



Defending Your Institution from Spear Phishing Attacks

April 21, 2016

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC,
an SEC-registered investment advisor. | ©2016 CliftonLarsonAllen LLP



Housekeeping

- If you are experiencing technical difficulties, please dial: **800-422-3623**.
- **Q&A session will be held at the end of the presentation.**
 - Your questions can be submitted via the **Questions Function at any time during the presentation.**
- The **PowerPoint presentation**, as well as the **webinar recording**, will be sent to you within the next 10 business days.
- For future webinar invitations, subscribe at CLAAconnect.com/subscribe.
- Please complete our online survey.



CPE Requirements

- Answer the polling questions
- If you are participating in a group, complete the CPE sign-in sheet and return within two business days
 - Contact webmaster@CLAconnect.com
- Allow four weeks for receipt of your certificate; it will be sent to you via email

** This webinar, once recorded, has not been developed into a self study course. Therefore, watching the recording will not qualify for CPE credit.*



About CliftonLarsonAllen

- A professional services firm with three distinct business lines
 - Wealth Advisory
 - Outsourcing
 - Audit, Tax, and Consulting
- More than 4,500 employees
- Offices coast to coast
- Serve more than 1,450 financial institutions



Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.



Speaker Introduction

Randy Romes

- Principal with CLA's information security services group
- Consultant for more than 16 years
- Leads a team of technology and industry professionals providing IT audits and security assessments for clients in a wide range of industries and diverse operating environments.



Learning Objectives

- At the end of this session, you will be able to:
 - Discuss a three-pronged approach to defend your financial institution from spear phishing attacks
 - Identify an action plan to protect your organization from cybercrime
 - Recognize appropriate steps to take if you've fallen victim to fraud



Our perspective...

CliftonLarsonAllen

- Started in 1953 with a goal of total client service
- Information Security offered as specialized service offering for over 20 years
 - Penetration testing
 - Vulnerability assessment
 - IT/Cyber security risk assessments
 - IT audit and compliance
 - Incident response and forensics
 - Security awareness training
 - Independent security consulting



Overview

- Hacker motivations and techniques
 - Current threats
 - Industry examples
- Case studies
- Strategies and defensive measures to mitigate risks of phishing attacks



Cyber Fraud Risk Themes

- Hackers have “monetized” their activity
 - More sophisticated hacking
 - More “hands-on” effort
 - Smaller organizations targeted
 - Black market economy
- Everyone is a target...
- Phishing is a root cause behind the majority of cyber fraud and hacking attacks



Cybercrime as an industry

- Suppliers
- Markets
- Service providers
("cybercrime as a service")
- Financing
- Trading systems
- Proliferation of business models



this is the **MARKET** where the storekeeper buys the food and brings it to his store near your house

Criminal Specialization

- Coder
- MaaS
- Attacker
- Aggregator
- Carder/distributor
- Street level criminal



Largest Cyber Fraud Trends - Motivations

- Most common cyber fraud scenarios we see affecting our clients
 - Theft of PII and PFI
 - Theft of credit card information
 - Member and corporate account take overs
 - Ransomware



Black Market Economy - Theft of PFI and PII

Active campaigns involving targeted phishing and hacking focused on common/known vulnerabilities.

RETAIL

- Target/Home Depot
- Jimmy Johns/Goodwill

Higher Education

- University of Indiana
- Rockhurst University

Large Personnel Breaches

- OPM
- Blue Cross Primera

Health Care Systems

- Community Health Systems



Account Takeovers – CATO

- Catholic church parish
- Hospice
- Regional bank
- Finance company
- Main Street newspaper stand
- Electrical contractor
- Utility company
- Industry trade association
- Rural hospital
- Mining company
- Credit Union (board members)
- On and on and on and on.....



CATO Lawsuits – UCC

A payment order received by the [bank] is “effective as the order of the customer, whether or not authorized, **if the security procedure is a *commercially reasonable* method of providing security** against unauthorized payment orders, and the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.”

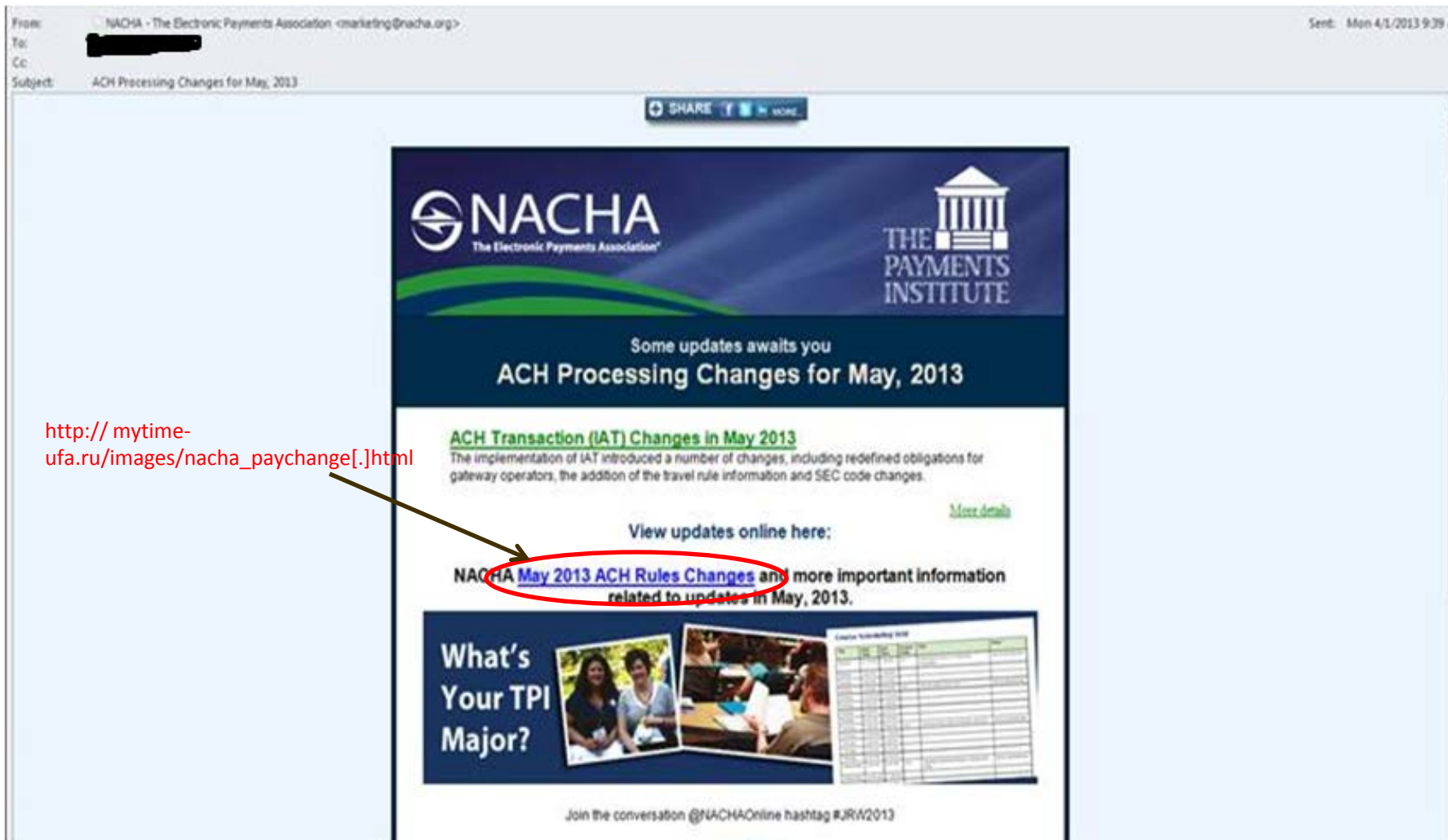


CATO Lawsuits – UCC

- Electrical Contractor vs Bank
 - > \$300,000 stolen via ACH through CATO
 - Internet banking site was “down” – DOS?
 - Contractor asserting bank processed bogus ACH file without any call back
- Escrow company vs Bank
 - > \$400,000 stolen via single wire through CATO
 - ◇ *Escrow company passed on dual control offered by the bank*
 - Court ruled in favor of bank
 - Company’s attorneys failed to demonstrate bank’s procedures were not commercially reasonable



Phishing – CATO – NACHA (ACH) Update



Phishing – CATO – NACHA (ACH) Update

- Employee clicked on a phishing email appearing to come from the National Automated Clearing House Association (NACHA)
 - Embedded link resolves to a Russian IP address
- Employee's internet banking credentials were compromised
- Employee's browser was hacked
 - Injected with malicious HTML registry setting
 - Pop-up asks for additional information when visiting banking site
 - Employee also received call from supporting actor in attack



Phishing – CATO – NACHA (ACH) Update

- Lessons learned
 - Weak/missing filtering capabilities
 - Lack of employee awareness
 - Excessive user access (operating system)
 - No segregation of duties (application)
 - No incident response plan
 - IT indicated the employees system was “clean” – this was not the case (training/awareness)
 - Lack of log retention/server logging not enabled
 - System was powered off



CATO Defensive Measures

- **Authentication:**

- Multi-layer authentication
- Multi-factor authentication
- Out of band authentication

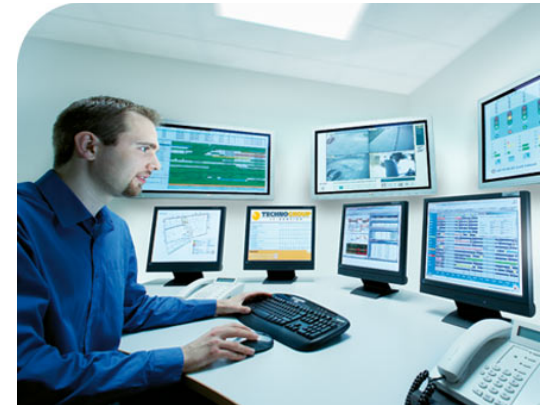
- **Filtering (“White Listing”):**

- Positive pay
- ACH block and filter
- IP address filtering

- **Monitoring:**

- Dual control
- Defined processes for payments
- Activity monitoring / Anomaly detection

- Manual vs. Automated controls



Phishing and Ransomware

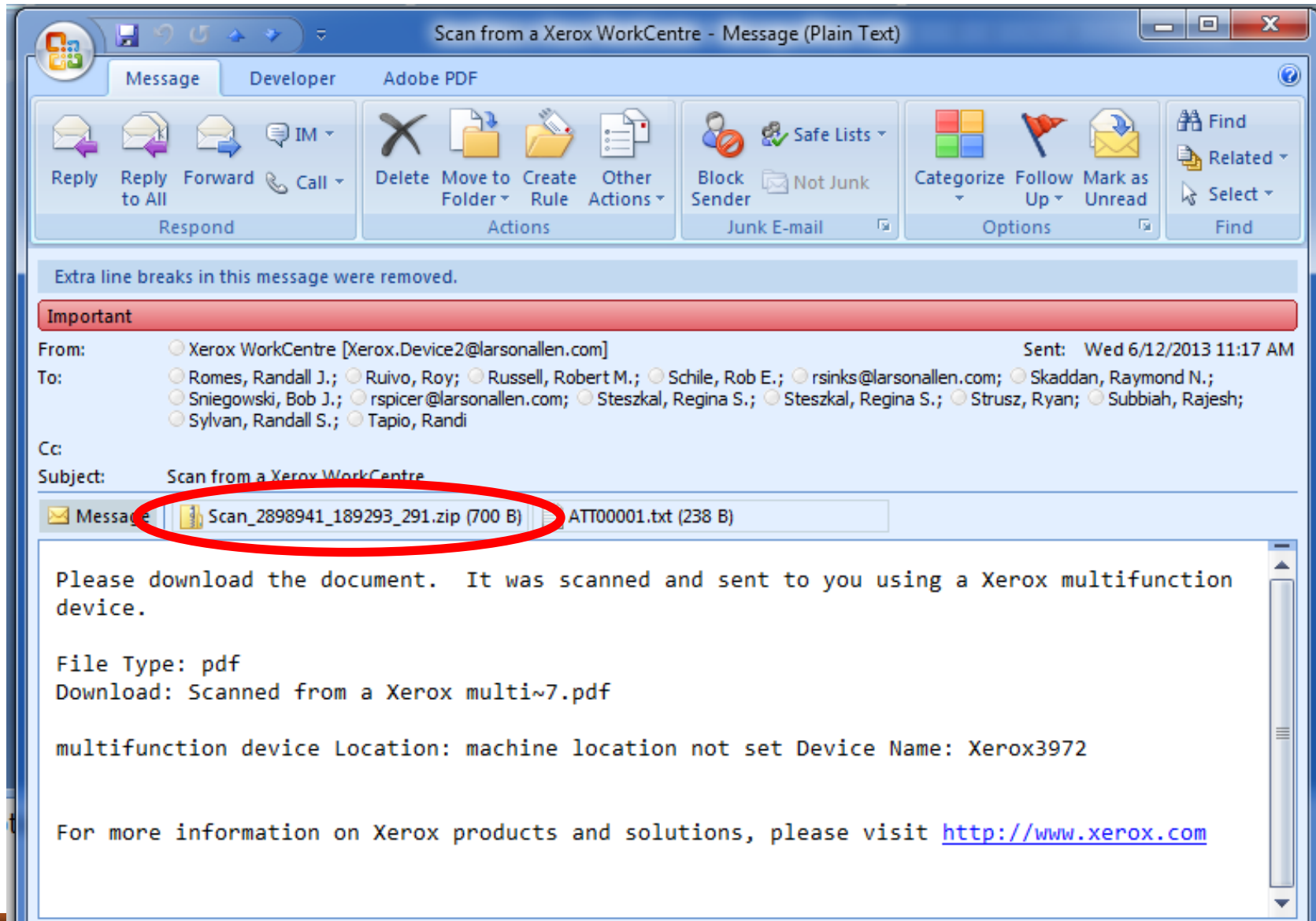
Hospital ransomware: A chilling wake-up call

Hollywood Presbyterian was forced to pay up, just like everyone else.



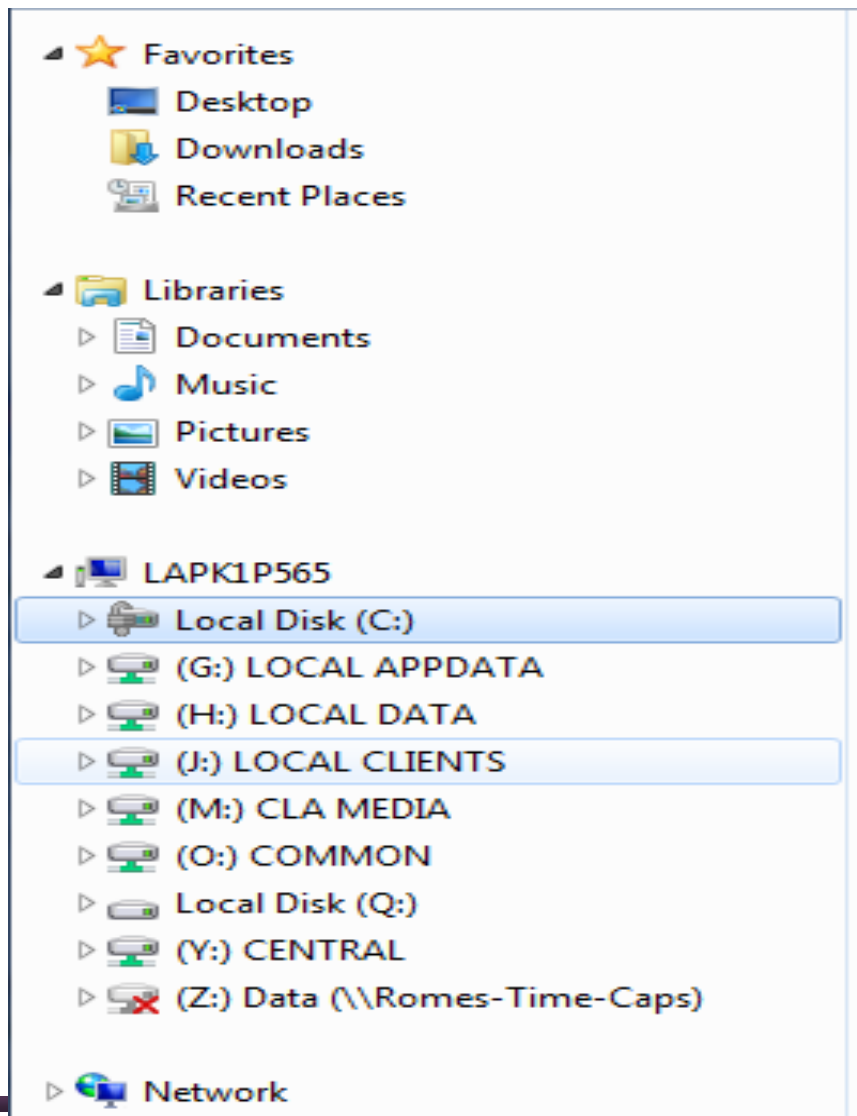
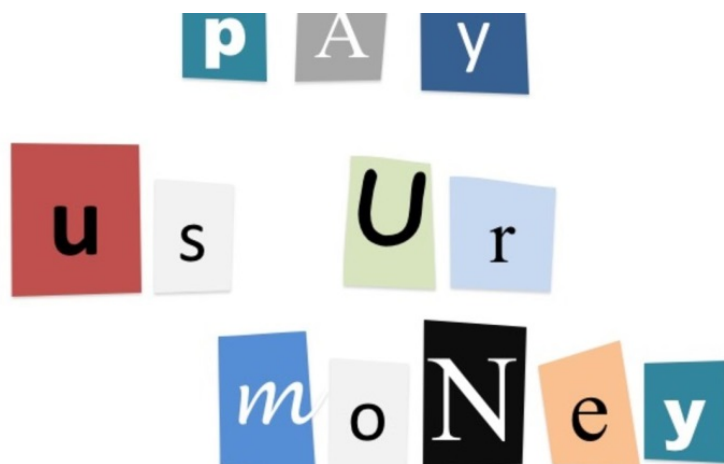
<http://www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/>

Phishing and Ransomware



Phishing and Ransomware

- Malware encrypts everything it can interact with

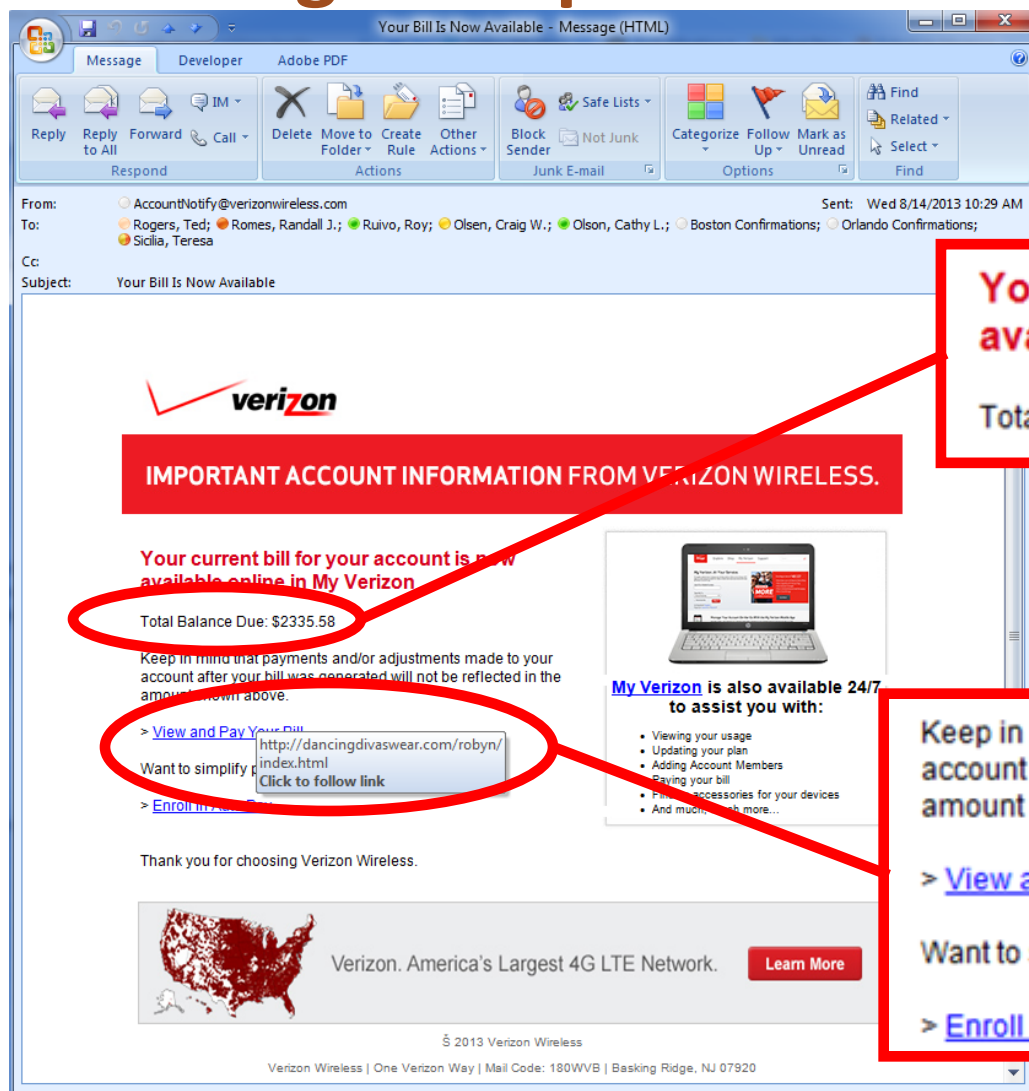


Phishing and Ransomware

- Filtering capabilities
- Users that are aware and savvy
- Minimized user access
- Working backups are critical...
- See appendix...



Phishing Examples



Your current bill for your account is now available online in My Verizon

Total Balance Due: \$2335.58

Your current bill for your account is now available online in My Verizon

Total Balance Due: \$2335.58

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> [View and Pay Your Bill](#)
http://dancingdivaswear.com/robyn/index.html
Click to follow link

Thank you for choosing Verizon Wireless.



Verizon. America's Largest 4G LTE Network.

[Learn More](#)

© 2013 Verizon Wireless

Verizon Wireless | One Verizon Way | Mail Code: 180WVB | Basking Ridge, NJ 07920

Keep in mind that payments and/or adjustments made to your account after your bill was generated will not be reflected in the amount shown above.

> [View and Pay Your Bill](#)

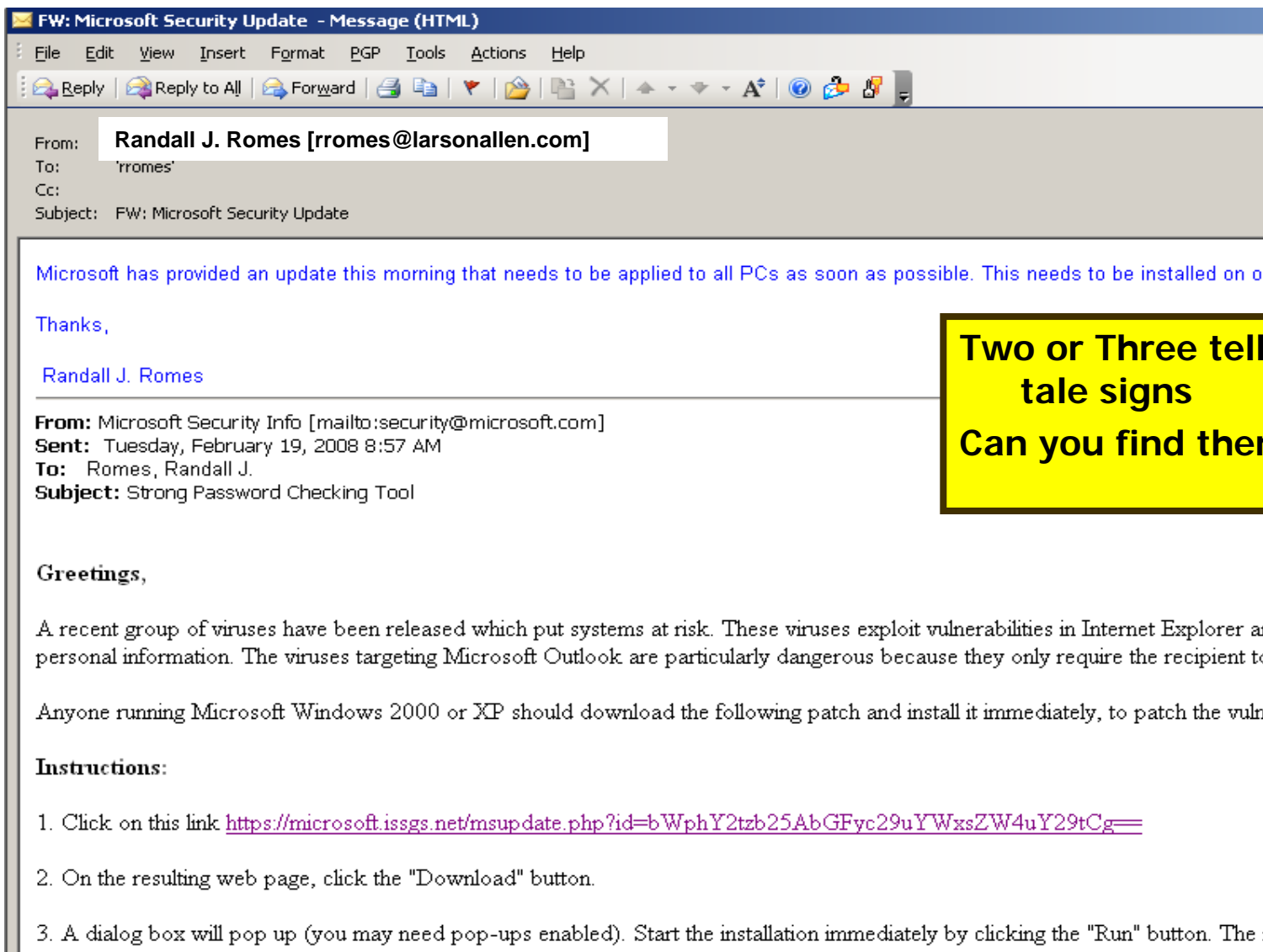
Want to simplify p

http://dancingdivaswear.com/robyn/index.html
Click to follow link

> [Enroll in Auto Pay](#)



Email Phishing – Targeted Attack



**Two or Three tell-tale signs
Can you find them?**



Email Phishing – Targeted Attack



Thanks,

Randall J. Romes

From: Microsoft Security Info [mailto:security@microsoft.com]
Sent: Tuesday, February 19, 2008 8:57 AM
To: Romes, Randall J.
Subject: Strong Password Checking Tool

Greetings,

A recent group of viruses have been released which put systems at risk. These viruses exploit vulnerabilities in Microsoft Outlook to steal personal information. The viruses targeting Microsoft Outlook are particularly dangerous because they only require the recipient to

Anyone running Microsoft Windows 2000 or XP should download the following patch and install it immediately, to patch the vulnerability.

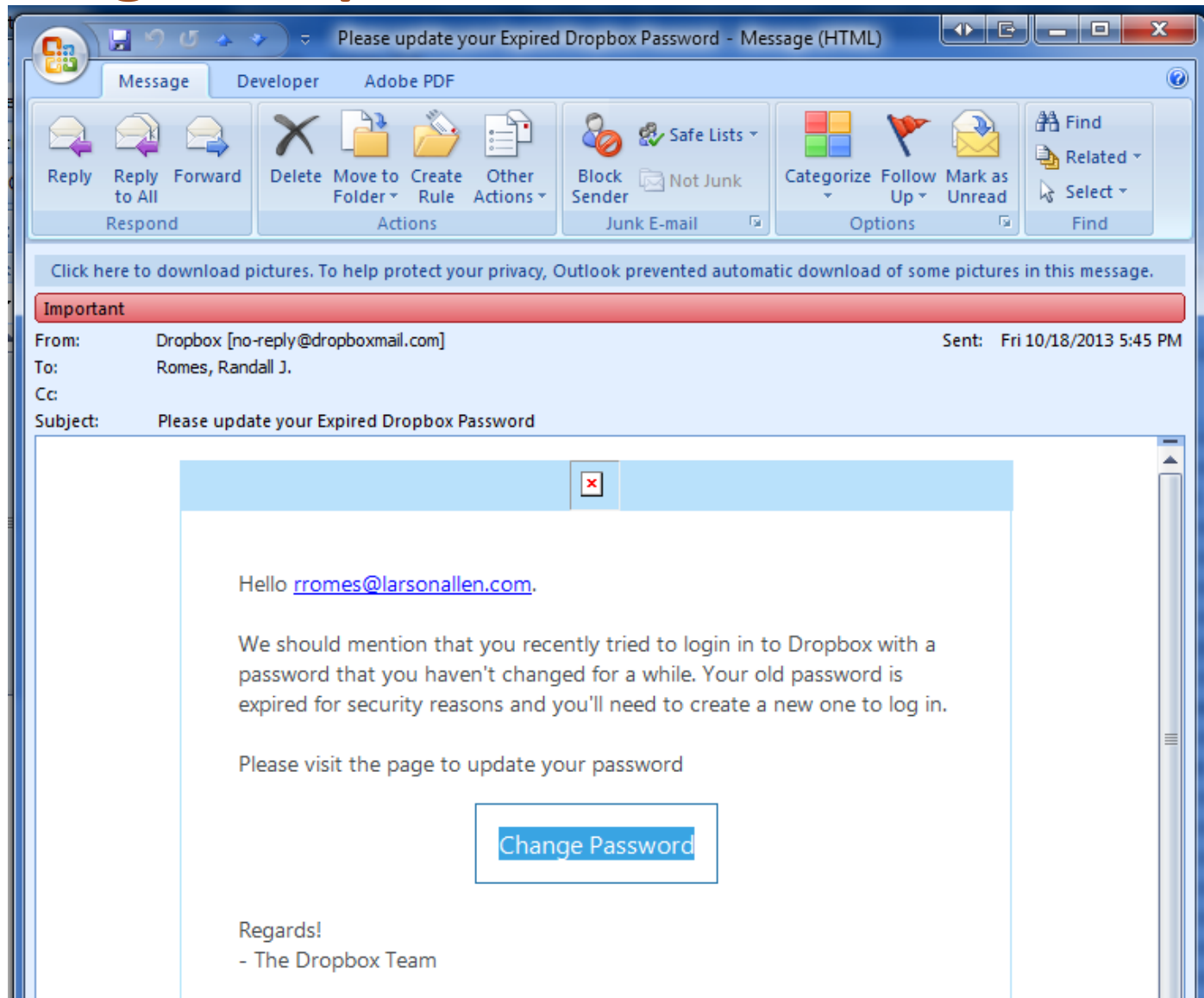
Instructions:

1. Click on this link <https://microsoft.issgs.net/msu>

Two or Three tell-tale signs
Can you find them?



Phishing Examples



Persuasion Attack – CEO Impersonation

- Email from CEO to CFO/Controller
 - CEO Gmail account has been compromised
 - CEO's email is spoofed (faked)
- Email does NOT contain suspicious links
- Email looks very legitimate
 - Attackers are performing reconnaissance on their targets
 - Use social media to know when CEO isn't available (e.g. vacation)



Persuasion Attack – CEO Impersonation

- CEO asks the CFO...
- Common mistakes
 1. Use of private email
 2. “Don’t tell anyone”
- Safeguards
 1. Never use email for sole method of authorization
 2. Ensure recipient has VERBALLY validated with “source” of email for financial transactions
- <http://www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html>

Omaha's ██████ loses \$17 million after spearphishing attack

Fraudsters convinced an Omaha company to send \$17.2 million to a bank in China



By [Maria Korolov](#) | [Follow](#)
CSO | Feb 13, 2015 4:20 PM PT

Fraudsters targeting an Omaha company last summer used extremely well-targeted emails to convince its controller to send a series of wires totaling \$17.2 million to a bank in China.

First, there were emails, supposedly from the CEO, saying that ██████ was buying a company in China. The emails weren't from the CEO's official email address, and, moreover, warned the controller not to communicate about the deal through other channels "in order for us not to infringe SEC regulations."

The emails also instructed the controller to get the wire instructions from an actual employee of the company's actual accounting firm ██████. Plus, the phone number provided in the email was answered by someone with the right name.

[MORE ON CSO: How to spot a phishing email](#)

Since ██████ was, in fact, discussing expanding in China, the controller fell for the emails and sent off the money.



Phishing Emails – Malicious Office Document

- Attackers are embedding malware in Office documents (Macros)
- Enabling Macros on the document allows the malicious code to run



Phishing Emails – Malicious Office Document

- Remediation
 - Don't open attachments from unknown sources
 - Don't open attachments you didn't expect
 - Don't enable Macros in unknown/untrusted documents



Pre-text Phone Calls (Phishing by phone)

- “Hi, this is Randy from Fiserv users support. I am working with Dave, and I need your help...”
 - Name dropping → Establish a rapport
 - Ask for help
 - Inject some techno-babble
- “I need you to visit the Microsoft Update site to download and install a security patch. Do you have 3 minutes to help me out?”
- Schemes result in losses from Home Equity Line of Credit (HELOC) accounts, fraudulent ACH transactions,...



Email Phishing – Targeted Attack

Download details: Express Security Update for Windows 2000/XP (KB929970) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites RSS Feeds Print Mail News Groups

Address <https://microsoft.isgs.net/msupdate.php?id=bWphY2tzb25AbGFyc29uYWxsZW4uY29tCg==>

Google G Go Bookmarks 4 blocked Check AutoLink AutoFill Send to

Microsoft

Download Center

Download Center Home

Search All Downloads Go [Advanced Search](#)

Product Families

- Windows
- Office
- Servers
- Developer Tools
- Business Solutions
- Games & Xbox
- MSN
- Windows Mobile
- All Downloads

Download Categories

- Games
- DirectX
- Internet
- Windows Security & Updates
- Windows Media
- Drivers
- Home & Office
- Mobile Devices
- Mac & Other Platforms
- System Tools
- Development Resources

Download Resources

Express Security Update for Windows 2000/XP (KB929970)

Brief Description

Install this update to address multiple security vulnerabilities in Internet Explorer and Outlook clients described in security upc

On This Page

- [Quick Details](#)
- [System Requirements](#)
- [Related Resources](#)
- [Overview](#)
- [Instructions](#)
- [What Others Are Downloading](#)

Download

Quick Details


File Name:	Express_Security_Update.exe
Version:	929970
Security Bulletins:	MS08-005
Knowledge Base (KB)	KB929970
Articles:	
Date Published:	4/21/2008
Language:	English
Download Size:	2.0 MB
Estimated Download Time:	5 min 56K

Only one tell-tale sign



Email Phishing – Targeted Attack

Download details: Express Security Update for Windows 2000/XP (KB929970) - Microsoft Internet Explorer

Address  <https://microsoft.issqs.net/msupdate.php?>

1

AutoLink AutoFill Send to

Microsoft

Download Center

Download Center Home

Search All Downloads Go [Advanced Search](#)

Product Families

- Windows
- Office
- Servers
- Developer Tools
- Business Solutions
- Games & Xbox
- MSN
- Windows Mobile
- All Downloads

Download Categories

- Games
- DirectX
- Internet
- Windows Security & Updates
- Windows Media
- Drivers
- Home & Office
- Mobile Devices
- Mac & Other Platforms
- System Tools
- Development Resources

Download Resources

Express Security Update for Windows 2000/XP (KB929970)

Brief Description

Install this update to address multiple security vulnerabilities in Internet Explorer and Outlook clients described in security update

On This Page

- [Quick Details](#)
- [System Requirements](#)
- [Related Resources](#)
- [Overview](#)
- [Instructions](#)
- [What Others Are Downloading](#)

Download

Quick Details

File Name:	Express_Security_Update.exe
Version:	929970
Security Bulletins:	MS08-005
Knowledge Base (KB) Articles:	KB929970
Date Published:	4/21/2008
Language:	English
Download Size:	2.0 MB
Estimated Download Time:	5 min 56K

Only one tell-tale sign





Key Defensive Strategies

Strategies

Our information security strategy should have the following objectives:

- Users who are aware and savvy
- Networks that are resistant to malware and attacks
- Be Prepared... Monitoring, Incident Response, Testing, and Validation



Strategies to Combat Social Engineering

- (Ongoing) user awareness training
- SANS First Five – Layers “behind the people”
 1. Secure/Standard Configurations (hardening)
 2. Critical Patches – Operating Systems
 3. Critical Patches – Applications
 4. Application White Listing
 - 5. Minimized user access rights**
 - **No browsing/email with admin rights**



Strategies to Mitigate Phishing Risks

- Filtering capabilities (white listing)
- Users who are aware and savvy
- Minimized user access rights
- Networks that are resistant to malware and attacks
- Preparedness... Monitoring, Alerting, and Incident Response Capabilities
- Working, Validated Backup and Restore Capabilities



Call To Action

Policies to set foundation

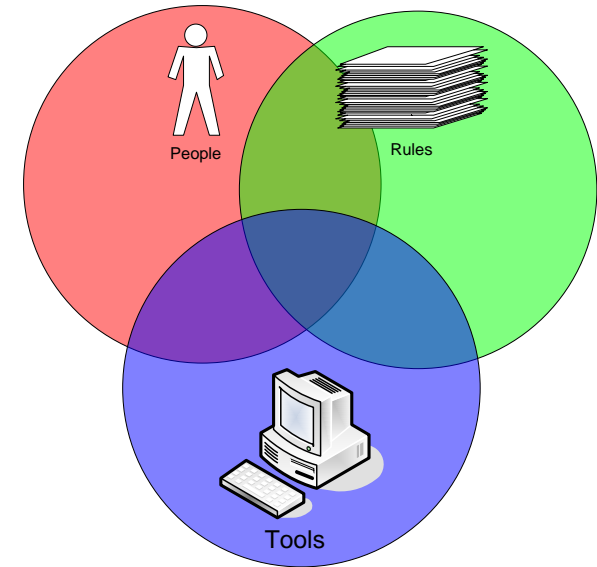
Train your users

Thoroughly assess your risks

Three R's: Recognize, React, Respond

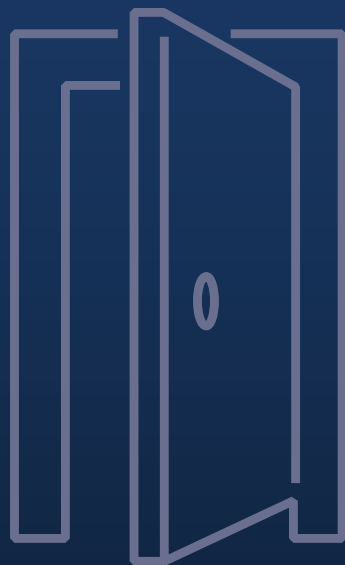
Thoroughly validate your controls

- High expectations of your vendors
- Penetration testing
- Application testing
- Vulnerability scanning
- Social engineering testing



Questions?





Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal
Information Security Services
randy.romes@CLAconnect.com
888-529-2648

CLAconnect.com

Resources – Hardening Checklists

Hardening checklists from vendors

- CIS offers vendor-neutral hardening resources

<http://www.cisecurity.org/>

- Microsoft Security Checklists

<http://www.microsoft.com/technet/archive/security/chklist/default.mspx?mfr=true>

<http://technet.microsoft.com/en-us/library/dd366061.aspx>

Most of these will be from the “BIG” software and hardware providers



Industry Breach Analysis Security Reports

- Intrusion Analysis: TrustWave (Annual)
 - <https://www.trustwave.com/whitePapers.php>
- Intrusion Analysis: Verizon Business Services (Annual)
 - <http://www.verizonenterprise.com/DBIR/>



Ransomware Defensive Measures

- Remove the connection
 - Reduce threat to network
 - Reduce remote connection
 - Eliminate risk of data loss
- Call IT helpdesk
- Describe what you were doing
 - Especially email
- Wait for instructions



Ransomware Safeguards

- Software Restriction Policies are one good way to prevent this.
 - [https://technet.microsoft.com/en-us/library/cc759648\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc759648(v=ws.10).aspx)
 - We can send some example policies if needed. There are a few clients who are going this route.



Ransomware Safeguards

- Stopping .exe launch from AppData locations and \$temp\$.
 - Malware we were looking at the other day dropped .bat, .vbs, and .exe in appdata folder.
 - Restricting what applications can run from appdata/temp is very important.
 - Webroot had a good write up on this a few days ago.
 - ◇ <http://www.webroot.com/blog/2016/02/22/locky-ransomware/>
 - ◇ Apparently the executable only runs in \$temp\$. Restricting what gets run from there that would help.



Ransomware Safeguards

- Do an audit of file permissions for where backups are stored.
 - Identify what users could encrypt backups if they were to become infected.
 - Generally, you would want the location very restrictive – read only access even for most administrators.
 - Backups should be done with a service account.
 - Users should not have access to the backup location.
 - You could also restrict the backup network access temporally similar to a bank vault.
 - ◇ That could be done with a simple script that would disable the port during the day and then reenable just before the backup starts.

