



CONNECT
COLLABORATE
Innovate

2018

Association CONFERENCE

*Cybersecurity Trends
A State of the Union*

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC,
an SEC-registered investment advisor. | ©2018 CliftonLarsonAllen LLP

Who am I?

- David Anderson
 - Farm kid turned hacker
 - Manager — Information Security team
 - Oversee IT security testing and audits
 - I am over 18

Agenda

- Ten Ways to Lose Everything
- Cybercrime Trends
- What a Cyberattack Looks Like
- Takeaways and Action Items

Ten Ways to Lose Everything



Ten Ways to Lose Everything

1. Users clicking links

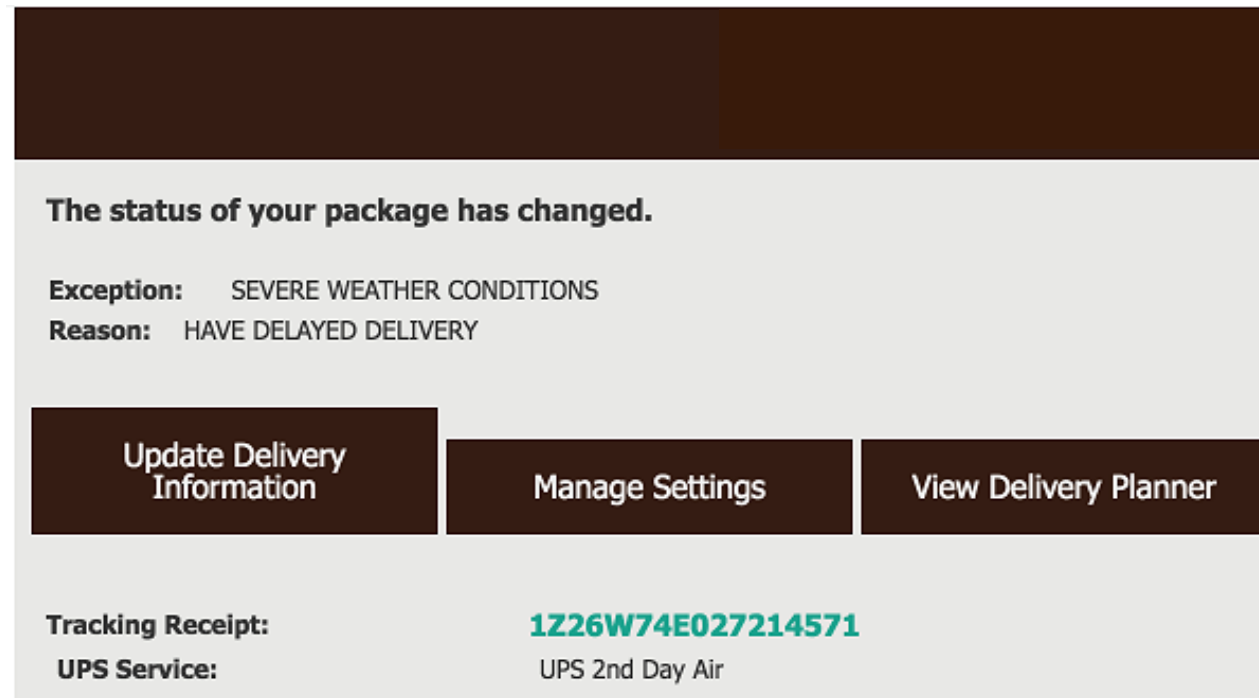
Fax Message [Caller-ID: MedSource]

You have received a 2 page fax on **Tuesday, December 19**, 2016 at 8:34 -500
The reference number for this fax is 84502384542

[Click here to view this message](#)

Ten Ways to Lose Everything

2. Users clicking links



Ten Ways to Lose Everything

3. Users clicking links


ADP Immediate Notification

Over the past few days we have had reports of issues with the distributed W-2's. As a result we are issuing W-2c (Corrected W-2) for a large subset ADP customers, including _____ employees. Please use ADP's W2 Secure Download portal below to obtain the corrected W-2 and contact your Human Resources department with any further questions.

[W2 Secure Download](#)

Ref: 22771

As usual, thank you for choosing ADP as your business affiliate!

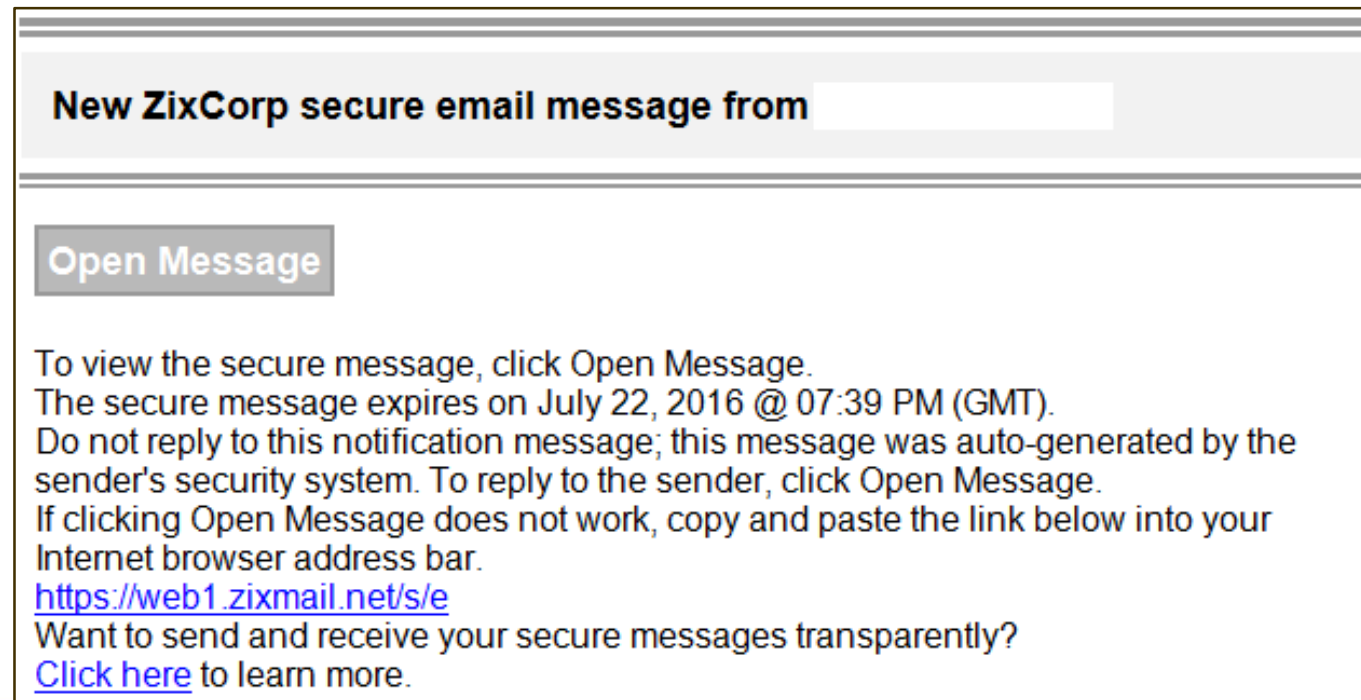


HR. Payroll. Benefits.

The ADP logo and ADP are registered trademarks of ADP, Inc.
In the business of your success is a service mark of ADP, Inc.
© 2012 ADP, Inc. All rights reserved.

Ten Ways to Lose Everything


4. Users clicking links



Ten Ways to Lose Everything

5. Users clicking links

Your wireless bill is ready.



The current billing statement for your wireless account is now available in My Verizon.

Please note, payments and/or adjustment made to your account since your invoice was generated will not be reflected in the amount shown.

In order to view your bill, please sign in to [My Verizon](#).

Thank you for choosing Verizon Wireless.

Online Bill Summary

Account Number:
XXXXXX5722-00009

Scheduled Automatic Payment:
01/15/2016

Total Amount Due:
\$ 958.54

[Pay Bill](#) | [View Online Bill](#)

Ten Ways to Lose Everything

6. Users clicking links

Hi,

I am applying for an IT internship and I received your email through our IT program here at ISU. I am really interested in learning about networking and system administration. Can you take a look at my resume and let me know if I would be a good fit for your program and if there are any current openings?

[Resume](#)

Ten Ways to Lose Everything

7. Users clicking links

Microsoft has released a tool that will ensure our computers and software are compatible with Windows 10. Please download and run the tool. The tool will run in the background so you can continue working and will not require you to reboot your computer.

If after running the tool, it says that your computer is not compatible, please let me know along with the reason it gives.

Download the Windows 10 Preparation Tool from the link on the top of the page at <http://windows10.microsoft.com>.

Ten Ways to Lose Everything

8. Users clicking links

Buongiorno!

In celebration of the grand opening of our new Alexandria franchise, and as a local favorite for authentic Italian food, we're offering coupons redeemable for one **FREE** lunch or dinner. This offer is being made in appreciation of the patronage of local businesses and is redeemable at any of our locations.

Your coupon is valid through the end of August. Follow the link for the direct download of your coupon, along with our valid menu items that may be purchased with your coupon. Please print out just the coupon and deliver it to your server to enjoy a **FREE** authentic Italian meal at Bello Cucina!

[Coupon Link](#)

Arrivederci,

Jason Mueller, Owner, Bello Cucino
106 West Lincoln Ave

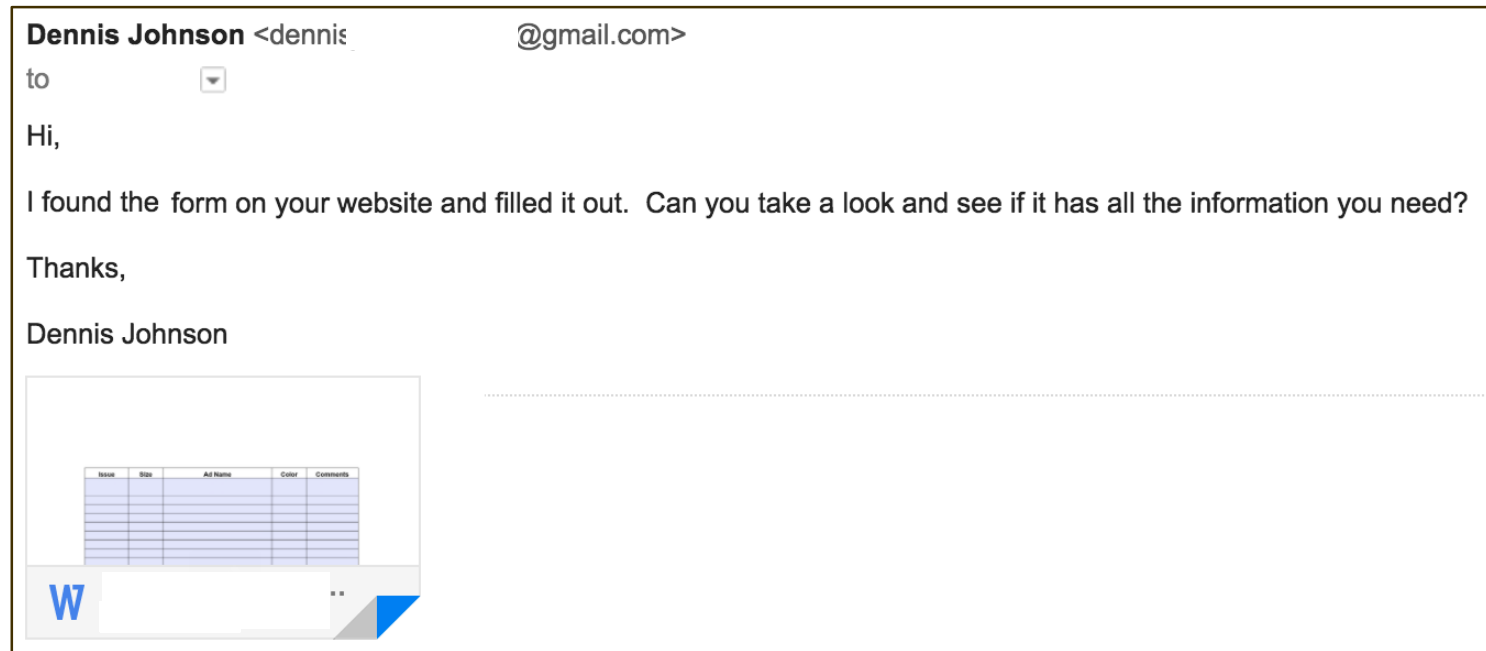
Ten Ways to Lose Everything

9. Users clicking links



Ten Ways to Lose Everything

10. Users opening attachments



Cybercrime Trends



Current State of Cybercrime

- All about the Benjamins
 - Theft of Personally Identifiable Information (PII)
 - Payment Fraud
 - Ransomware
- Hacking is run like a business
 - Specialization

The Cost

- Global cybercrime is costing businesses **\$600 billion** annually
- Estimate that it will reach into the **trillions** in next few years

Theft of PII

- Every organization stores information about their employees in electronic format
 - Payroll/Tax/W2
 - Email address
- Many store other sensitive data
 - Credit card information
 - Health information

Marketplace for Stolen Credit Cards

Home Buy CC CC Orders **Buy Dumps** Dump orders Checker Tickets

Hello, [REDACTED] Cart (1) 9.45\$ Balance: 3.0\$ [Add money](#) [Replace policy](#) [Logout](#)

101
201

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [Bulk Orders - Low Prices!](#) [Clear](#) [Search](#)

	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
<input type="checkbox"/>	371736	AMEX	CREDIT		07/15	Yes	110	United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14	30\$	+
<input type="checkbox"/>	371555	AMEX	CREDIT		09/16	Yes	101	United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14	30\$	+
<input type="checkbox"/>	371736	AMEX	CREDIT		03/17	Yes	101	United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14	30\$	+
<input type="checkbox"/>	371564	AMEX	CREDIT		05/15	Yes	110	United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14	30\$	+
<input type="checkbox"/>	371554	AMEX	CREDIT		04/17	Yes	101	United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14	30\$	+
<input type="checkbox"/>	371242	AMEX	CREDIT	GREEN	06/17	Yes	101	United States, 98512, Olympia, WA	AMERICAN EXPRESS COMPANY	American Sanctions 14	30\$	+
<input type="checkbox"/>	371570	AMEX	CREDIT		10/16	Yes	101	United States, 97123, Hillsboro, OR	BANK OF AMERICA	American Sanctions 14	30\$	+
<input type="checkbox"/>	371381	AMEX	CREDIT		10/16	Yes	201	United States, 30328, Atlanta, GA	CITIBANK <small>Dump or cc of this particular bank (BIN)</small>	American Sanctions 14	24\$	+

Payment Fraud

- Every organization interacts with their bank electronically
 - Wire transfers & ACH payments
 - Online banking
- Corporate Account Take Over (CATO)
 - Compromise accounts/credentials that can move money

Payment Fraud

- Can occur via technical means
 - Attackers “hack” into finance computers
 - Banking Trojans monitor online banking
 - Create fake employees in payroll/ACH file
- Can occur via non-technical means
 - Social engineering
 - ◊ Fake CEO scam

Ransomware

- Cryptolocker, Locky, WannaCry, etc.
- Encrypts all data, holds in “ransom” for \$\$
 - Data on local machine and on network

Ransomware

AMERICA

LA Hospital Pays Hackers Nearly \$17,000 To Restore Computer Network

February 17, 2016 · 9:08 PM ET

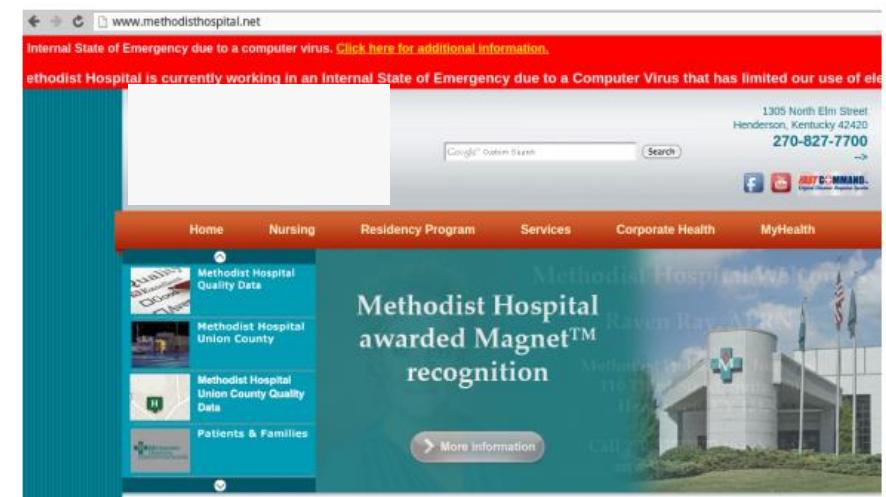
LAURA WAGNER



22 Hospital Declares 'Internal State of Emergency' After Ransomware Infection

MAR 16

A Kentucky hospital says it is operating in an "internal state of emergency" after a ransomware attack rattled around inside its networks, encrypting files on computer systems and holding the data on them hostage unless and until the hospital pays up.



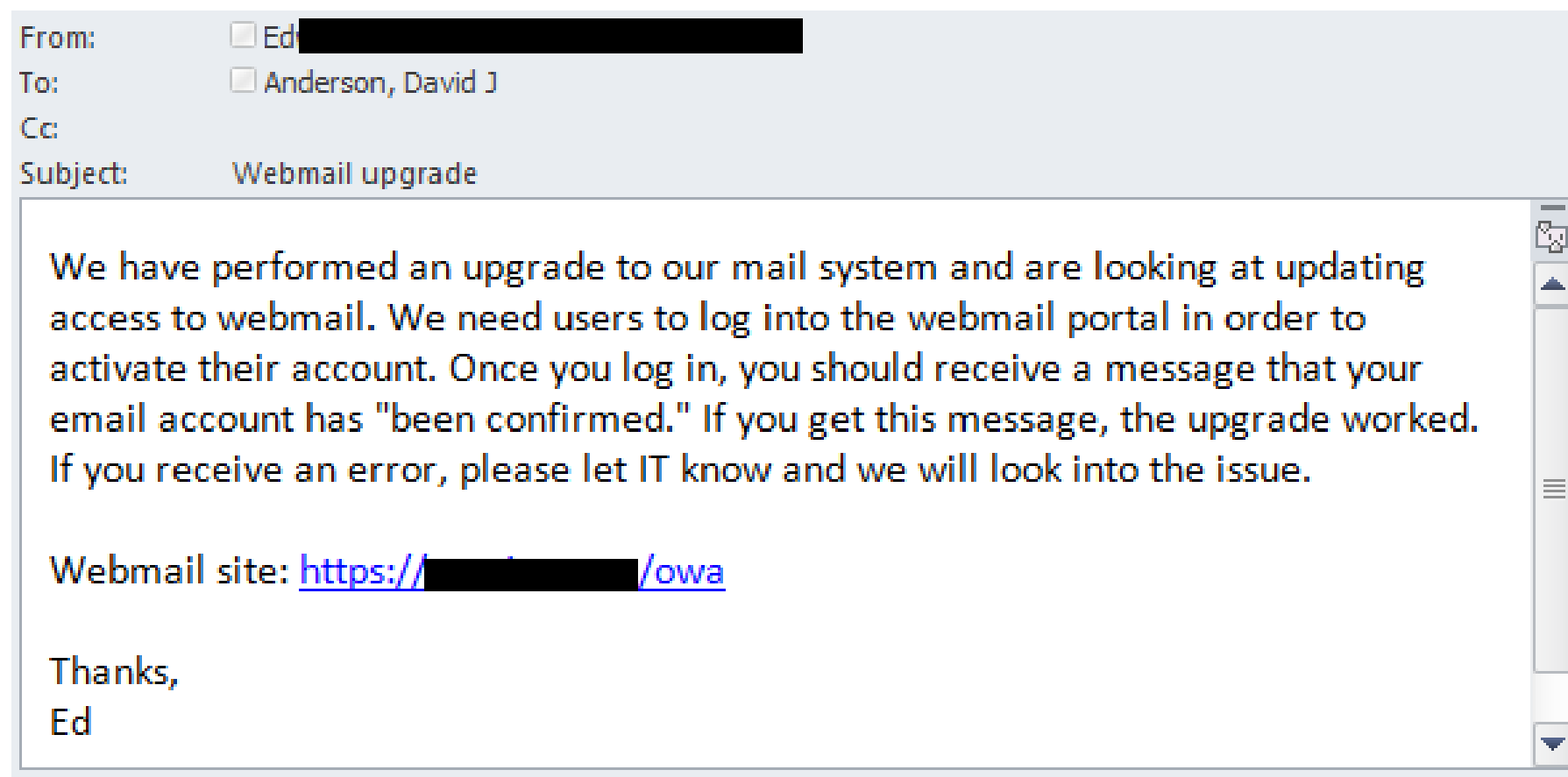
Walk Through a Cyberattack



Reconnaissance

- Who's who in the company?
 - LinkedIn
- Understand what services are exposed to the internet
 - Webmail
 - VPN
 - Other web application

Phishing



Unauthorized Access

Webmail



Microsoft®
Outlook® Web App

Exchange Email Account Update

☒ This is a public or shared computer
☐ This is a private computer

Domain\user name:

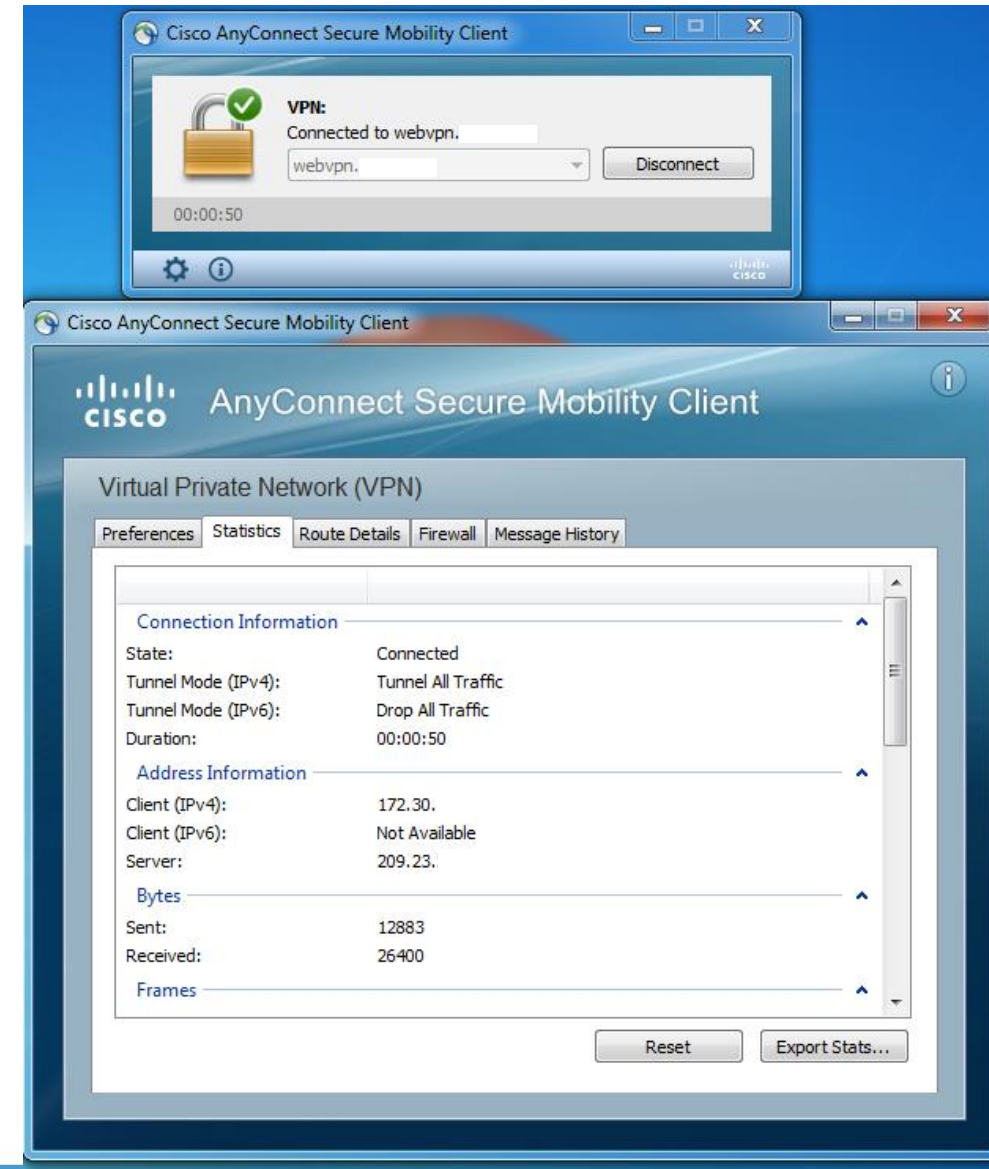
Password:

[Sign in](#)

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

Unauthorized Access

VPN



Takeaways and Action Items



Strategies and Objectives

- Users who are aware and savvy
- Networks that are hardened and resistant to malware and attacks
- Resilience Capabilities: Monitoring, Incident Response, Testing, and Validation

Governance Framework

- CIS Critical Controls
- ISO 27001
- PCI-DSS
- HIPAA HITECH
- NIST
- Etc.

Develop Baselines and Standards

- Example:
CIS Critical Controls

First 5 CIS Controls
Eliminate the vast majority of your
organisation's vulnerabilities

- 1: Inventory of Authorized and Unauthorized Devices →
- 2: Inventory of Authorized and Unauthorized Software →
- 3: Secure Configurations for Hardware and Software →
- 4: Continuous Vulnerability Assessment and Remediation →
- 5: Controlled Use of Administrative Privileges →

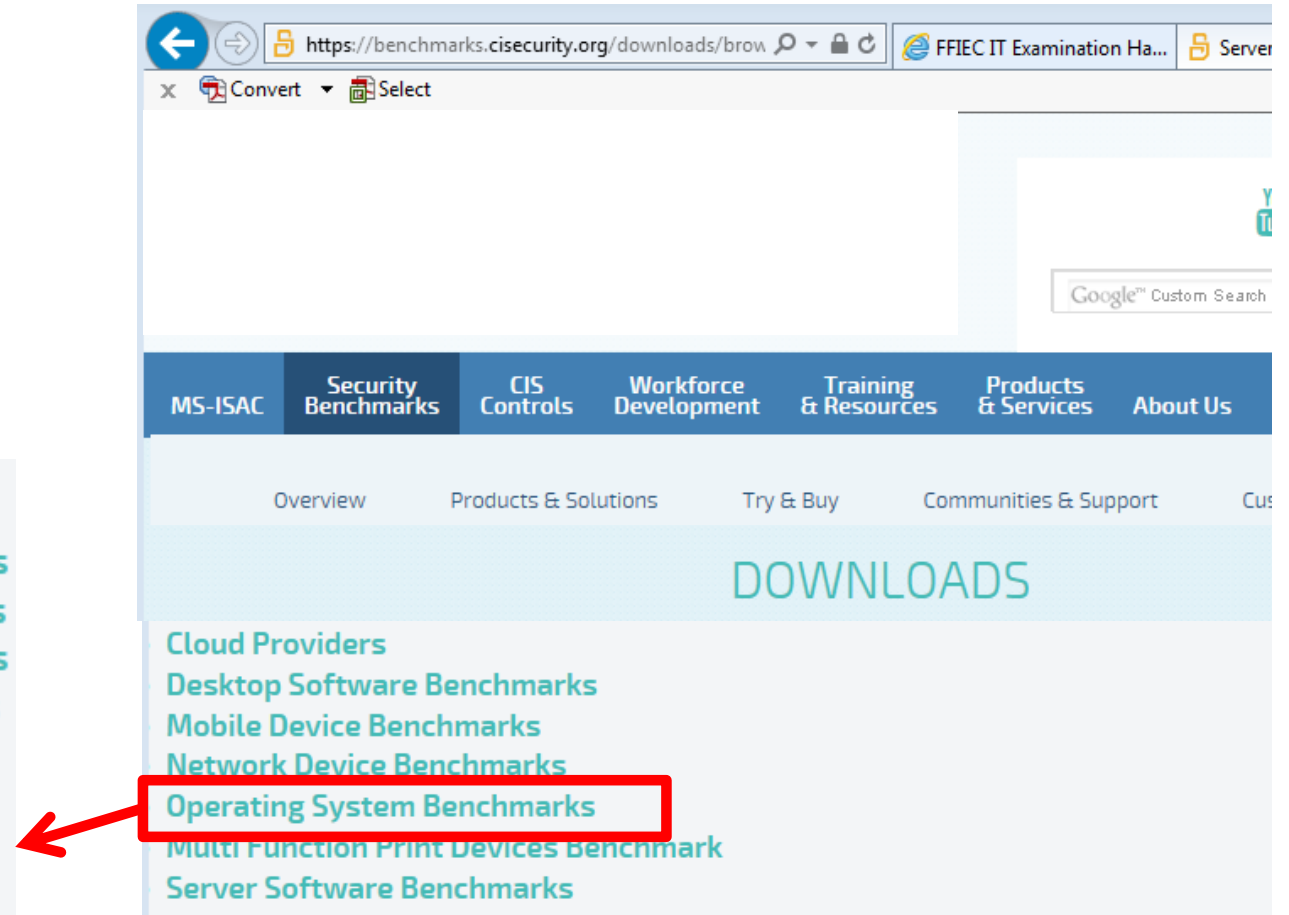
All 20 CIS Controls
Secure your entire organization against
today's most pervasive threats

- 6: Maintenance, Monitoring, and Analysis of Audit Logs →
- 7: Email and Web Browser Protections →
- 8: Malware Defenses →
- 9: Limitation and Control of Network Ports →
- 10: Data Recovery Capability →
- 11: Secure Configurations for Network Devices →
- 12: Boundary Defense →
- 13: Data Protection →
- 14: Controlled Access Based on the Need to Know →
- 15: Wireless Access Control →
- 16: Account Monitoring and Control →
- 17: Security Skills Assessment and Appropriate Training to Fill Gaps →
- 18: Application Software Security →
- 19: Incident Response and Management →
- 20: Penetration Tests and Red Team Exercises →

Develop Baselines and Standards

- Example:
CIS Critical Controls

- Microsoft Windows 10 Benchmarks
- Microsoft Windows Server 2000 Benchmarks
- Microsoft Windows Server 2003 Benchmarks
- Microsoft Windows Server 2008 Benchmarks
- Microsoft Windows Server 2012 Benchmarks
- Microsoft Windows 7 Benchmarks
- Microsoft Windows 8 Benchmarks
- Microsoft Windows NT Benchmarks
- Microsoft Windows XP Benchmarks



Operational Discipline

- Change Management
- Vulnerability and Patch Management
- System Monitoring
- Exception Control and Documentation

Action Items

1. Harden email system
 - Phishing is the #1 way attackers get in
2. Implement two-factor authentication (2FA) on external services
 - If you can access it from the internet, make sure it requires 2FA

Action Items

3. Change vendor default passwords
 - Every system and application comes with default passwords
4. Test backup systems
 - Ensure you can recover from outages/ransomware
5. Enable and configure auditing/logging
 - Every system supports auditing – configure it

Action Items

6. Validate your expectations are being met (TEST IT!)
 - Social engineering testing
 - Penetration testing
 - Vulnerability assessments
 - Disaster recovery/business continuity testing

Questions

Thank you!

David Anderson, OSCP
Manager, Information Security
david.anderson@CLAconnect.com
612-376-4699

CLAconnect.com