NEW YORK
STATE OF
OPPORTUNITY.

Office of Information
Technology Services

Cyber Safety and Responsibility for Cyber Citizens

March 13, 2017

What We're Going To Talk About

- My office
- The threats you face
- What you can do to minimize these threats

- Ask questions at any time
- Please keep heckling to a minimum

Cyber Security Is A Shared Responsibility!

New York State
Enterprise Information Security Office

Mission:

The EISO provides cyber security leadership, governance and vision for the State. Our mission is achieved through a risk-based framework, industry best practices, and key partnerships.

New York State
Enterprise Information Security Office

- Within the NYS Office of Information Technology Services (formerly called NYS OFT)
- Formerly NYS Office of Cyber Security
- Oversee and coordinate security services provided to state agencies.
- Security Policy and Standards
- Training, Awareness, Outreach
- Incident Response, Digital Forensics
- Vulnerability and Threat Management
- Security Monitoring and Intelligence

A Normal Day in Your World…

Current Cyber Threat Environment

- Risks go beyond the lost or stolen laptop.
- Threats are becoming increasingly sophisticated and are evolving more rapidly.
- Moving from individual exhibitions of technical skill to global criminal and financial enterprises.

Risk “Reality” Check

- Security firm finds 11 year-old creating malware to steal game passwords
- Worldwide Threat Assessment of the U.S. Intelligence Community lists cybersecurity as the top threat to U.S. security
- 2M Facebook, Google Accounts Compromised
- California Firm Loses $1.5 mil to Cyber Thieves Who Send Loot to China and Russia
- Target (110 million), Neiman Marcus (1.1 million) Michaels (3 million), PF Chang’s & Home Depot (TBD)
- Anthem Blue Cross security breach – 80 Million records

Risk “Reality” Check

- Spam comprises 1 in 1.51 e-mails worldwide

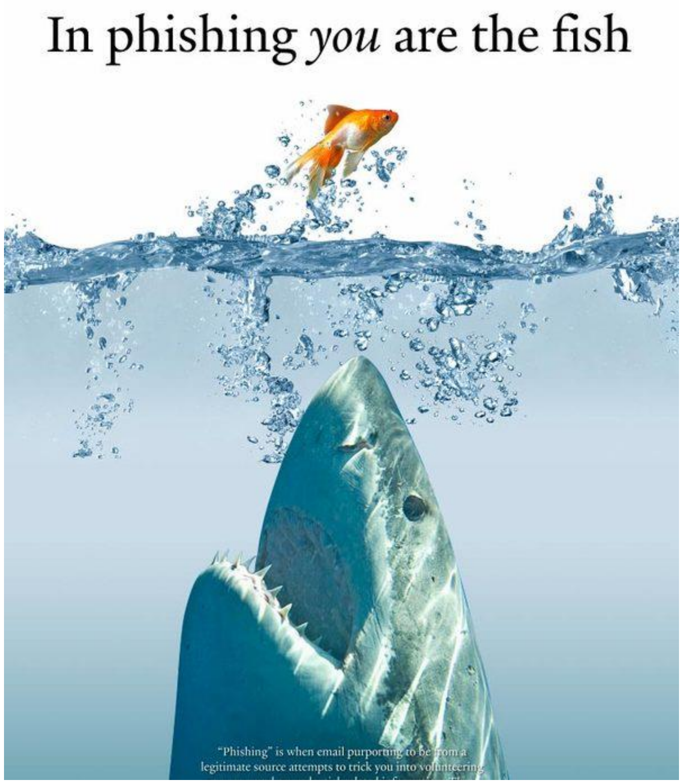
- 87% of spam messages contained a URL hyperlink
- 76% of spam delivered by spam botnets
- 29 Billion estimated global email spam/day

- Security Breaches on the rise
- +700% (1 →8) increase in the number of security mega breaches with more than 10 Million identities exposed
- 552 Million total identities exposed

http://www.gao.gov/assets/660/652170.pdf

Phishing Scams

What are Phishing Scams?

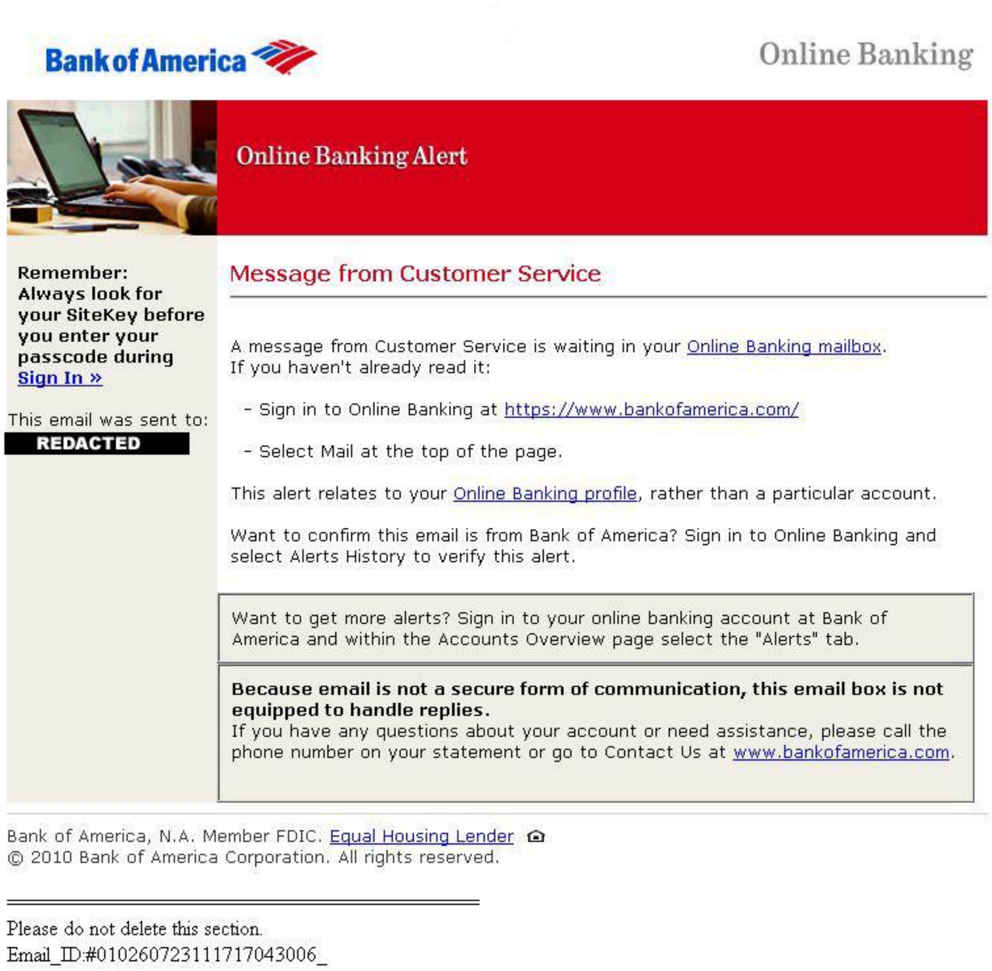

In phishing *you* are the fish
"Phishing" is when email purporting to be from a
legitimate source attempts to trick you into volunteering

Phishing Scam –

- Phishing emails appear to come from a **financial institution,** or other company or trusted source with whom the recipient **may do business**.
- The message attempts to trick the recipient into **clicking a link or attachment**.
- The link may take the user to a site with malicious code; a corrupt attachement may do the same.

Phishing Scam

If it sounds too good to be true…



Online Banking Alert

Remember:
Always look for your SiteKey before you enter your passcode during
Sign In »

This email was sent to:
REDACTED

Message from Customer Service

A message from Customer Service is waiting in your Online Banking mailbox.
If you haven't already read it:

- Sign in to Online Banking at https://www.bankofamerica.com/
- Select Mail at the top of the page.

This alert relates to your Online Banking profile, rather than a particular account.

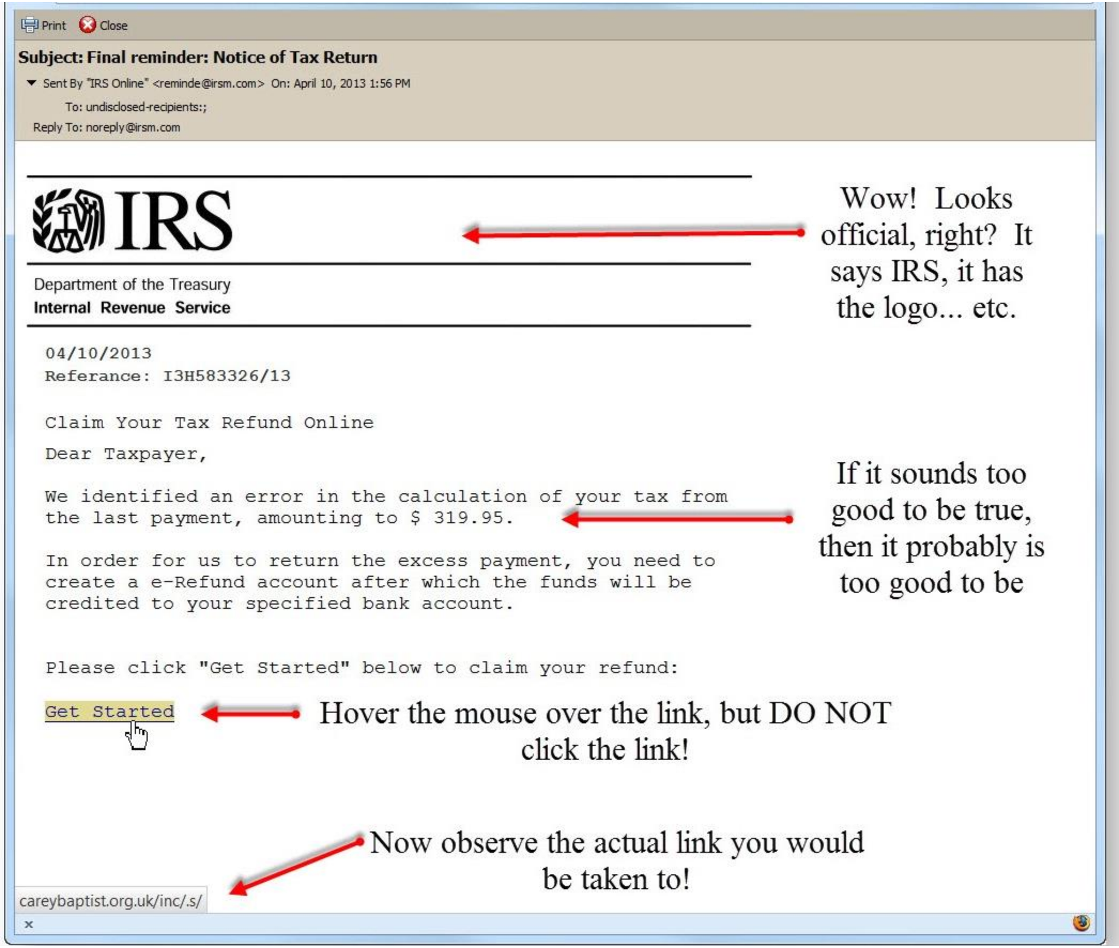
Want to confirm this email is from Bank of America? Sign in to Online Banking and select Alerts History to verify this alert.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

Because email is not a secure form of communication, this email box is not equipped to handle replies.
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2010 Bank of America Corporation. All rights reserved.

Please do not delete this section.
Email_ID:#010260723111717043006_



Subject: Final reminder: Notice of Tax Return

Sent By "IRS Online" <reminde@irsm.com> On: April 10, 2013 1:56 PM

To: undisclosed-recipients:;

Reply To: noreply@irsm.com

IRS

Department of the Treasury
Internal Revenue Service

04/10/2013
Referance: I3H583326/13

Claim Your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to $ 319.95.

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

careybaptist.org.uk/inc/.s/

Wow! Looks official, right? It says IRS, it has the logo… etc.

If it sounds too good to be true, then it probably is too good to be

Hover the mouse over the link, but DO NOT click the link!

Now observe the actual link you would be taken to!

Some are Seasonal or Opportunistic

Valentine’s Day…

Think of when taxes are due…

Malvertising

Malvertising

- Is a relatively new attack vector for cyber criminals that is quickly on the rise.

- With malvertising, fake malicious ads are delivered (often via advertising networks) to well-known websites as a way to reach millions of users at once on websites they normally trust.

- After visiting the trusted website, malvertising attacks are presented and can download malicious code directly onto a user's computer when the victim views the compromised ad.

- Millions of users have been infected by malvertising threats recently, as evidenced by the high-profile attacks on The New York Times, Gizmodo, TechCrunch, WhitePages.com and other sites.

The New York Times

Thursday, September 16, 2010 Last Update: 12:28 PM ET

Poverty Rate Rose Sharply in 2009, Says Census Bureau
By ERIK ECKHOLM
13 minutes ago
The report said that 44 million people, or one in seven residents, lived in poverty in the United States in 2009, the highest rate since 1994.
- Text of the Report
- Post a Comment
- Comments

Doug Mills/The New York Times

Senators Press Geithner on China Policy
By SEWELL CHAN 7 minutes ago
As Treasury Secretary Timothy F. Geithner listed complaints about China's economic policies, senators expressed impatience with the administration.
- Energy Costs Push Up U.S. Producer Prices 9:42 AM ET

Paterson Says He'll Lay Off Workers Before Jan. 1

In Britain, Pope Criticizes Response to Abuse Crisis
By RACHEL DONADIO and ALAN COWELL 9:22 AM ET
Pope Benedict XVI on Thursday

OP-ED: JIMMY CARTER
North Korea Wants to Make a Deal
Pyongyang is sending strong signals about its willingness to resume peace negotiations.
- Collins: Mr. Smith Goes to Anchorage | Comments (89)
- Kristof: A Boy and a Bicycle(s)
- Editorial: The Tea Party's Snarl

Log in to see what your friends are sharing on nytimes.com. Privacy Policy | What's This?

- In Iraq, Clearer Image of U.S. Support
- Yankees Caps Are Popular Among Criminals

At 12:10 PM ET

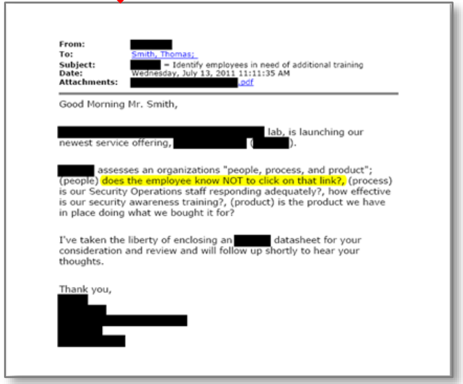
S.&P. 500	Dow	Nasdaq
1,119.71	10,547.99	2,289.72
-5.34	-24.74	-11.60
-0.47%	-0.23%	-0.50%

Source: http://www.net-security.org/secworld.php?id=9305

Banking Trojans – Botnets
Zeus Attacks

Banking Trojan Overview

Attacker crafts a convincing e-mail with <u>malicious links or attachments</u> and sends it to likely targets.



From: [redacted]
To: Smith, Thomas;
Subject: [redacted] – Identify employees in need of additional training
Date: Wednesday, July 13, 2011 11:11:35 AM
Attachments: [redacted].pdf

Good Morning Mr. Smith,

[redacted] lab, is launching our newest service offering, [redacted] ([redacted]).

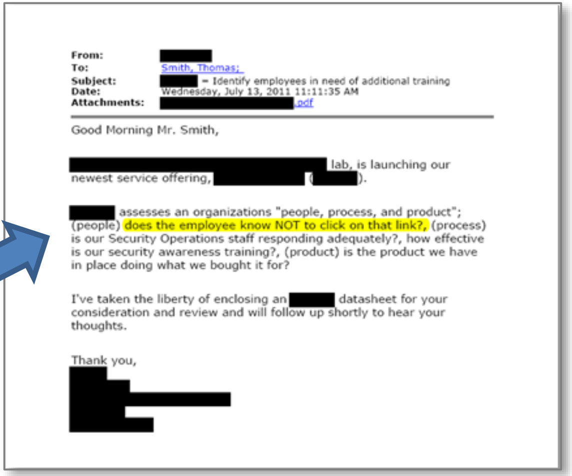
[redacted] assesses an organizations "people, process, and product"; (people) does the employee know NOT to click on that link?, (process) is our Security Operations staff responding adequately?, how effective is our security awareness training?, (product) is the product we have in place doing what we bought it for?

I've taken the liberty of enclosing an [redacted] datasheet for your consideration and review and will follow up shortly to hear your thoughts.

Thank you,

[redacted]

Banking Trojan Overview



From: [redacted]
To: Smith, Thomas;
Subject: [redacted] – Identify employees in need of additional training
Date: Wednesday, July 13, 2011 11:11:35 AM
Attachments: [redacted].pdf

Good Morning Mr. Smith,

[redacted] lab, is launching our newest service offering, [redacted] ([redacted]).

[redacted] assesses an organizations "people, process, and product"; (people) does the employee know NOT to click on that link?, (process) is our Security Operations staff responding adequately?, how effective is our security awareness training?, (product) is the product we have in place doing what we bought it for?

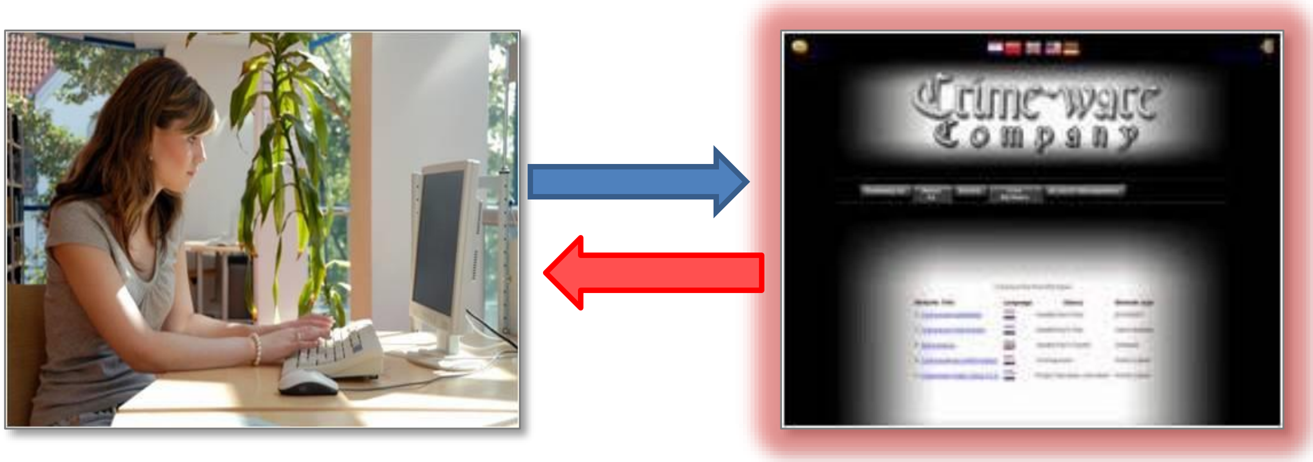
I've taken the liberty of enclosing an [redacted] datasheet for your consideration and review and will follow up shortly to hear your thoughts.

Thank you,

[redacted]

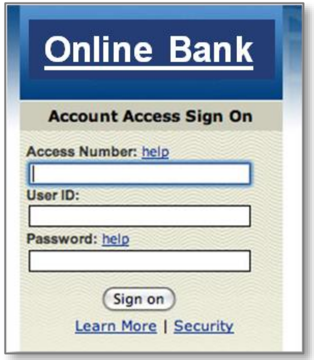
Recipient clicks on a <u>link</u> or opens an <u>attachment</u>.

Banking Trojan Overview



User’s PC is exploited to download and install malicious software that quickly hides itself from view/detection.

Banking Trojan Overview



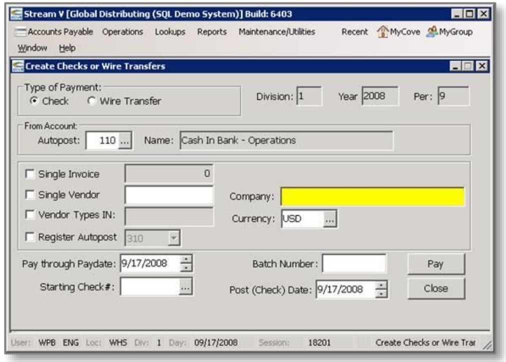
Online Bank

Account Access Sign On

Access Number: help

User ID:

Password: help



Stream V [Global Distributing (SQL Demo System)] Build: 6403

Create Checks or Wire Transfers

Type of Payment: ● Check ○ Wire Transfer

Division: 1 Year 2008 Per: 9

From Account

Autopost: 110 ... Name: Cash In Bank - Operations

□ Single Invoice 0

□ Single Vendor

Company:

□ Vendor Types IN:

Currency: USD ...

□ Register Autopost 310

Pay through Paydate: 9/17/2008

Batch Number:

Starting Check#: ...

Post (Check) Date: 9/17/2008

User: WPB ENG Loc: WHS Div: 1 Day: 09/17/2008 Session: 18201 Create Checks or Wire Trar

Attacker uses the <u>stolen</u> credentials to initiate additional <u>fraudulent</u> transactions from the victim’s account.

Other NYS Local Government Cyber Heists

- Town of Poughkeepsie, January 2010
  - Four of nine successful attempts to electronically steal money from local bank.
  - $378,000 transferred to accounts in the Ukraine.
  - Town officials say all money restored (months later)
- Town of Pittsford, June 2011
  - $139,000 transferred to accounts in Russia and Ukraine.
- Thefts investigated by local police, FBI and US Secret Service.

Ransomware

Ransomware

- Encrypts files on a victim’s computer and any connected shares or drives

- Files are held until a ransom is paid, allowing the victim to regain access to the files.

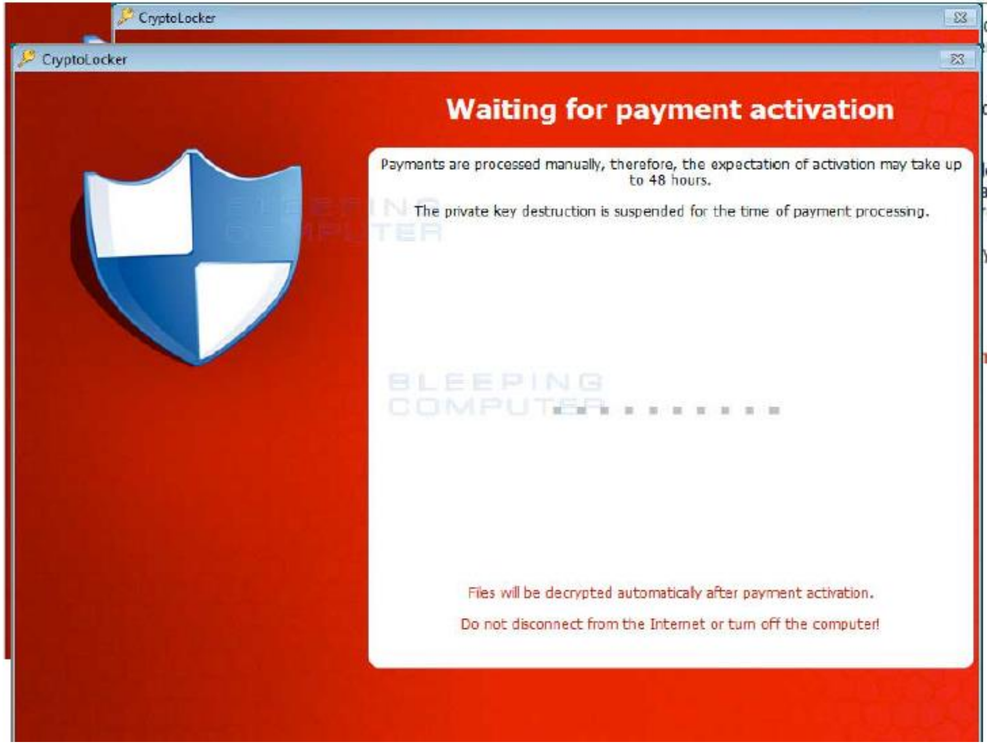
- Ransomware is often spread through a phishing email, a seemingly legitimate email that tricks users into clicking on a link or attachment.

- Includes Cryptolocker, Cryptowall, Jigsaw

-

  Ilion (2014) – Ransomware incidents affect government computers

Cryptolocker



Waiting for payment activation

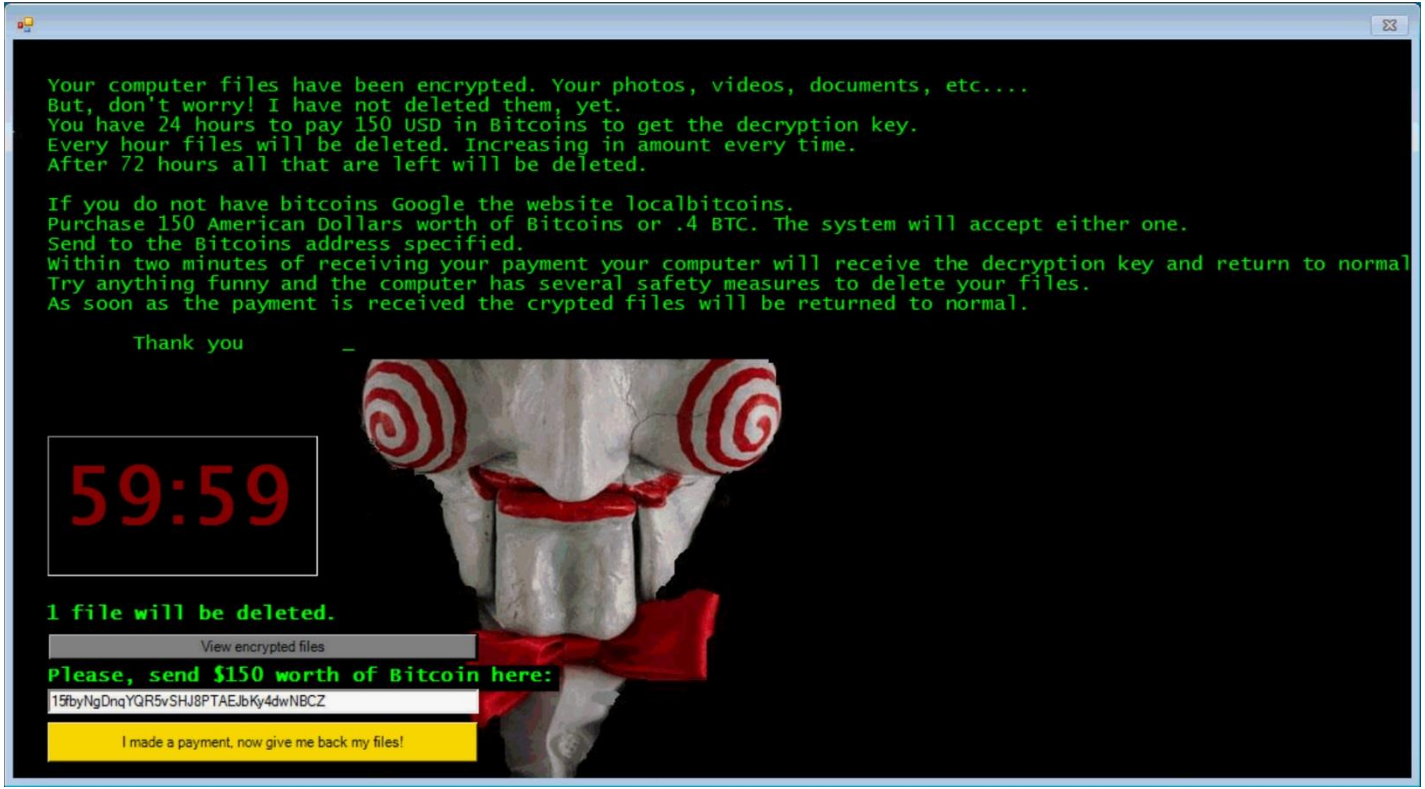
Payments are processed manually, therefore, the expectation of activation may take up to 48 hours.

The private key destruction is suspended for the time of payment processing.

Files will be decrypted automatically after payment activation.

Do not disconnect from the Internet or turn off the computer!

Jigsaw



```
Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.

       Thank you
```

59:59

1 file will be deleted.

Please, send $150 worth of Bitcoin here:

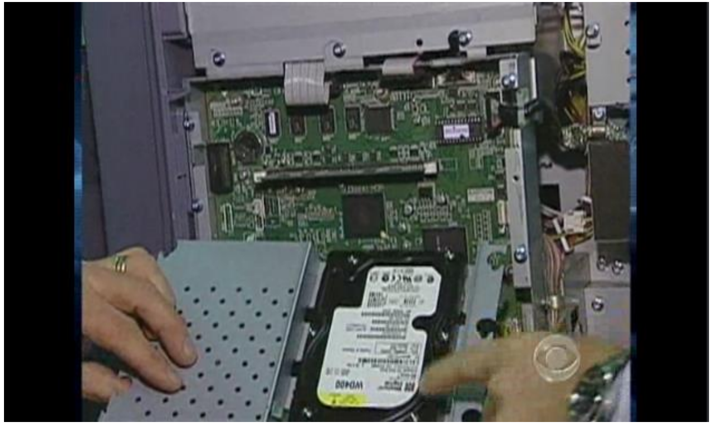
15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

Cyber Crime

Commercialization of Cyber Crime

Data Disposal

Copier Machines – A Security Risk



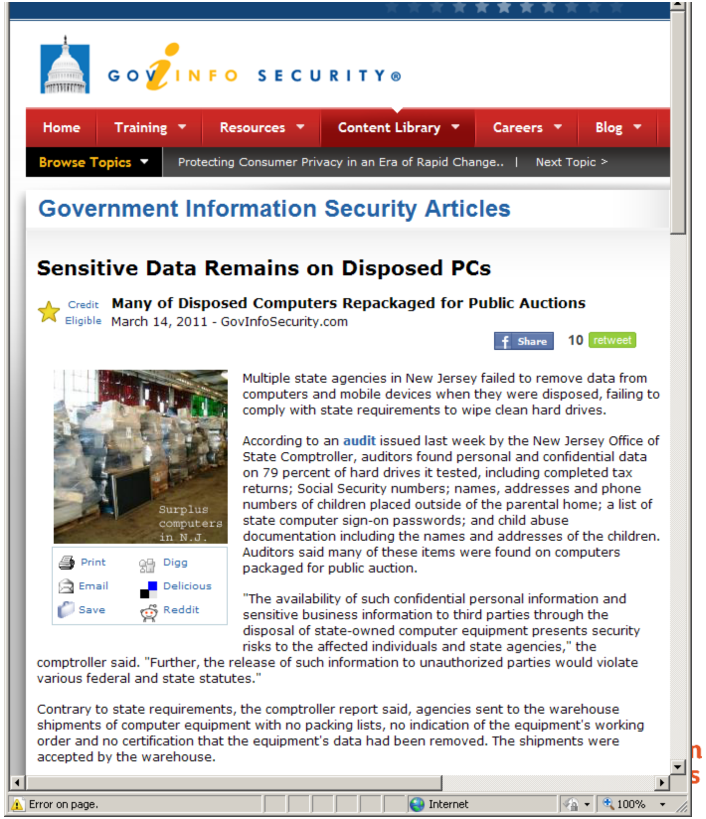
Recent news coverage has highlighted the fact that confidential information can be recovered from printers, copiers and similar devices after they are sent to surplus or returned to the vendor at the end of their lease. Some of the confidential information recently reported to be found on these machines included social security numbers, birth certificates, bank records, income tax forms, medical records, and pay stubs with names.

Source: http://www.cbsnews.com/video/watch/?id=6412572n
OCS Newsletter: http://www.cscic.state.ny.us/cscorner/news/2010-07.cfm

Sensitive Data Remains on Disposed PCs

March 14, 2011 - According to an audit issued by the New Jersey Office of State Comptroller, auditors found personal and confidential data on 79 percent of hard drives it tested, including completed tax returns; Social Security numbers; names, addresses and phone numbers of children placed outside of the parental home; a list of state computer sign-on passwords; …

http://www.govinfosecurity.com/articles.php?art_id=3427&rf=2011-03-15-eg



Government Information Security Articles

Sensitive Data Remains on Disposed PCs

Credit Eligible **Many of Disposed Computers Repackaged for Public Auctions**

March 14, 2011 - GovInfoSecurity.com

Multiple state agencies in New Jersey failed to remove data from computers and mobile devices when they were disposed, failing to comply with state requirements to wipe clean hard drives.

According to an audit issued last week by the New Jersey Office of State Comptroller, auditors found personal and confidential data on 79 percent of hard drives it tested, including completed tax returns; Social Security numbers; names, addresses and phone numbers of children placed outside of the parental home; a list of state computer sign-on passwords; and child abuse documentation including the names and addresses of the children. Auditors said many of these items were found on computers packaged for public auction.

"The availability of such confidential personal information and sensitive business information to third parties through the disposal of state-owned computer equipment presents security risks to the affected individuals and state agencies," the comptroller said. "Further, the release of such information to unauthorized parties would violate various federal and state statutes."

Contrary to state requirements, the comptroller report said, agencies sent to the warehouse shipments of computer equipment with no packing lists, no indication of the equipment's working order and no certification that the equipment's data had been removed. The shipments were accepted by the warehouse.

The Internet Of Things (IOT)

The Internet of Things

As more and more devices are connected to the Internet, they are exposed to potential compromise and abuse.

Actionable Steps

What Should You Do?

1. Learn of and use basic security principles.

- ✓ Employ basic security practices, such as using strong passwords and changing your passwords regularly
- ✓ Internet usage guidelines or policy
- ✓ Establish rules of behavior describing how to handle and protect citizen information and other vital data

What Should You Do?

2. Protect information, computers and networks from cyber attacks.

✓ Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

✓ Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

What Should You Do?

3. Provide firewall security for your Internet connection.

- ✓ A firewall is a set of related programs that prevent outsiders from accessing data on a private network.
- ✓ Make sure the operating system’s firewall is enabled or install free firewall software available online.
- ✓ If employees work from home, ensure that their home system(s) are protected by a firewall.

What Should You Do?

4. Mobile device security

- ✓ Mobile devices can create significant security challenges, especially if they hold confidential or personal information or can access official networks.
- ✓ Password-protect your device devices, encrypt data, and install security apps to prevent criminals from stealing information while the device is on public networks.
- ✓ Do you know what to do if your device is lost or stolen?

What Should You Do?

5. Make backup copies of important data.

- ✓ Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, financial files.
- ✓ Backup data automatically if possible, or at least weekly and store the copies securely, either offsite or in the cloud.

What Should You Do?

6. Control physical access to your computers and create user accounts for each user.

- ✓ Prevent access or use of computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended.
- ✓ Make sure a separate user account is created for each user and require strong passwords.
- ✓ Administrative privileges should only be given to those that need it.

What Should You Do?

7. Secure your Wi-Fi networks.

- ✓ If you have a Wi-Fi network for your home, make sure it is secure, encrypted, and hidden.
- ✓ To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

****Do not log into accounts, especially financial accounts, when using public wireless networks.****

What Should You Do?

8. Limit access to data and information, and limit authority to install software.

- ✓ Individuals should only be given access to the specific data/systems needed for their jobs, and should not be able to install any software without permission.

What Should You Do?

9. Employ best practices on payment cards.

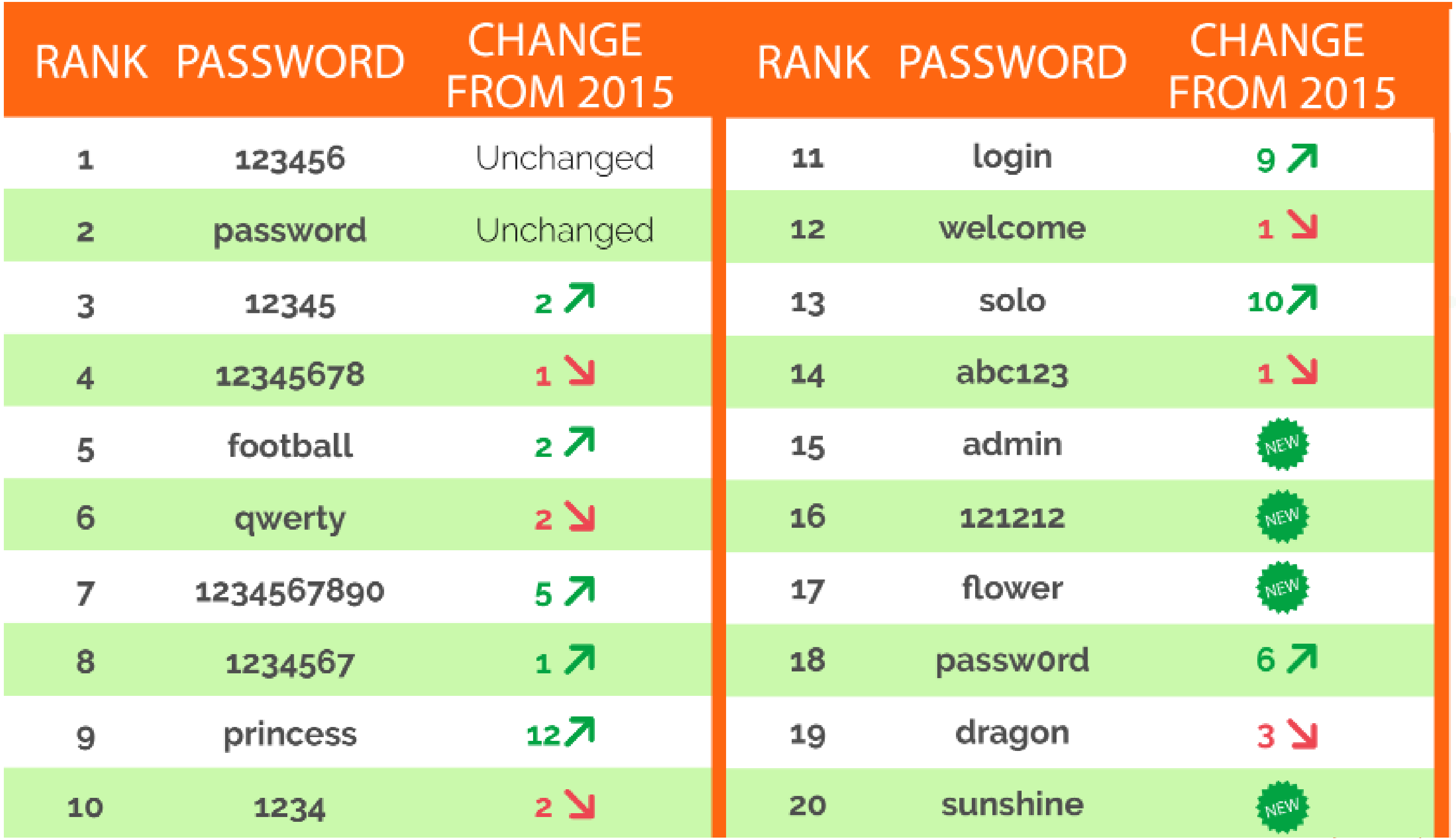
- ✓ Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used.
- ✓ You may also have additional security obligations pursuant to agreements with your bank or processor.
- ✓ Isolate payment systems from other, less secure programs and don’t use the same computer to process payments and surf the Internet.

What Should You Do?

10. Passwords and authentication.

- ✓ Use unique passwords and change passwords on a regular basis (90 days?)
- ✓ Consider using multifactor authentication that requires additional information beyond a password to gain entry.
- ✓ Consider using a passphrase
  - ✓ “I Really Like Pizza!”
  - ✓ “I Re@lly L!ke P!zz@”
  - ✓ L!kEm@il022017

Password Wall of Shame



RANK	PASSWORD	CHANGE FROM 2015
1	123456	Unchanged
2	password	Unchanged
3	12345	2 ↗
4	12345678	1 ↘
5	football	2 ↗
6	qwerty	2 ↘
7	1234567890	5 ↗
8	1234567	1 ↗
9	princess	12 ↗
10	1234	2 ↘
11	login	9 ↗
12	welcome	1 ↘
13	solo	10 ↗
14	abc123	1 ↘
15	admin	NEW
16	121212	NEW
17	flower	NEW
18	passw0rd	6 ↗
19	dragon	3 ↘
20	sunshine	NEW

Passwords are like toothbrushes…
they're best when fresh & should not be shared.

20th Annual NYS Cyber Security Conference

June 7-8, 2017

Cyber Security Your – Mine – Everyone's Responsibility!

NYS Office of Information Technology Services

Enterprise Information Security Office

www.its.ny.gov/eiso

Cyber.Outreach@its.ny.gov

518-242-5200