

Beyond the Firewall: How to Defend Against Cyber Threats

October 30, 2018

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor



©2018 CliftonLarsonAllen LLP



Create Opportunities
We promise to know you and help you.

Disclaimers

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.



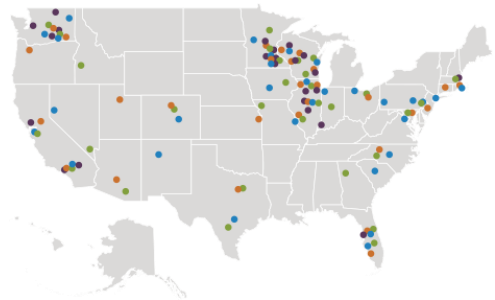
Housekeeping

- 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.



About CLA

- A professional services firm with three distinct business lines
 - Wealth Advisory
 - Outsourcing
 - Audit, Tax, and Consulting
- More than 5,400 employees
- Offices coast to coast
- CLA's information security team combines certified technical professionals, including system administrators and network engineers, with CPAs who have key industry and IT audit experience.



Learning Objectives

At the end of this session, you will be able to:

- Detect the different ways hackers can access your personal and business systems
- Identify new and emerging cyber threats
- Isolate weaknesses in your systems
- Recognize defense tactics to thwart system threats





Beyond the Firewall: How to Defend Against Cyber Threats

Are You Prepared?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Cyber Security Services

Cyber security assessment and consulting offered as specialized service for over 20 years

- Penetration Testing and Vulnerability Assessment
 - Black Box, Red Team, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance
 - GLBA/FFIEC, HIPPA/HITRUST, PCI-DSS, NIST, NERC/CIP, CJIS, etc....
- Incident response and forensics
- Security awareness training
- Independent security consulting
- Internal audit support



C:\whoami

- “Professional Student”
- Science Teacher/Self Taught Computer Guy
- IT Consultant - Project Manager – IT Staff/Help Desk - Hacker
- Assistant Scout Master (Boy Scouts)



Raise Your Hand If...



INTRODUCING
echo dot

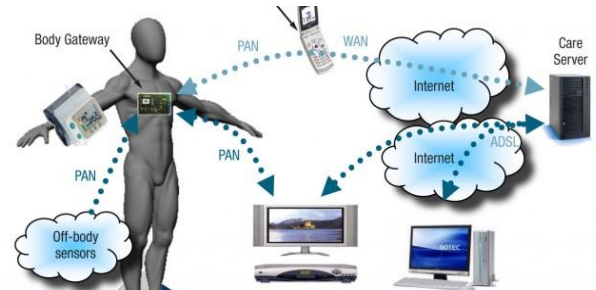
Add Alexa to any room



amazon tap

ALEXA-ENABLED
PORTABLE SPEAKER

JUST TAP & ASK



Cloud Computing, Compute Model for a Smarter Planet
Globalization and Globally Available Resources





Sun Tzu:

*“Know your enemy and
know yourself and you can
fight a hundred battles
without disaster.”*

The Current State of Cybercrime

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an
SEC-registered investment advisor

Cyber Fraud Themes – “Know They Enemy”

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



Largest Cyber Fraud Trends - Motivations

- Black market economy to support cyber fraud
 - Business models and specialization
- Most common cyber fraud scenarios we see affecting our clients
 - Theft of PII and PFI
 - ◊ W2/Payroll/Benefit info
 - Theft of credit card information
 - Theft of Credentials and Account take overs
 - Ransomware and Interference w/ Operations



Recent Data Breaches - PrivacyRights.Org

©2018 CliftonLarsonAllen LLP

Date Made Public	Company	Total Records	Description of Incident
10/22/18	The Centers for Medicare and Medicaid Services -	75,000	According to the press release on their website, "Earlier this week, CMS staff detected anomalous activity in the Federally Facilitated Exchanges, or FFE's Direct Enrollment pathway for agents and brokers. The Direct Enrollment pathway, first launched in 2013, allows agents and brokers to assist consumers with applications for coverage in the FFE. At this time, we believe that approximately 75,000 individuals' files were accessed. While this is a small fraction of consumer records
10/10/18	Cigna	3,500	Location of breached information: Network Server Business associate present: No
10/9/18	Minnesota Department of Human Services	20,800	Location of breached information: Email Business associate present: No
10/8/18	Oklahoma Department of Human Services	813	Location of breached information: Paper/Films Business associate present: Yes
10/7/18	Dr. Amy Woodruff	10,862	Location of breached information: Network Server Business associate present: No
10/7/18	Dr. Robert Carpenter	3,000	Location of breached information: Network Server Business associate present: No
10/5/18	Gold Coast Health Plan	37,005	Location of breached information: Email Business associate present: Yes
10/5/18	National Ambulatory Hernia Institute	15,974	Location of breached information: Network Server Business associate present: No
10/5/18	Northwest Surgical Specialists, P.C.	2,050	Location of breached information: Email Business associate present: No
10/3/18	Tillamook Chiropractic, PC	4,058	Location of breached information: Desktop Computer, Network Server Business associate present: No
10/1/18	Chegg	40,000,000	According to a filing the company left with the SEC, Chegg, a technology giant specializing in textbook rental, has confirmed a data breach affecting some 40 million customers. Data exposed included usernames, email addresses, shipping addresses and hashed passwords. The company does not believe that financial data was taken.
9/28/18	Facebook, Inc.	50,000,000	According to the New York Times, Facebook suffered an "attack" on their system that led to the exposure of information of 50,000,000 users. "The company discovered the breach earlier this week, finding that attackers had exploited a feature in Facebook's code that allowed them to take over user accounts. Facebook fixed the vulnerability and notified law enforcement officials. More than 90 million of Facebook's users were forced to log out of their accounts Friday morning, a
9/20/18	Personal Assistance Services of Colorado, LLC	1,839	Location of breached information: Email Business associate present: No
9/14/18	Guardant Health, Inc.	1,112	Location of breached information: Email Business associate present: No
9/7/18	Catholic Charities Neighborhood Services,	565	Location of breached information: Email Business associate present: No

https://www.privacyrights.org/data-breaches?title=&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&org_type%5B%5D=2437&taxonomy_vocabulary_11_tid%5B%5D=2436&=Search+Data+Breaches



Marketplace for Stolen Information

Attackers buy and sell data on cyber black market

– “The Dark Web” - similar to amazon.com

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	Expres	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\$	+



Create Opportunities | We promise to know you and help you.



Firewalls Are Hard to Break People on the Other Hand...

Social Engineering Improves the Hackers Odds

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

What Makes Social Engineering Successful?

“Amateurs hack systems, professionals hack people.”

Bruce Schneier

Social Engineering relies on the following:

- The appearance of “authority”
- People want to avoid inconvenience
- Timing, timing, timing...



Pre-text Phone Calls (Phishing by phone)

- “Hi, this is Randy from Comcast Business 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 fraudulent ACH transactions,...



Physical (Facility) Security

Compromise the site:

- “Hi, Sally said she would let you know I was coming to fix the printers...”



Plant devices:

- Keystroke loggers
- Wireless access point
- CDs or Thumb drives





Email Phishing Is a Root Cause Underlying Most Breaches

Two Minutes of Inconvenience

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Email Phishing Objectives

Goals:

- Convince target to do something
- Gain access to:
 - Business email accounts (“BEC” or “Business Email Compromise”)
 - Financial accounts (payroll, AR/AP, e-Treasury management, etc.)
 - Network resources and confidential/sensitive information
 - Personal email accounts, cloud accounts, social media accounts

Malware infection via:

- Links to malicious website containing drive-by malware
- Email attachments
 - ZIP, RAR, HTA, JAR, etc....
 - Office documents with MACROS and/or PowerShell script

FILE

MESSAGE

MIMECAST

ADOBE PDF

Ignore

Junk

Delete

Reply

Reply All

Forward

Meeting

More

Proposals SENT

To Manager

Team Email

Move

Rules

OneNote

Actions

Mark Unread

Categorize

Follow Up

Translate

Find

Related

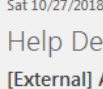
Select

Zoom

Zoom

Dynamics 365

Sat 10/27/2018 5:12 PM

Help Desk <mypassword@claconnect.com>
[External] ACTION REQUIRED: Password Review

To: Romes, Randall J.

Retention Policy: CLA Inbox - 18 Months (1 year, 6 months)

Expires: 4/27/2020

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, the government has mandated higher information security standards. As passwords are the primary mechanism of defense against unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standards.

Every three years, CPA firms are required to obtain an independent review of their system of quality control for their accounting and auditing practice. The most recent review report received by CLA expressed a rating of pass, which is the most positive report that can be received!

Please assist us in continuing to be compliant and visit <https://passwordsecurity.claconnect.com> to test the strength of your passwords. Failure to do so may result in your account being locked out.

Thank you for your cooperation,

CLA IT Security

*This email may contain confidential and privileged information for the sole use of the intended recipient.
Any review or distribution by others is strictly prohibited.
If you are not the intended recipient, please contact the sender and delete all copies. Thank you.*

Phishing?

Citrix Receiver - New Version - Message (HTML)

FILE MESSAGE MIMECAST ADOBE PDF

Ignore Delete Reply Reply All Forward Meeting To Manager Team Email Move Rules OneNote Actions Mark Unread Categorize Follow Up Translate Find Related Select Zoom

Delete Respond Quick Steps Move Tags Editing Zoom

Thu 10/25/2018 6:31 AM

Service Desk

Citrix Receiver - New Version

To: CLA All

Retention Policy: CLA Inbox - 18 Months (1 year, 6 months) Expires: 4/25/2020

Important Message

What: Citrix Receiver – New Version
Who: All Personnel
Date: Thursday 11/01/2018
Time: 6 a.m. CT
Impact: When you login on Thursday morning you will be prompted to install the updated Citrix Receiver. The update is available in software center now if you would like to run it prior to Thursday morning. In software center, select "Receiver for Windows Repair."

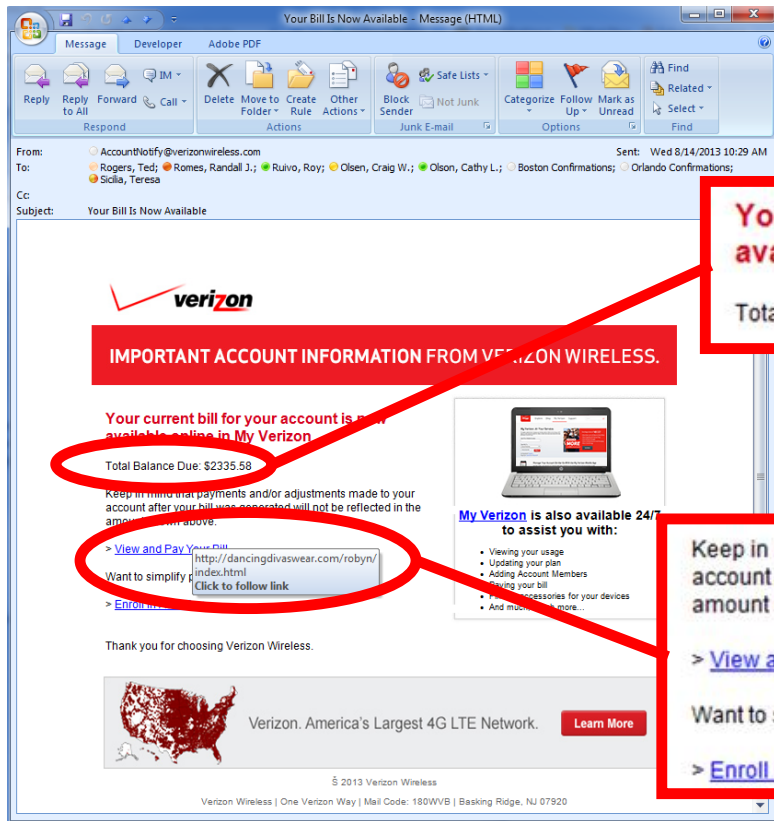
Installing Citrix Receiver:
When you receive the message below click Install to begin the installation. You can click cancel to delay the install temporarily but will continue to receive the install message until the receiver has been updated.

Citrix Receiver

This installation will terminate all Citrix applications.
Please save and close any open Citrix applications before installing.



Phishing?



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

Total Balance Due: \$2335.58

IMPORTANT ACCOUNT INFORMATION FROM VERIZON WIRELESS.

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)
Want to simplify your bill payment?
[Click to follow link](http://dancingdivaswear.com/robyn/index.html)

> [Enroll in Auto Pay](#)

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 your bill payment?

<http://dancingdivaswear.com/robyn/index.html>
[Click to follow link](#)

> [Enroll in Auto Pay](#)





Payment Fraud

Impersonation and Persuasion

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Payment Fraud – Account Take Overs

- Most organizations and individuals perform payments electronically
 - Wire transfers & ACH payments
 - Online banking
- Corporate Account Take Over (CATO)
 - Compromise accounts/credentials that can move money
- Persuasion Attacks
 - Convince others to send money



Corporate Account Take Over's (CATO)

- 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 – controls were not consistent
- 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
 - Bank demonstrated risk conversations, escrows companies waiver of controls, and acceptance of risk



Persuasion Attacks

CEO asks the controller...

Common mistakes

1. Use of private email
2. “Don’t tell anyone”

Omaha's Scoular Co. 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 Scoular 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, KPMG. 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 Scoular was, in fact, discussing expanding in China, the controller fell for the emails and sent off the money.

<http://www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html>



Create Opportunities | We promise to know you and help you.

Persuasion Attacks

Krebs on Security

In-depth security news and investigation

- <https://krebsonsecurity.com/tag/bec/>

CEO asks the accountant...

Common mistakes

1. Use of private email
2. "Don't tell anyone"

18 Firm Sues Cyber Insurer Over \$480K Loss

A Texas manufacturing firm is suing its cyber insurance provider for refusing to cover a \$480,000 loss following an email scam that impersonated the firm's chief executive.

At issue is a cyber insurance policy issued to Houston-based **Ameriforge Group Inc.** (doing business as "AFGlobal Corp.") by **Federal Insurance Co.**, a division of insurance giant **Chubb Group**. AFGlobal maintains that the policy it held provided coverage for both computer fraud and funds transfer fraud, but that the insurer nevertheless denied a claim filed in May 2014 after scammers impersonating AFGlobal's CEO convinced the company's accountant to wire \$480,000 to a bank in China.

According to documents filed with the U.S. District Court in Harris County, Texas, the policy covered up to \$3 million, with a \$100,000 deductible. The documents indicate that from May 21, 2014 to May 27, 2014, AFGlobal's director of accounting received a series of emails from someone claiming to be **Gean Stalcup**, the CEO of AFGlobal.



"Glen, I have assigned you to manage file T521," the phony message to the accounting director **Glen Wurm** allegedly read. "This is a strictly confidential financial operation, to which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)? This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do not speak with anyone by email or phone regarding this. Regards, Gean Stalcup."





Ransomware

Would you like your pictures back?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Ransomware

Ransomware victims pay cybercriminals to save family photos

Theresa and Billy Niedermayer felt they had no choice but to cave in to the demand

By David Common, [CBC News](#) | Posted: Mar 11, 2015 5:00 AM ET | Last Updated: Mar 12, 2015 9:53 AM ET

“Theresa and Billy Niedermayer paid an \$800 ransom to get precious family photos of their three young boys back from cybercriminals.”



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/>

Ransomware

Hackers Demand \$770,000 Ransom From Canadian Banks

Cybercrime: FBI Says Ransomware, Extortion Continue to Dominate

Mathew J. Schwartz (@euroinfosec) • June 1, 2018 • 0 Comments



Bank of Montreal head office in Montréal. (Photo: DXR, via Wikimedia Commons)

Hackers have demanded a ransom of 1 million Canadian dollars (\$770,000) each from two banks, payable in the cryptocurrency exchange system Ripple's XRP token, national Canadian broadcaster [CBC News](#) reports.

See Also: [How to Keep Your Endpoints Safe from Cybercrime](#)

The ransom demand comes on the heels of the Bank of Montreal, operating as BMO Financial Group, and Simplii Financial, a banking subsidiary of the Canadian Imperial Bank of Commerce, on Monday reporting that they'd been warned that some of their client data may have been exposed on Sunday (see [Two Canadian Banks Probe Alleged Exposure of Customer Data](#)).



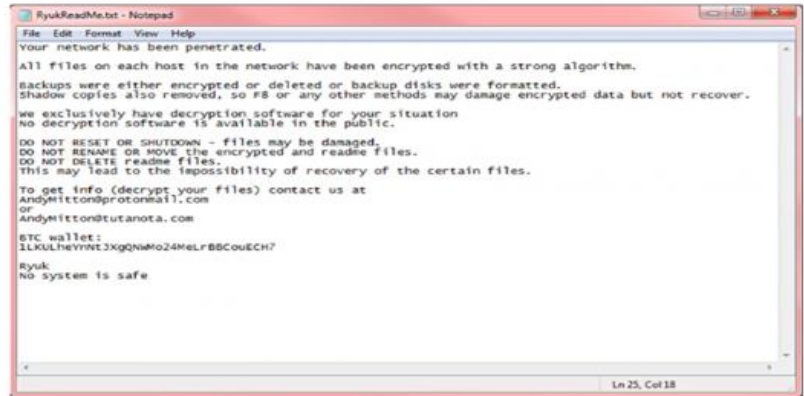
Ransomware

This
week...

Connecticut City Pays Ransom After Crypto-Locking Attack

Separately, a Water Utility Hit by Ryuk Ransomware Vows to Restore, Not Pay

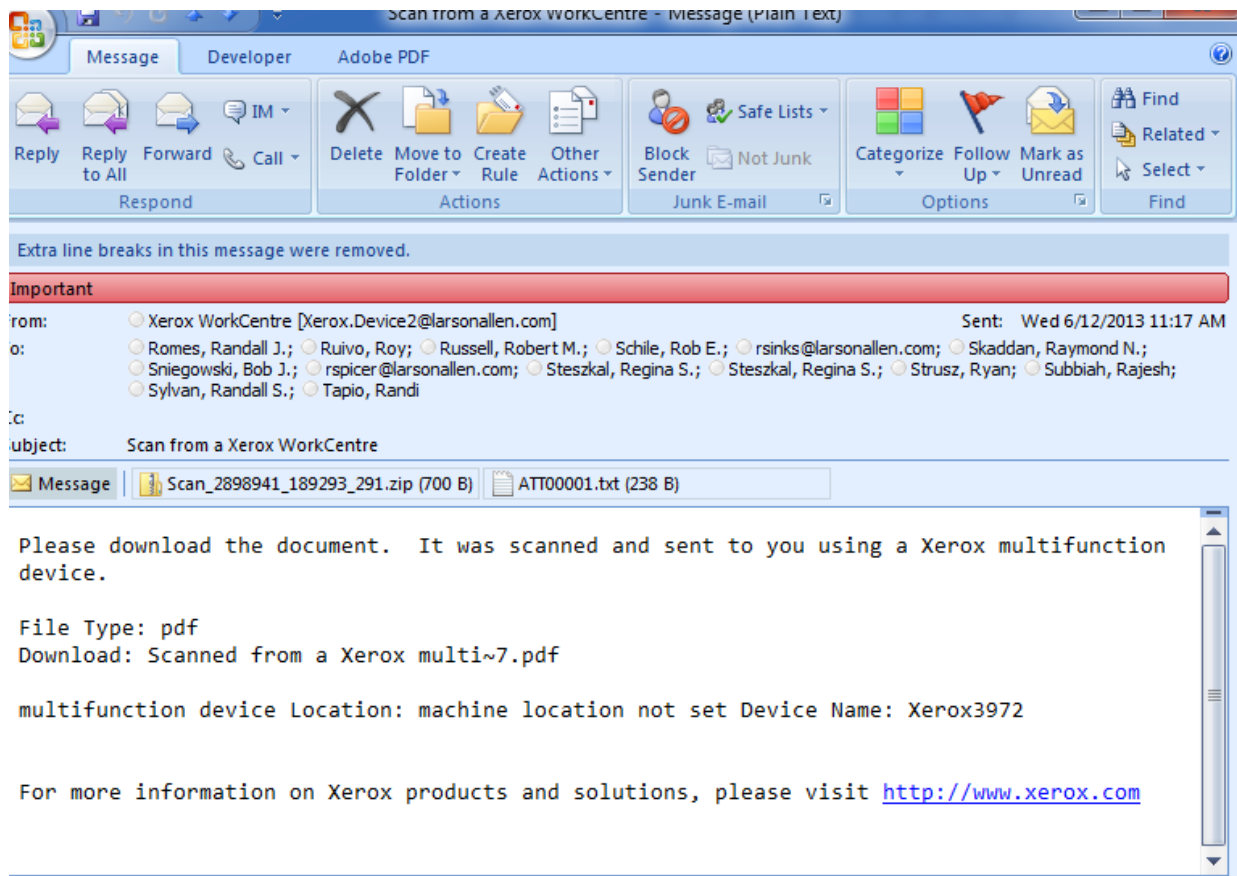
Mathew J. Schwartz (@euroinfosec) • October 22, 2018 1 Comment



A ransom note displayed by Ryuk ransomware that infected systems at a North Carolina water utility (Source: [Check Point](#))

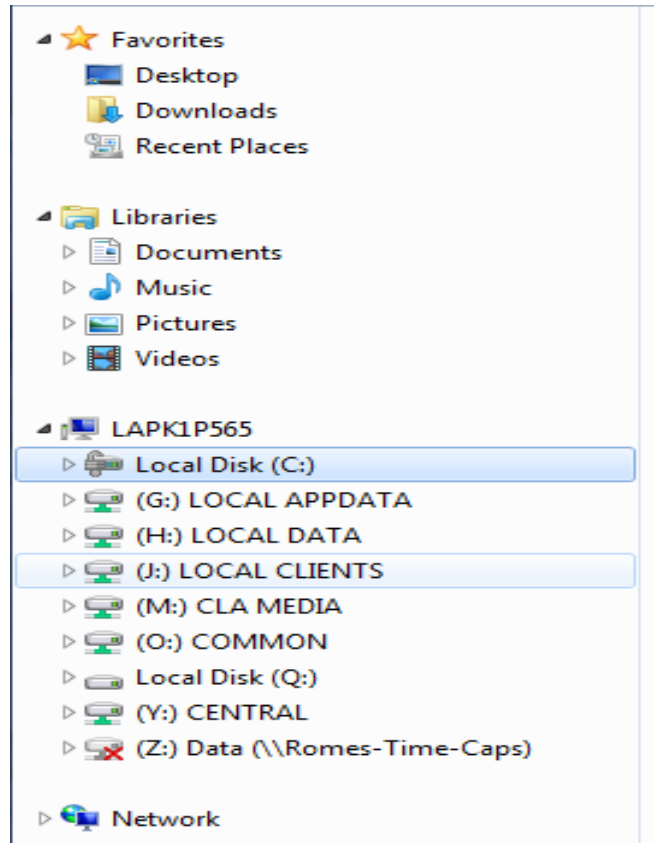
A tale of two different ransomware victims' responses: One town in Connecticut says it was left with little choice but to pay a ransom after attackers crypto-locked its systems. But a water utility in North Carolina, which was hit by a similar attack, says it will rebuild its systems rather than give attackers any money.

Ransomware



Ransomware

- Malware encrypts everything it can interact with



Ransomware Defensive Strategies

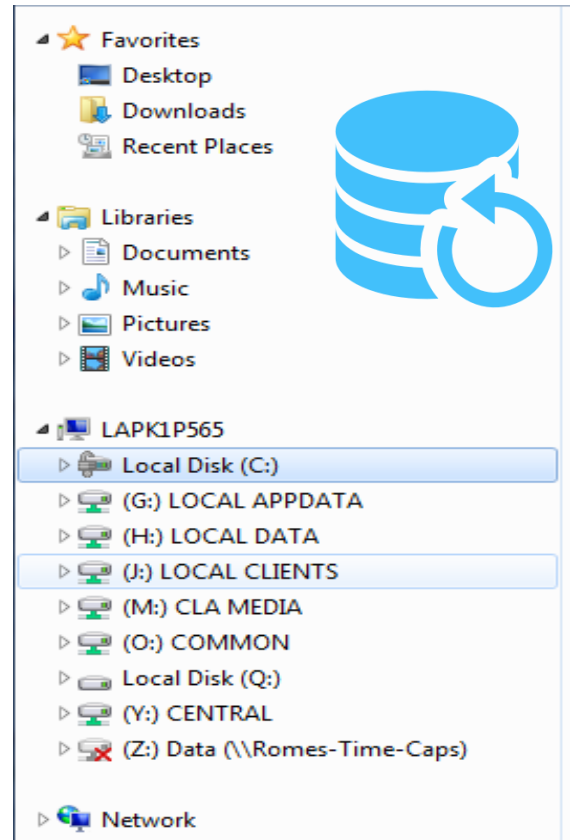
1. Filtering capabilities
2. Users that are aware and savvy
3. Minimized User Access Rights
4. Current operation systems and up to date/patched software



Ransomware

Defensive Strategies

5. Working backup and restore capabilities
6. Secure the backup process
 - Backups should be done with a service account.
 - Storage location of back ups should be very restrictive – read only access even for most administrators.
 - Identify which users could encrypt backups if they were to become infected.
 - You could also restrict the backup network access temporally similar to a bank vault.





The Boy Scouts Motto:

“Be Prepared”

Strategies and Action Items

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

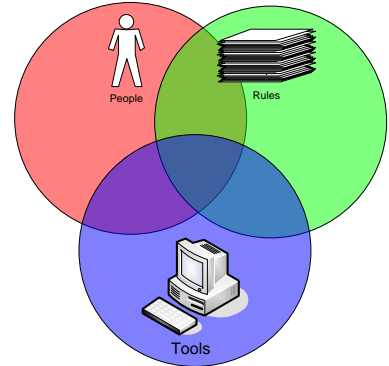
Strategies

Our information security strategy should have the following objectives:

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



Policies and Standards



- People, Rules and Tools
 - What do we expect to occur?
 - How do we conduct business?

- Standards based operations from a governance or compliance framework:
 - GLBA/FFIEC, HIPAA, NERC/CIP, CJIS
 - PCI – DSS
 - CIS Critical Controls, HITRUST, NIST, ISO

Standards Based Operations



Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>



Standards Based Operations

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 3: Secure Configurations for Hardware and Software				
Family	CSC	Control Description	Foundational	Advanced
System	3.1	Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	Y	
System	3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.	Y	



Standards Based Operations

- Secure Standard Builds
- Hardening Checklists

- 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



Disciplined Change and Exception Management

- Disciplined change management
- Disciplined vulnerability and patch management
- Consistent Exception Control & Documentation
 - Should include risk evaluation , risk mitigation strategies, and acceptance of risk
 - Expiration and re-analysis of risk acceptance



System and Vulnerability Management and Monitoring

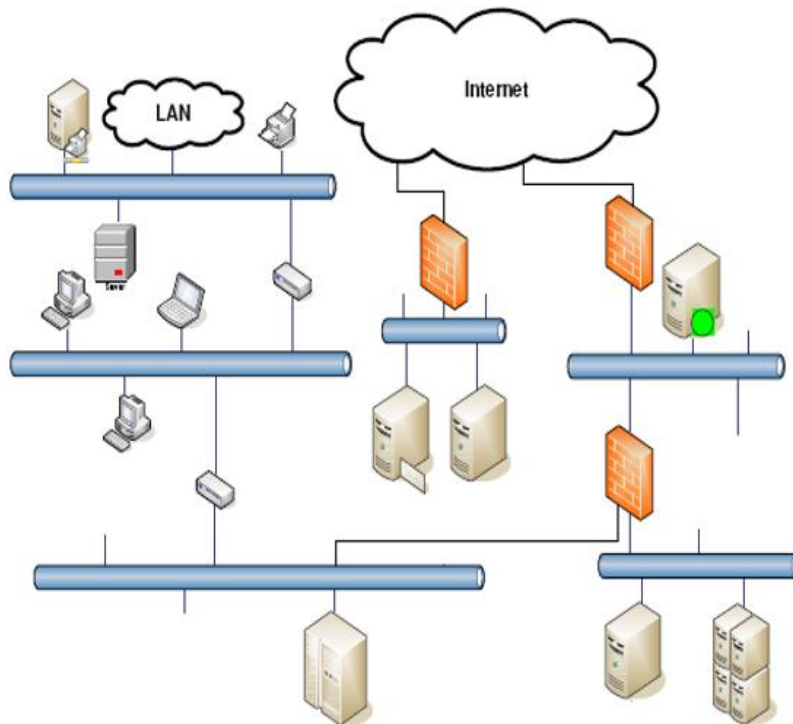
- Monitoring (built in)
 - Key system configurations
 - System and application logs
 - Accounts
 - Critical data systems/files
 - Data activity and flow
- Scanning (independent)
 - Patch Tuesday and vulnerability scanning
 - Rogue devices



Know Your Network

Know What “Normal” Looks Like

- Infrastructure
 - Servers & Applications
 - Data Flows
 - Archiving vs. Reviewing
-
- System inventory
 - Application inventory
 - Data inventory



Audit Logs and Password Auditing

- Configure system auditing/logging
 - Understand and document logging capabilities
 - Ensure all systems are configured to log important information
 - Retain logs for at least 1 year, longer is better
- Audit systems for default/weak passwords
 - Most systems have default passwords
 - ◇ Google: “Default password list”
 - Don’t overlook “simple” systems
 - ◇ E.g. Printer/multi-function devices, IP security cameras, etc.



Passwords

- Good Passwords
- Password Managers
- Two Factor/
Multi-Factor
Authentication

Password Audit	Total
Number of passwords audited	855
Passwords cracked	794
Passwords that were all letters	63
Passwords that were all numbers	5
Passwords that were an English word	20
Passwords that were a word with numbers appended to it	200
Passwords that were the same as the username	6
Passwords that do not meet Windows complexity	584



Protect Against Email Phishing

- Harden email gateway (spam filter)
 - Block potentially malicious file attachments
 - ◇ (e.g. ZIP, RAR, HTA, JAR)
 - Flag Office documents that contain Macros as suspicious
 - Prevent your organization's domain from being spoofed
 - ◇ Sender Policy Framework (SPF)
 - ◇ Custom rule to evaluate SMTP Letter FROM field
 - Flag emails that originate from the Internet
 - ◇ E.g. Modify subject line to say 'External'



Action Items

- Test backup systems
 - Periodically test backup systems to ensure you can recover from ransomware
 - Have IT perform a full, bare-metal system restore (operating system, applications, and data)
 - Have IT document how long it takes to recover various files or systems

➤ **PRACTICE**



Action Items

- TEST systems and people - Validate that your expectations are being met for cybersecurity
 - Penetration Testing
 - ◇ Collaborative/Informed/White Box
 - ◇ Uninformed/Black Box
 - Social Engineering Testing
 - True Breach Simulation
 - ◇ Red Team/Blue Team

➤ **PRACTICE**





Personal/Home Cybersecurity

Strategies and Action Items

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Update Your Software!

- Use current, up-to-date operating systems and software
- Turn on automatic updates
- Ensure your Anti-virus software is up-to-date
- Update third party software (Chrome, iTunes, Spotify, etc.)



IoT Devices

- Careful of what you plug in to your network
 - Cameras
 - Smart thermostats
 - Smart light bulbs
- Segment IoT devices when possible
- Alexa, Google Home and privacy concerns
- Smart TV's



Accounts and Data

- Multiple Passwords?
- Don't link your accounts
 - (i.e. “log in w/ Facebook”)
- Back up your data

Password1
Password2
Summer18
Spring18



Monitor and Alert – Google/Gmail

1-50 of 8,994

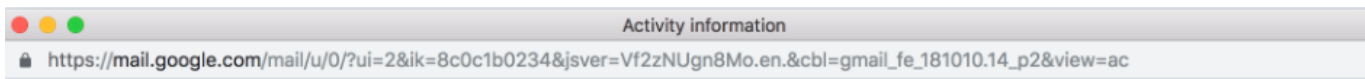
<input type="checkbox"/>			From	Subject	Date
<input type="checkbox"/>			Minnesota Youth Soc.	Experience Life Time Sport O...	Oct 17
<input type="checkbox"/>			Google Calendar	Notification: Wild Hockey vs. ...	Oct 16
<input type="checkbox"/>			Elizabeth Swenson	Advanced ELA 7: Reading Req...	Oct 16
<input type="checkbox"/>			Troop 106 - Phillip.	Aug minutes & meeting remin...	Oct 16
<input type="checkbox"/>			MoviePass	You're invited! - Pre-Release S...	Oct 16
<input type="checkbox"/>			Troop 106 - Jason B. 2	New Photos - I added photos f...	Oct 16

6.36 GB (42%) of 15 GB used [Manage](#) [Terms](#) · [Privacy](#) · [Program Policies](#) Last account activity: 4 minutes ago

[Details](#)



Monitor and Alert – Google/Gmail



Activity information

https://mail.google.com/mail/u/0/?ui=2&ik=8c0c1b0234&jsver=Vf2zNUgn8Mo.en.&cbl=gmail_fe181010.14_p2&view=ac

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. [Learn more](#)

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

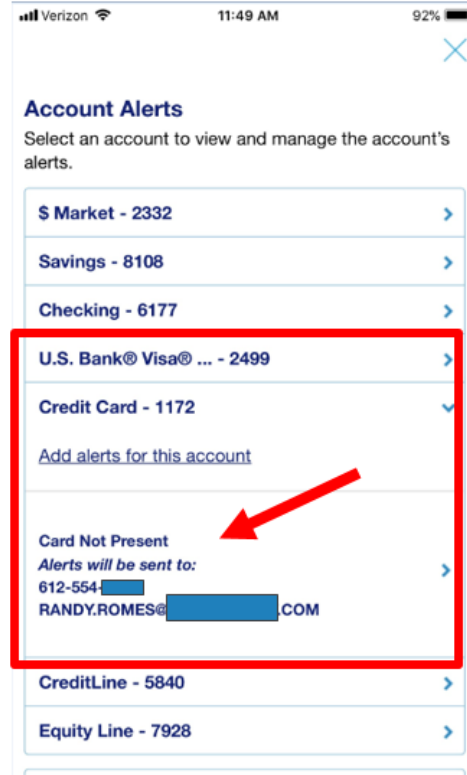
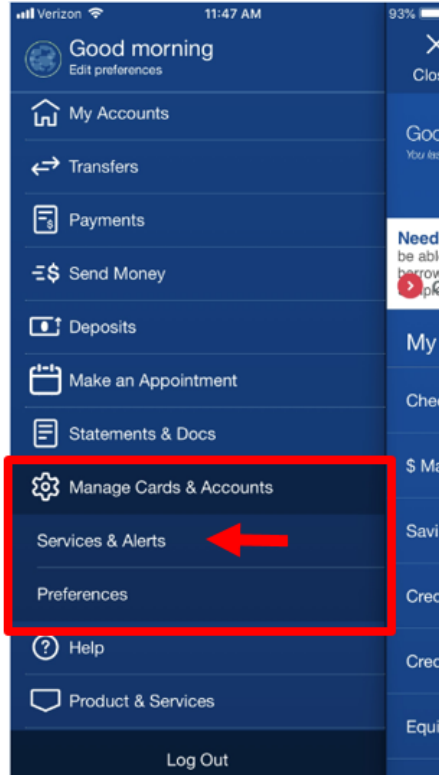
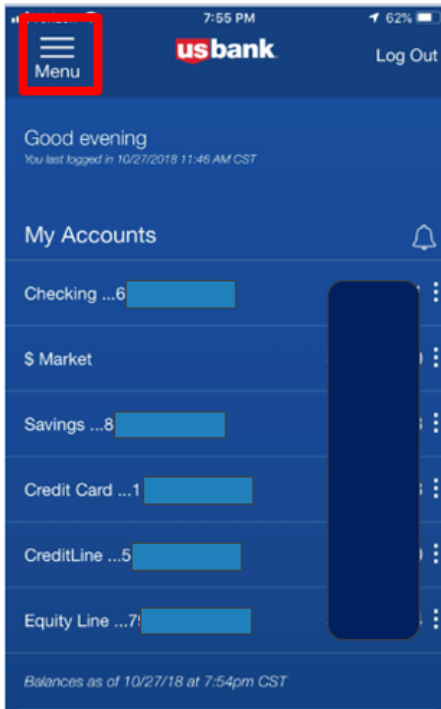
[Sign out all other Gmail web sessions](#)

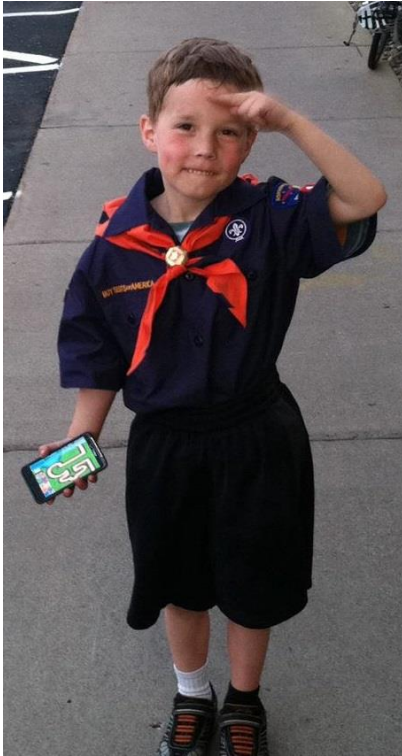
Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Authorized Application (445112211283-sk04feuogpcjd3dq8eshrdnr4bpm1sfk.apps.googleusercontent.com) Show details	United States (40.97.151.149)	1:59 pm (5 minutes ago)
Browser (Chrome) Show details	* United States (MN) (2600:1014:b065:3cfe:912c:198:482:1e24)	1:47 pm (17 minutes ago)
Browser (Chrome) Show details	* United States (MN) (2600:1014:b065:3cfe:912c:198:482:1e24)	1:05 pm (59 minutes ago)
Browser (Chrome) Show details	* United States (MN) (2600:1014:b065:3cfe:912c:198:482:1e24)	12:39 pm (1 hour ago)
Browser (Chrome) Show details	* United States (MN) (2600:1014:b065:3cfe:912c:198:482:1e24)	11:43 am (2 hours ago)
Authorized Application (450232826690-0rm6bs9d2fps9tifvk2oodh3tasd7vi7.apps.googleusercontent.com) Show details	United States (MN) (73.5.138.250)	4:19 am (9 hours ago)
Browser (Chrome) Show details	* United States (MN) (73.5.138.250)	12:03 am (14 hours ago)
Browser (Chrome) Show details	* United States (MN) (73.5.138.250)	Oct 26 (14 hours ago)
Browser (Chrome) Show details	* United States (MN) (67.137.57.251)	Oct 26 (19 hours ago)



Monitor and Alert – Banking





Questions?





Thank you!

Randy Romes
CISSP, CRISC, MCP, PCI-QSA
Principal - Information Security
Direct: 612-397-3114
Randy.Romes@claconnect.com

