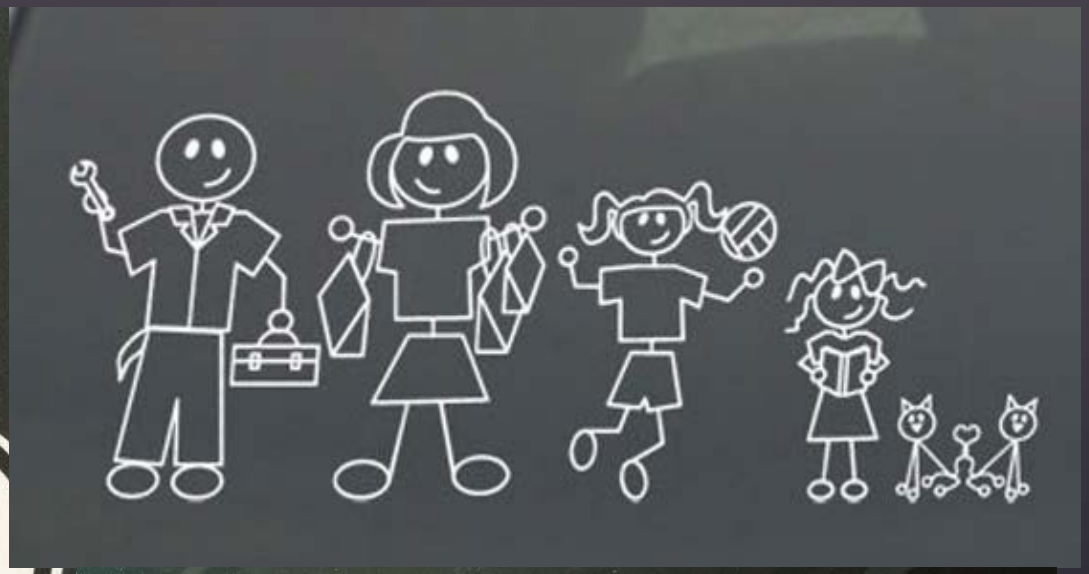
What is it?

- The art of manipulating people by deception to divulge confidential information that is then used for fraudulent purposes.

How do they do it?

- Researching your family, pets, likes, hobbies, cars, work, relatives and co-workers…
- Talking to you personally, searching online, digging through your trash, emails, etc.

What do you advertise?



What do you advertise?

What do you advertise?

Social Engineering Schemes

- Vishing - Voice
- Smishing – SMS texts
- Phishing - Email
- Spear Phishing - Email

DAVE YOST
Ohio Auditor of State

The Human Element

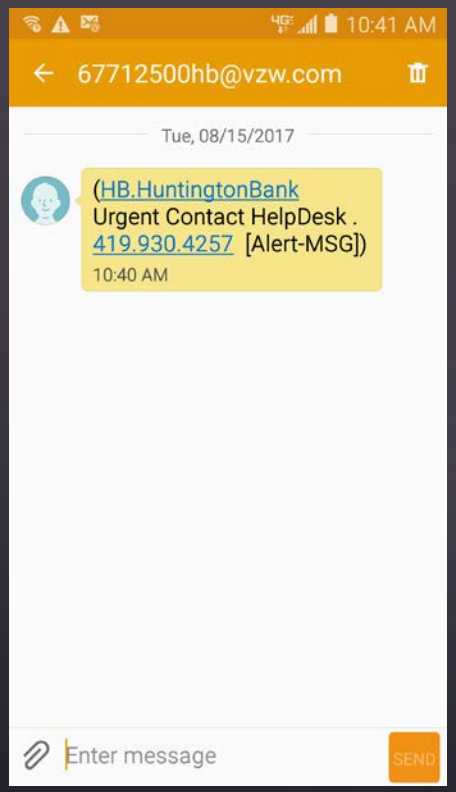
Vishing

- Use of Voice/phone calls to obtain information
- IRS phone scam
- Microsoft Help Desk phone scam
- Google business listings
- Free vacations
- Free security system
- Credit Cards

Vishing Case Study – Madison Co. Ag Society

The treasurer of the agricultural society was targeted by a visher.

Smishing



- Use of SMS text messaging to gain information
- Typically includes a link directing you to sign into something
- May appear as a common name or company

Dad Story ☺

Phishing

- An attempt to obtain sensitive information through email by posing as a trustworthy source.
- Seeking usernames, passwords, credit card details, money, access to computer networks or injecting malware.
- Asks you to click on a link which sends you to fake websites.

You have received a new Doc.5518 via Google Doc

Google Docs <allenderdm@uindy.edu>

You forwarded this message on 10/17/2016 1:18 PM.

Sent: Mon 10/17/2016 1:14 PM

To:

Retention Policy: 180 Days (6 months) Expires: 4/15/2017

This email bypassed my SPAM filters because of the real email address.

Hello,

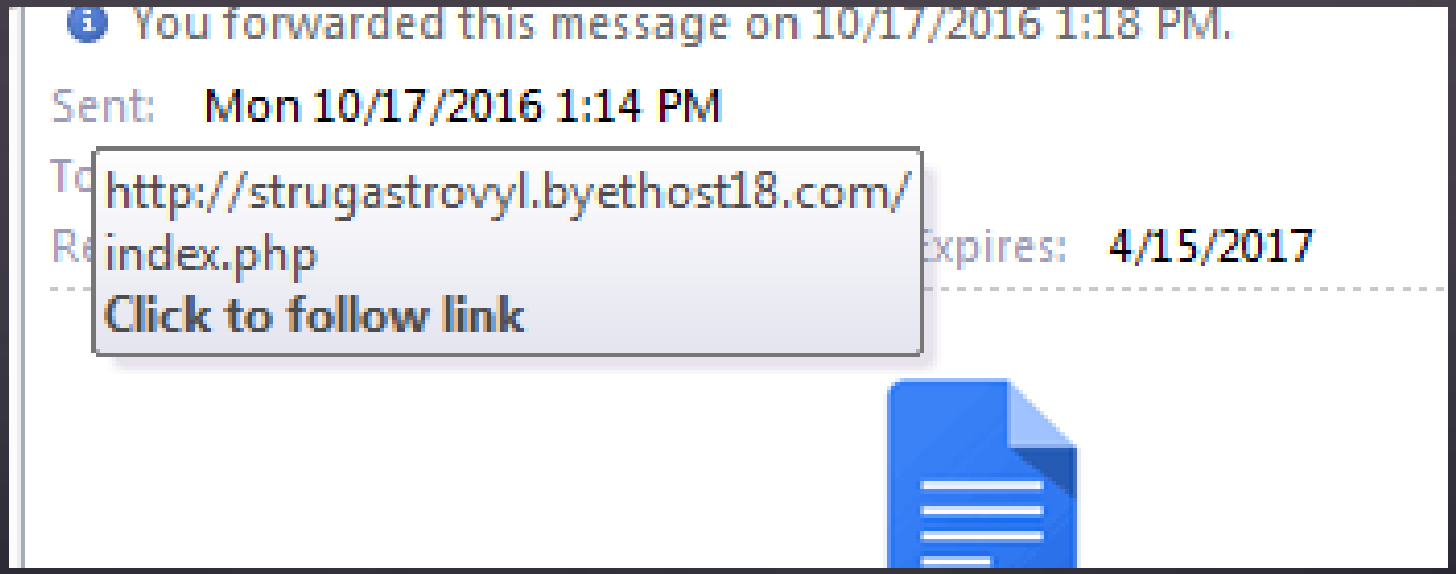
A secure document was sent to you via Google Docs.

Follow the link below to visit Google Docs webpage to view your document.

https://www.google.com/docs_view_now

Best Regards,

Google Team.


You forwarded this message on 10/17/2016 1:18 PM.
Sent: Mon 10/17/2016 1:14 PM
http://strugastrovyl.byethost18.com/
index.php
Click to follow link
Expires: 4/15/2017

What do I look for?

- To whom is it addressed?
- Grammar and spelling
- Deals too good to be true
- Is it somebody you deal with?
- Were you expecting the email?
- Does it include links? (learn to hover!)
- Asks for personal information
- Check domain names/email addresses
- Includes a reason they can't be reached personally
- Deadlines or urgency

How do I know it's fake?

- Act as if they are all fake…
- Do not click links in any email
- Do not call any numbers in an email
- Type the URL in yourself and lookup numbers yourself.

School Story

Spear Phishing Case Study – local school

The treasurer of a local school went on vacation and while she was gone her assistant treasurer received the following emails …

From: Treasurer
Date: Thu, May 5, 2016 at 12:19 PM
Subject: RE:
To: Asst. Treasurer

Hi Asst. Treasurer

Do you have a moment? I am tied up here and there is an urgent matter i need you to take care of. We have a pending invoice from our new vendor and i have asked them to send me a copy of the invoice. Hopefully i should received it later today or tomorrow and i will appreciate if you can process a transfer payment before the cut off time. What details do you need to process this to hit the vendor's account today?

Thanks,
Treasurer

From Treasurer
Date: Thu, May 5, 2016 at 12:56 PM
Subject: RE:
To Asst. Treasurer

Hi Asst. Treasurer

Kindly go ahead and initiate the transfer on my behalf today. Here is the information for the transfer:

Wells Fargo bank
6099 S State St Murray, Utah 84107
Beneficiary: Alberta Rosarita Jones
349 Walnut St. Suite 3075. Cincinnati, OH 45202
Routing: 124002971
Account:

Amount: $38,520

Get back to me with the notification of transfer via email once you get the transfer done.

Thanks,
Treasurer

From: Treasurer
Date: Mon, May 16, 2016 at 8:22 AM
Subject: FW:
To: Asst. Treasurer

Asst. Treasurer

According to Angie's email we need to make a transfer payment today for books today. Kindly email me to let me know if you are available to process this transfer.

Thanks,
Treasurer

16.05.2016, 07:58, Treasurer

Attend to this immediately and make sure the payment goes out today.

Superintendent

This e-mail may contain confidential and/or privileged information and is covered by the Electronic Communications Privacy Act, 18 USC SS 2510-2521. If it does not contain privileged information concerning a

From: Treasurer
Date: Mon, May 16, 2016 at 9:18 AM
Subject: Re:
To: Asst. Treasurer

Please process the transfer payment in the amount of $93,710 today and get back to me with the notification of transfer via email once you get the transfer done. Wiring instructions attached.

Thanks,
Treasurer

Attachment for malware delivery.

This e-mail may contain confidential and/or privileged information and is covered by the Electronic Communications Privacy Act, 18 USC SS 2510-2521. If it does not contain privileged information concerning a BWLSD employee or student, this e-mail and responses are subject to Ohio public records requests. If you are not the intended recipient (or have this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorized copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

Re:

1 message

Treasurer

Mon, May 16, 2016 at 9:18 AM

Reply-To: l@yandex.com>

To: Asst. Treasurer

Please process the transfer payment in the amount of $93,710 today and get back to me with the notification of transfer via email once you get the transfer done. Wiring instructions attached.

Thanks,

Treasurer

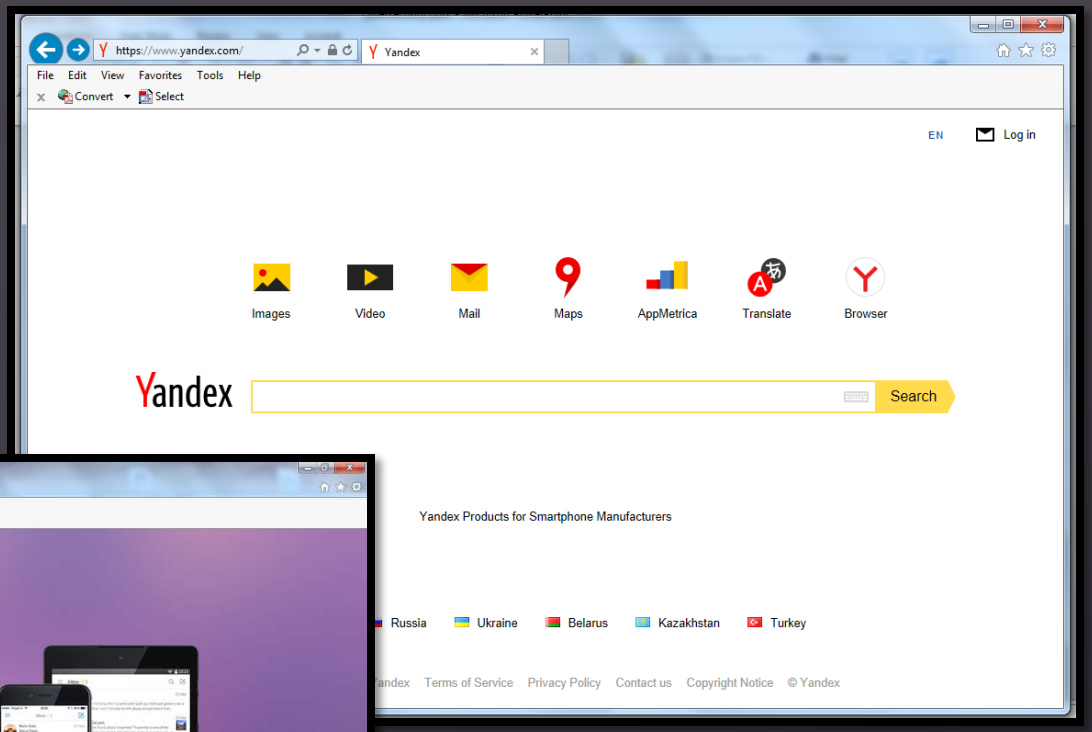
16.05.2016, 15:26, " Asst. Treasurer :

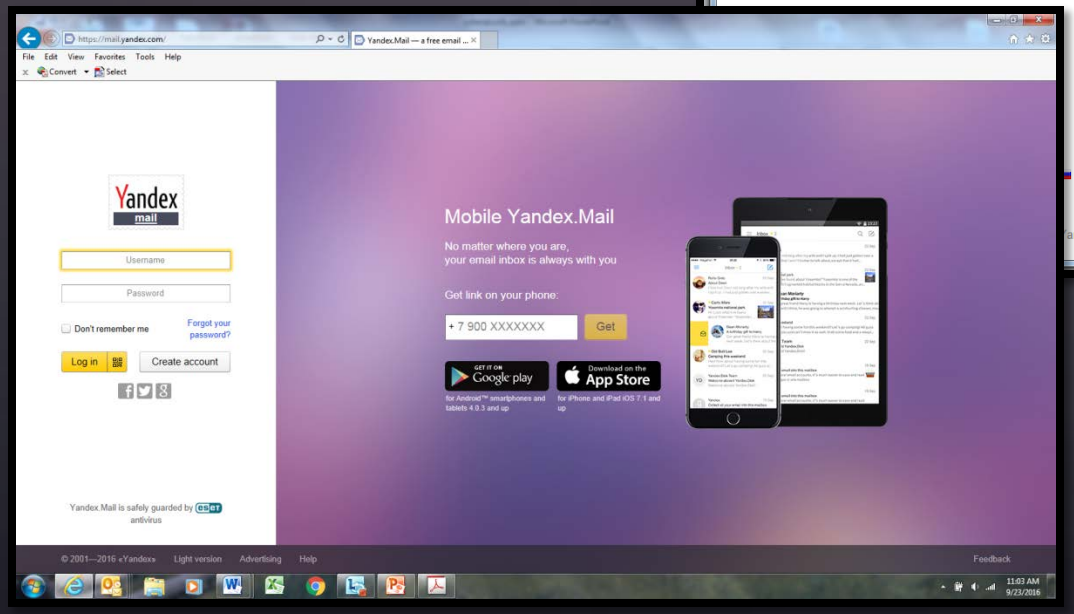
I'm here all day. :)

When she hit reply it actually showed the real email address the suspect used.

Yandex

A Russian based Google-type service with email

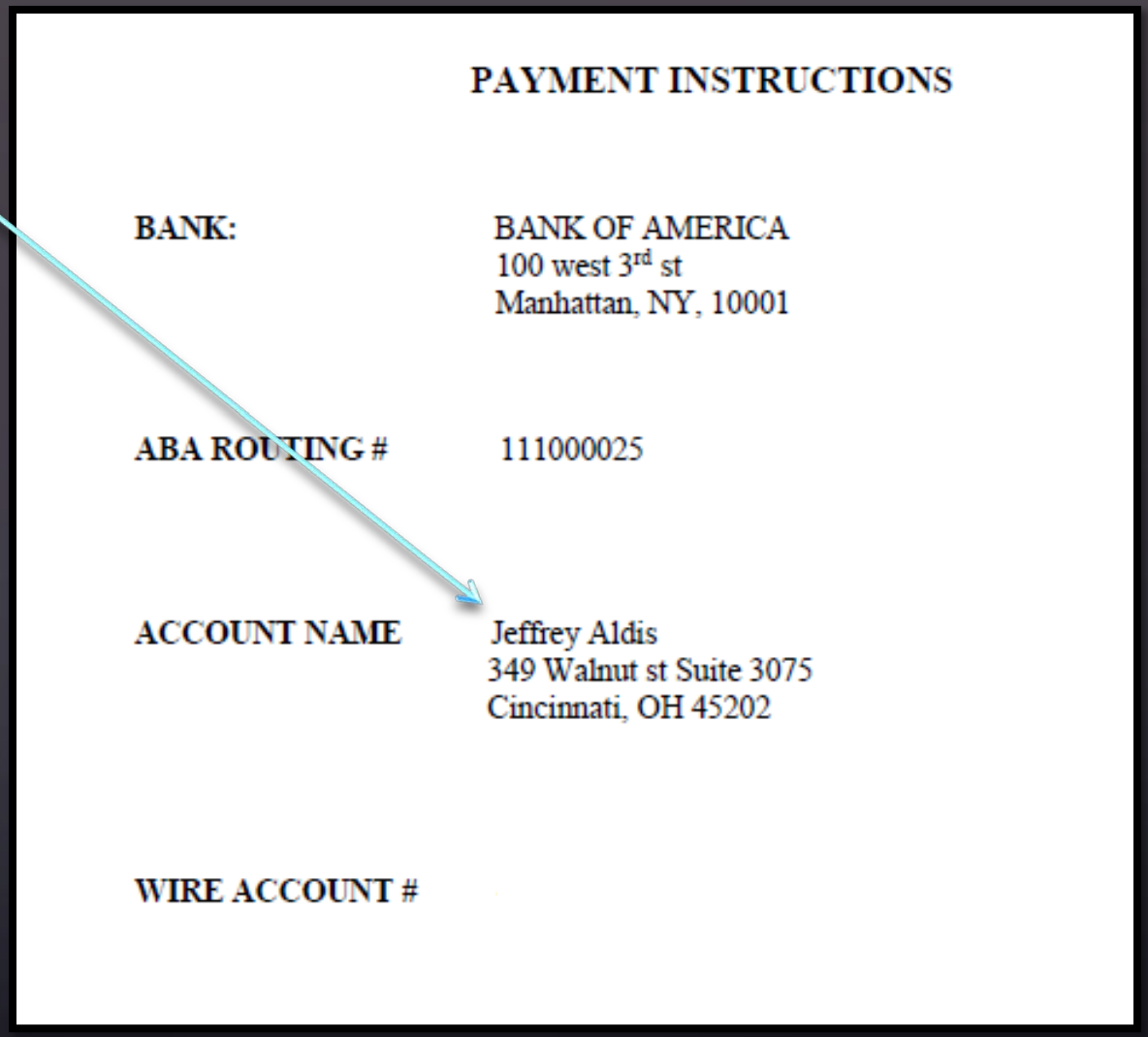




DAVE YOST
Ohio Auditor of State

www.ohioauditor.gov

Google the address or name to see if they even exist.



PAYMENT INSTRUCTIONS

BANK:	BANK OF AMERICA 100 west 3rd st Manhattan, NY, 10001
ABA ROUTING #	111000025
ACCOUNT NAME	Jeffrey Aldis 349 Walnut st Suite 3075 Cincinnati, OH 45202
WIRE ACCOUNT #	

Wi-Fi Safety

What do I look for?

- Don't trust
- Ask an employee for the Wi-Fi network name
- Use a VPN – Virtual Private Network
- If you must use Wi-Fi, do not go to secure sites. Save it until later.
- Use your cell phone as a hotspot

Top 25 passwords

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

DAVE YOST
Ohio Auditor of State

Pineapple's and Pumpkins

Rotten piece's of fruit!

DAVE YOST
Ohio Auditor of State

www.ohioauditor.gov

WiFi Pineapple

172.16.42.1:1471/#/modules/DWall

Most Visited | Drive Me Insane! | WiGLE: Wireless Netw... | ';-- Have I been pwned? P... | Crypto Sheriff | Shodan | AMP Threat Grid

WiFi Pineapple

- Dashboard
- Recon
- Profiling
- Clients
- Modules
  - Manage Modules
  - DWall
  - Evil Portal
  - SSLsplit
- Filters
- PineAP
- Tracking
- Logging
- Reporting
- Networking
- Configuration
- Advanced

DWall Settings

DWall is currently running.

Disable | Stop Listening

URLs

Client	URL
172.16.42.109	http://ocsp.digicert.com /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFEn0vYoYv3YGmMXeQ(%3D%3D
172.16.42.109	http://ip-api.com/json

Cookies

Client	Cookie

Data

Client	Data

Images

Bring Your Own Device

- USB's
- Cell Phones
- Tablets
- Laptops
- Anything requiring connection to your Wi-Fi

- Do you have a policy?

For IT Folks

- IT should be looking at the NIST guidelines and CIS Controls.
  - https://www.cisecurity.org/controls/
  - https://www.nist.gov/cyberframework
- Limit Employee Privileges
- Encrypt Hard Drives
- Have Backups in Place!!!!!

You became a victim -What now?

United States Secret Service

Electronic Crimes Task Force:
www.secretservice.gov/investigation/#field

- Cleveland ECTF - (216) 750-2058
- Cincinnati ECTF - (513) 684-3585

Local Field Offices: www.secretservice.gov/contact/

Federal Bureau of Investigation

Cyber Task Forces:
www.fbi.gov/contact-us/field-offices

- Cleveland Office - (216) 522-1400
- Cincinnati Office - (513) 421-4310

Internet Crime Complaint Center

www.ic3.gov

Mitigation

Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov

Make sure you are within federal requirements regarding reporting information breaches: https://www.us-cert.gov/incident-notification-guidelines

Download the Incident Reporting Form here: https://www.us-cert.gov/report

Contact Information

Nicole Beckwith
Fraud Investigator/Digital Forensic Analyst
Cell Phone: (937) 307-4303
E-mail: NBeckwith@ohioauditor.gov

Follow me on Twitter @NicoleBeckwith
for breaking news, tips and tricks.

Fraud Hotline:
1-866-FRAUD-OH

Ohio Auditor of State
Dave Yost

88 E. Broad St.
Columbus, Ohio 43215
Phone: (800) 282-0370 Fax: (614) 466-4490
Email: ContactUs@OhioAuditor.gov

www.**OhioAuditor**.gov