From: Gregory Diefenbach on behalf of Gregory Diefenbach <gregg.diefenbach@neric.org>

To: Adrienne Leon; Alison Gorton; Althea Johnson; "Amanda Wing"; Andrew Giaquinto (agiaquinto@sgcsd.net); Anjelieeque Martinez (martineza@scolonie.org); Anthony DiPace (adipace@sharonsprings.org); Audrey Hendricks; bcarey@schodack. k12. ny. us (bcarey@schodack.k12.ny.us); bill Hogan (bhogan@albany.k12.ny.us); Brady Regan - Forecast5 (bregan@forecast5analytics.com); Breen, Taryn; Brenda Kane (brkane@bhbl.org); Carbon, Sharifa; Carl; Carrie Nyc-Chevrier (cnycchevrier@niskyschools.org); chris abdoo (cabdoo@bhbl.org); Chris Karwiel; Chris Ruberti (rubertich@mohonasen.org); Christina. coughlin (christina.coughlin@nysed.gov); Colleen Dicaprio; cook, Ruth; Edson, Larry; Elaine Hopper; Filicia DAversa; Fisher, Sherri; francis rielly (frielly@voorheesville.org); Gregory Diefenbach; Hilary Hofstein; HOTALING, ADAM; J. Lana Hower; "Jacqlene McAllister"; jamie maloney (jmaloney@niskyschools.org); Jay O"Connor (jay.oconnor@questar.org); Jeff Bryant (Jeff@bryantasset.com); Jeffrey Bradt; Jeffrey Luks; Jeffrey Miriello (jmiriello@cairodurham.org); Jeffrey Rivenburg (jrivenburg@duanesburg.org); Jennifer Bennett; Joanne Moran (jmoran@rcscsd.org); John Mattox; John Rizzo (rizzoj@guilderlandschools.net); John Tamburello; Joseph Greco; Joseph Karas (JKaras@schalmont.net); Joseph. Gilchrist@nysed. gov (Joseph.Gilchrist@nysed.gov); jsullivan@nbtbank.com; Judy Frost; Judy Kehoe (jkehoe@bcsd.neric.org); Karen Capozzi (kcapozzi@berlincentral.org); Kathy Beardsley (kbeardsley@questar.org); Kathy Wetmore (wetmkath@shenet.org); kcietek@menands.org; Keith Heid - watervliet (kheid5@vlietschools.org); Kevin Fottrell (kfottrell@newlebanoncsd.org); Kimberly Duran; Lewis, Kimberly; Lisa Kyer; Lyn Derway; mangrisano@wynantskillufsd.org; Marc Iorio; marco zumbolo (zumbolom@bpcsd.org); Mark Jones; meghan heimroth (mheimroth@rcsd.k12.ny.us); Michele Jones; mike ouimet (ouimetm@averillpark.k12.ny.us); Mike Vespi (mvespi@forecast5analytics.com); Mike. Los@questar. org (Mike.Los@questar.org); Neil T. Sanders (sandersn@guilderlandschools.net); "Paul Overbaugh"; rebecca hull (hullrebe@shenet.org); Richard Longhurst; Robert Bonaker; robyn bhend (bhendr@greenville.k12.ny.us); rose fiddemon (Rose.fiddemon@questar.org); "ryusko@gfsd.org"; sarah blood (sblood@schoharie.k12.ny.us); Sarah Morrison; Scott Hoot (scotthoot@ncolonie.org); Scott Whittmore - Queensbury UFSD (swhittemore@queensburyschool.org); Sheila Gilroy; Stacy King-McElhiney (sking@bkwschools.org); Stacy Mackey (smackey@cohoes.org); Stephanie Steinhart (ssteinhart@brunswickcsd.org); stephen McNally (stephen.mcnally@nysed.gov); STEVE SCHLOICKA (sschloicka@poughkeepsieschools.org); Tabatha Biggane; Terry Gillooley (Terry.gillooley@middleburghcsd.org); Tim Hilker; Timothy Mundell; Tracey Fraleight (fraleight@crcs.k12.ny.us); turcottec@wcsd.org; WagerLi@egcsd.org; Wendy Ashley; Wes Clark (wclark@hoosicvalley.k12.ny.us); Zautner, Steve

Subject: Cyber presentation from 6/14

Date: Tuesday, June 18, 2019 10:01:50 AM

Attachments: NERIC BOCES Presentation - June 2019 FINAL.pdf

Importance: High

The attached is the cybersecurity presentation that was made at the 6/14 CUSBO meeting…Gregg

Gregg Diefenbach, NYSRSBA
Deputy Director for Administrative and Management services
900 Watervliet-Shaker Road
Albany, NY 12205
518-464-5150
Gregg.Diefenbach@neric.org

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

Cyber Safety and Responsibility for Cyber Citizens

June 18, 2019

Cyber Security Is A Shared Responsibility!

New York State
Chief Information Security Office

Mission:

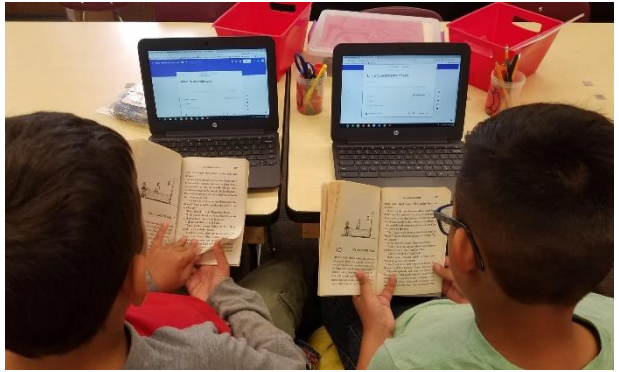
The CISO provides cyber security leadership, governance and vision for the State. Our mission is achieved through a risk-based framework, industry best practices, and key partnerships.

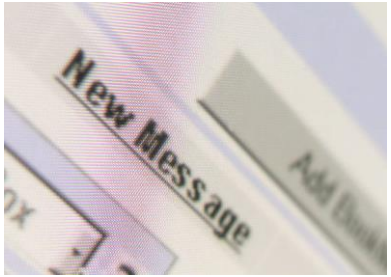
New York State
Chief Information Security Office

- Within the NYS Office of Information Technology Services
- 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…

NERIC
Northeastern
Regional
Information
Center

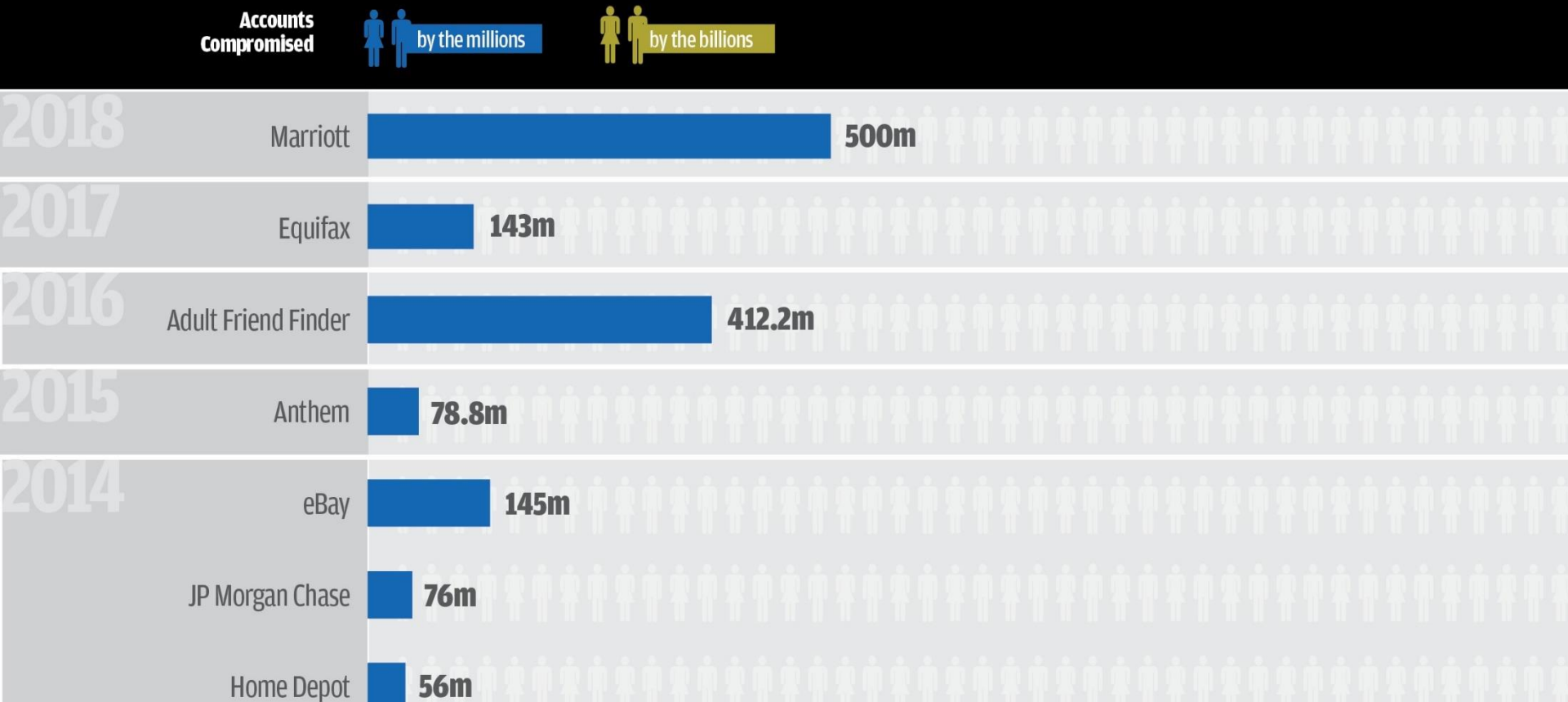




Current Cyber Threat Environment

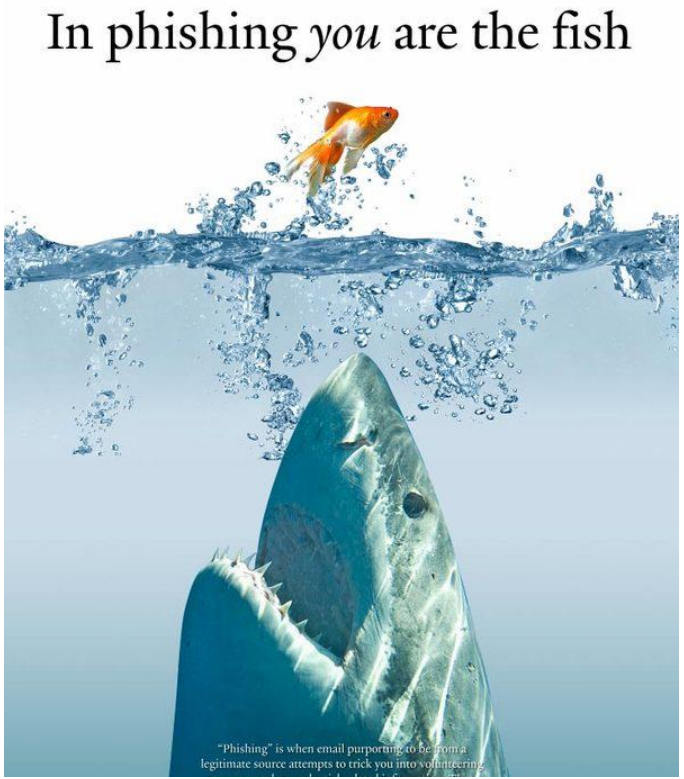
- **Risks go beyond the lost or stolen laptop.**
- **Threats are becoming increasingly sophisticated and are evolving more rapidly.**
- **Moving from individual exhibitions of technical skill to global criminal and financial enterprises.**

Biggest DATA BREACHES of the 21st century



Biggest DATA BREACHES of the 21st century

What are Phishing Scams?



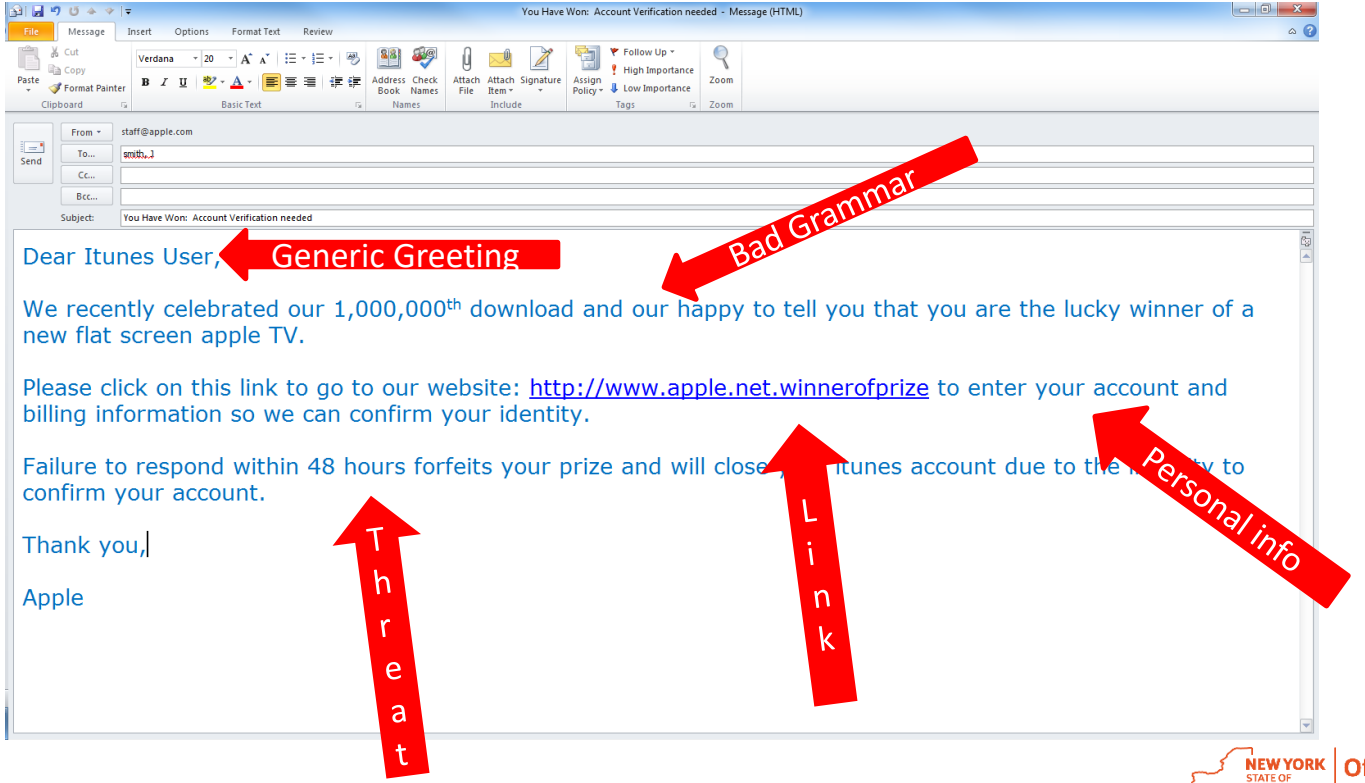
Phishing Scam –

- **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 attachment may do the same.**

Phishing Scam

If it sounds too good to be true…

Phishing Messages (text or E-mail)



Print Close

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

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

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.

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

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

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

Now observe the actual link you would be taken to!

careybaptist.org.uk/inc/.s/

Some are seasonal or opportunistic

Valentine's Day…

Think of when taxes are due…

Malvertising

Malvertising

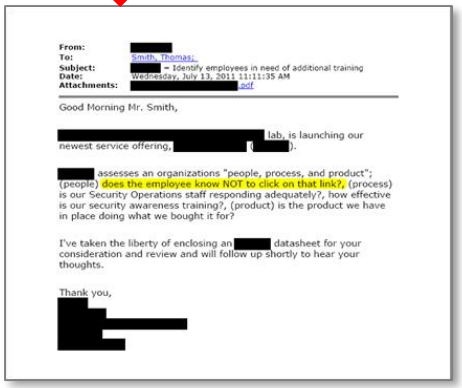
- Is a relatively new attack vector for cyber criminals that is quickly on the rise.
- With malvertising, fake malicious ads are delivered (often via advertising networks) to well-known websites as a way to reach millions of users at once on websites they normally trust.
- After visiting the trusted 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.

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

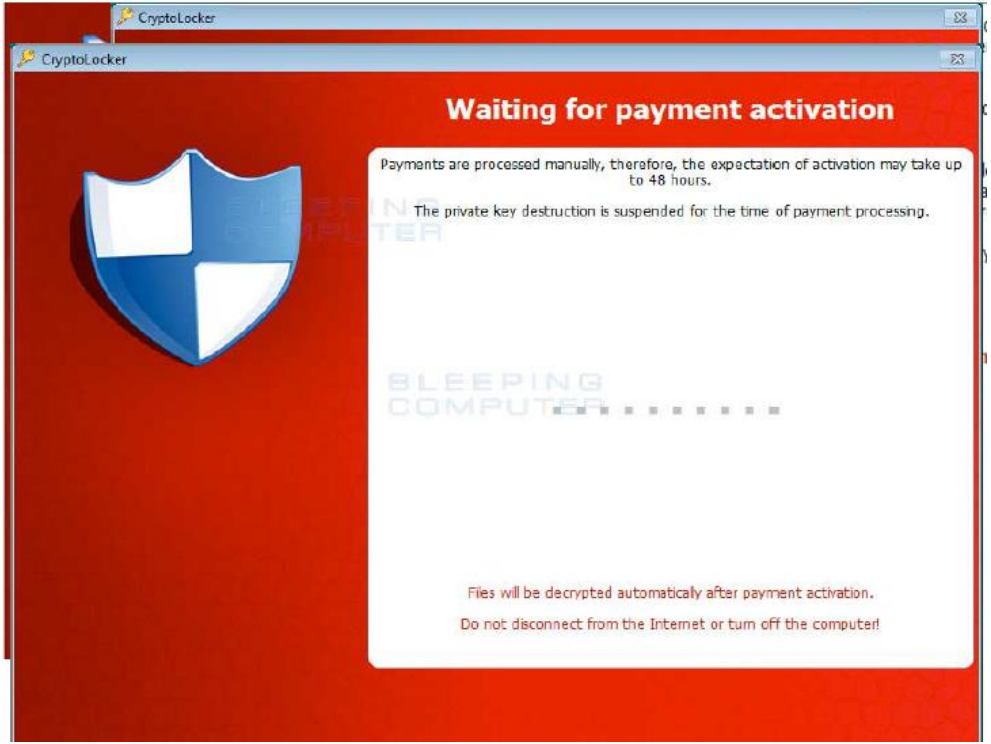
User visits bank site and logs into their account. Malicious code steals their credentials and sends them off to the attacker

Ransomware

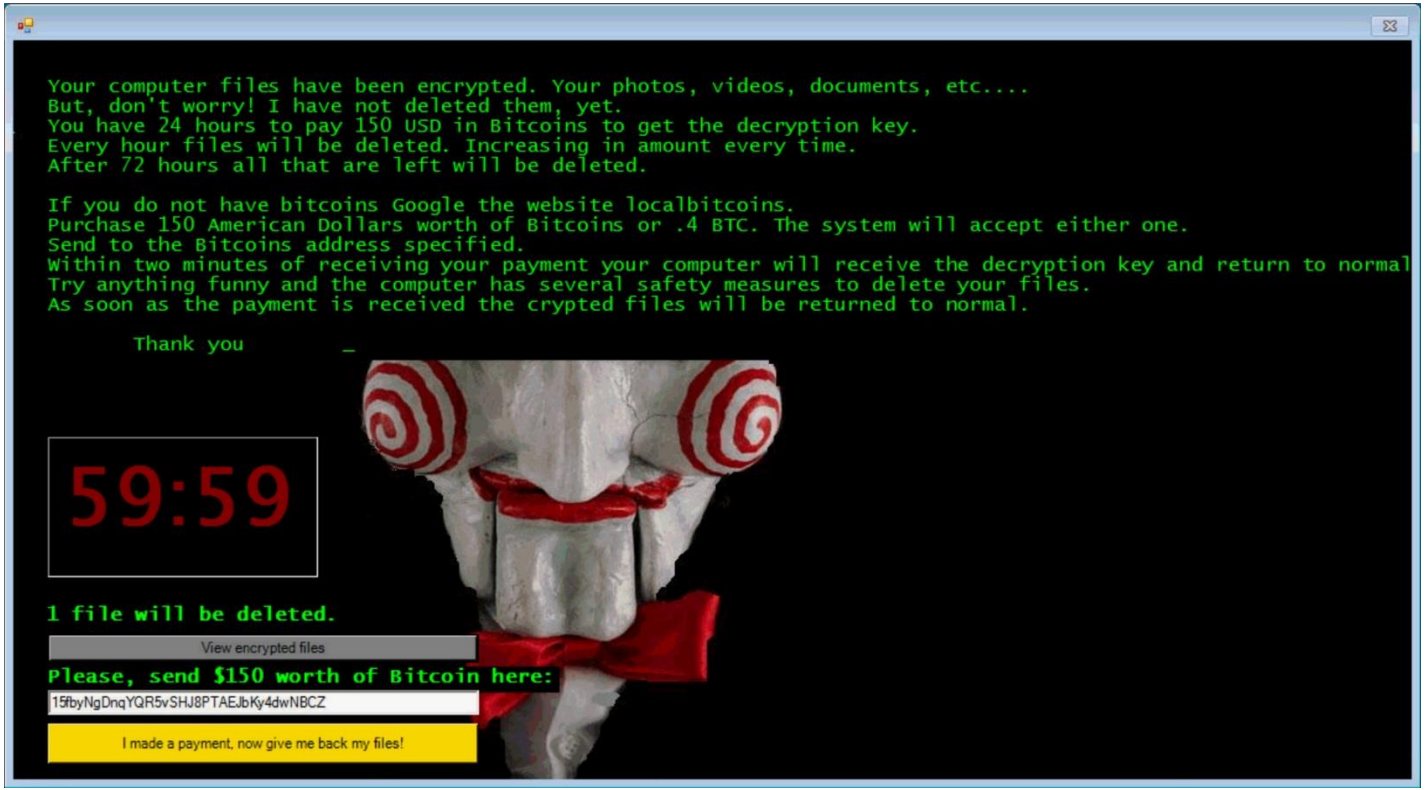
- Encrypts files on a victim's computer and any connected shares or drives. Files are held until a ransom is paid, allowing the victim to regain access to the files.
- Ransomware is often spread through a phishing email, a seemingly legitimate email that tricks users into clicking on a link or attachment.
- Includes Cryptolocker, Cryptowall, Jigsaw.
- Ilion (2014) – Ransomware incidents affect government computers

Source: http://osc.state.ny.us/localgov/audits/villages/2015/ilion.pdf

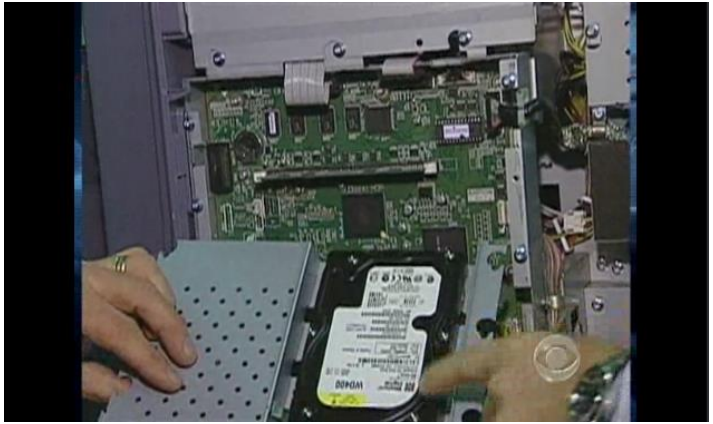
Cryptolocker



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.
View encrypted files
Please, send $150 worth of Bitcoin here:
15fbyNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ
I made a payment, now give me back my files!

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

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

GOVINFOSECURITY®

Home | Training | Resources | Content Library | Careers | Blog

Browse Topics | Protecting Consumer Privacy in an Era of Rapid Change.. | Next Topic >

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

Share 10 retweet

Surplus computers in N.J.

Print Digg Email Delicious Save Reddit

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.

Error on page. Internet 100%

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 your 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. 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 2016

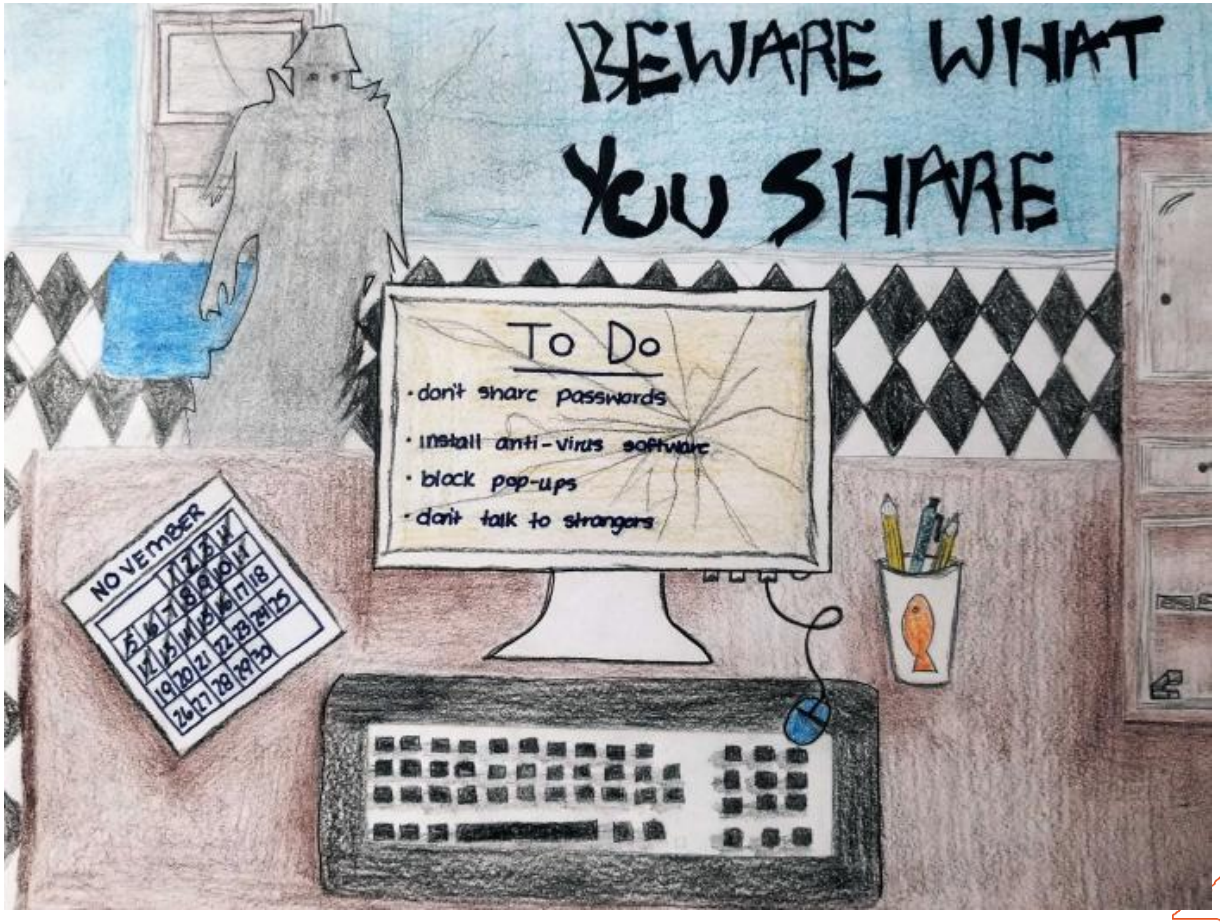
RANK	PASSWORD	CHANGE FROM 2015	RANK	PASSWORD	CHANGE FROM 2015
1	123456	Unchanged	11	login	9 ↗
2	password	Unchanged	12	welcome	1 ↘
3	12345	2 ↗	13	solo	10 ↗
4	12345678	1 ↘	14	abc123	1 ↘
5	football	2 ↗	15	admin	NEW
6	qwerty	2 ↘	16	121212	NEW
7	1234567890	5 ↗	17	flower	NEW
8	1234567	1 ↗	18	passw0rd	6 ↗
9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

Password Wall of Shame 2018

1. 123456	11. princess
2. password	12. admin
3. 123456789	13. welcome
4. 12345678	14. 666666
5. 12345	15. abc123
6. 111111	16. football
7. 1234567	17. 123123
8. sunshine	18. monkey
9. qwerty	19. 654321
10. iloveyou	20. !@#$%^&*

Create “Cyber-Aware” Schools

2018
Cyber Security Awareness
"Kids Safe Online"
2019
New York State K-12 Poster Contest
New York State Office of Information Technology Services
Enterprise Information Security Office
Certificate of Participation
Presented To
For your involvement in the NYS "Kids Safe Online" Poster Contest
NEW YORK STATE OF OPPORTUNITY.
Office of Information Technology Services
Kids Safe ONLINE


BEWARE WHAT YOU SHARE
To Do
· don't share passwords
· install anti-virus software
· block pop-ups
· don't talk to strangers
NOVEMBER

COMMON SENSE MEDIA

Family Media Agreement

common sense®

I, _____ , will:

... take care.

- ☐ I will take care of the device I'm using and tell my family if it's broken, stolen, or lost. As a family, we have agreed on the consequences if I lose or break a device, and I understand those consequences.
- ☐ Unless I have paid for a device with my own money or it was a gift, I understand that the device belongs to the family member(s) who bought it.
- ☐ _____

... stay safe.

- ☐ I will not create accounts or give out any private information — such as my full name, date of birth, address, phone number, or photos of myself — without my family's permission.
- ☐ I will not share my passwords with anyone other than my family. I will ask my family to help me with privacy settings if I want to set up devices, accounts, or profiles.
- ☐ If anyone makes me feel pressured or uncomfortable or acts inappropriately toward me online, I'll stop talking to that person and will tell a family member or other trusted adult about it.
- ☐ _____

... think first.

- ☐ I will not bully, humiliate, or upset anyone online — whether through sharing photos, videos, or screenshots, spreading rumors or gossip, or setting up fake profiles — and I will stand up to those who do.
- ☐ I know that whatever I share online can spread fast and far. I will not post anything online that could harm my reputation.
- ☐ Whenever I use, reference, or share someone else's creative work online, I will give proper credit to the author or artist.

WE ARE FROM
TECH SUPPORT
WE ARE HERE TO
DELETE YOUR COOKIES

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

Free Resources

Training

- NYS – Security Awareness
- Cybrary.IT
- Texas Engineering Extension Service (TEEX.org)
- FedVTE (USALearning.gov)

Awareness Resources

- NYS
  - Information Technology Services
  - Comptroller IT Audit
- US Dept of Homeland Security, Stop.Think.Connect
- US Federal Trade Commission (FTC)
- MS-ISAC

The K-12 Cyber Incident Map

484 Incidents Since January 2016

The K-12 Cyber Incident Map is a visualization of cybersecurity-related incidents reported about U.S. K-12 public schools and districts from 2016 to the present.** 'Cyber' incidents include:

- phishing attacks resulting in the disclosure of personal data (blue pins);
- other unauthorized disclosures, breaches or hacks resulting in the disclosure of personal data (purple pins);
- ransomware attacks (yellow pins);
- denial-of-service attacks (green pins); and
- other cyber incidents resulting in school disruptions and unauthorized disclosures (red pins).

The K-12 Cyber Incident Map is interactive. In addition to being able to shrink or enlarge the map, **clicking on a pin** will provide a summary of information about each specific incident, including the year the incident became public, the school/district involved, the incident type, a brief description of the incident, and the source of the data about the incident.

Cyber Security
Your – Mine – Everyone's Responsibility!

John Borst
NYS Office of Information Technology Services
Chief Information Security Office
www.its.ny.gov/eiso
518-242-5200 John.Borst@its.ny.gov