Higher Education Webinar

Cyber Hygiene for a Remote Workforce

David Anderson, Principal
Kadian Douglas, Principal

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Create Opportunities

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.

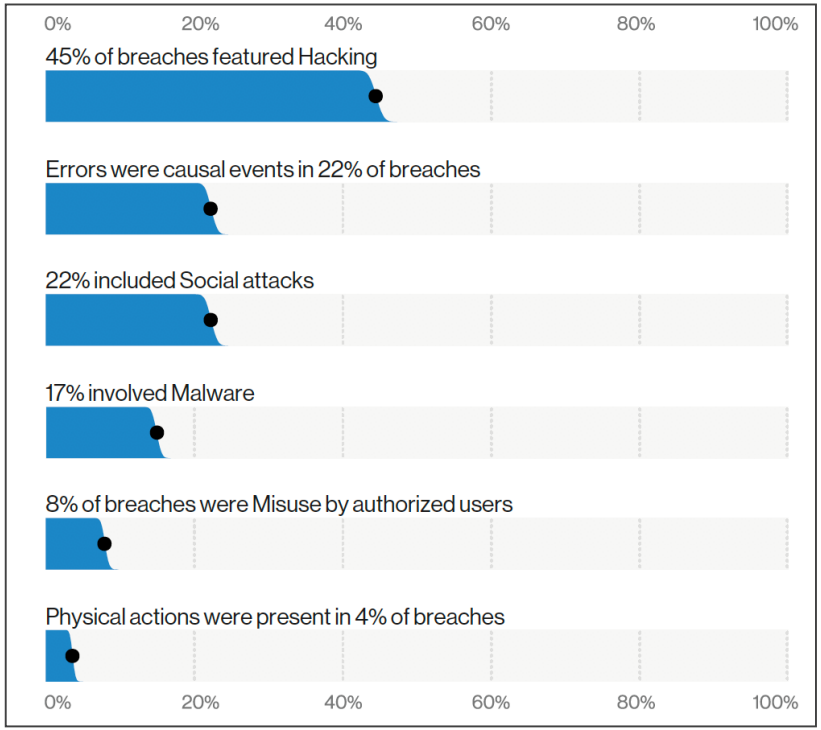
Learning Objectives

- Identify common attacks that are increasing due to the shift in remote work
- Recognize what types of remote access are acceptable and/or secure
- Identify opportunities when implementing a remote workforce

Recent Trends

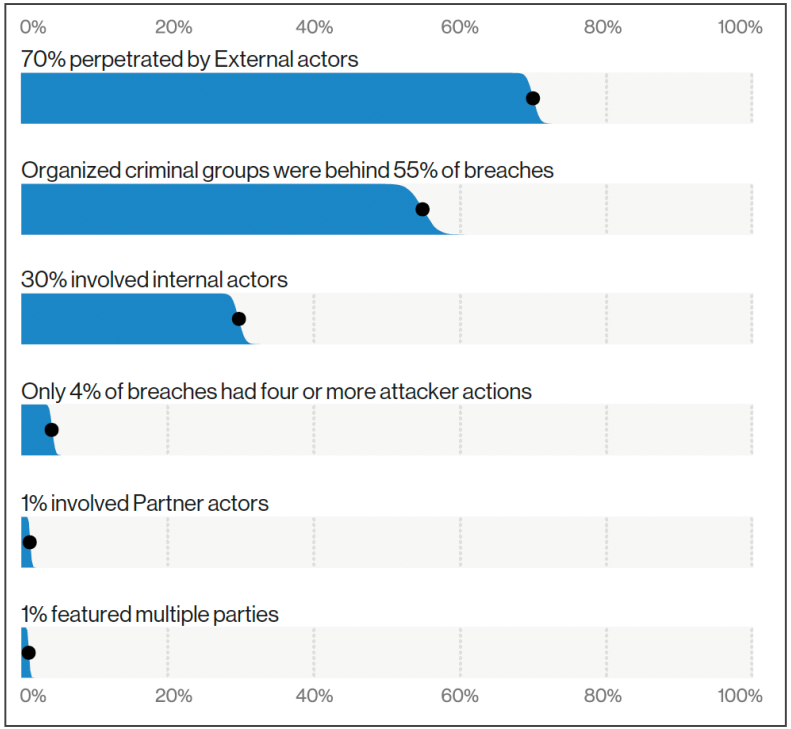
Across All Industries

Causes of Data Breaches



Across All Industries

Who's Behind the Breaches



Threat Actors (Education)

Who is behind the security incident?

67% External

33 % Internal

Threat Actor Motivations (Education)

92% FINANCIAL

5% FUN

Impacts Due to COVID

- Suppressed department budgets
- Routine IT tasks paused to support remote workforce
- Compromising security controls to support remote workforce
  - New practices = new weaknesses

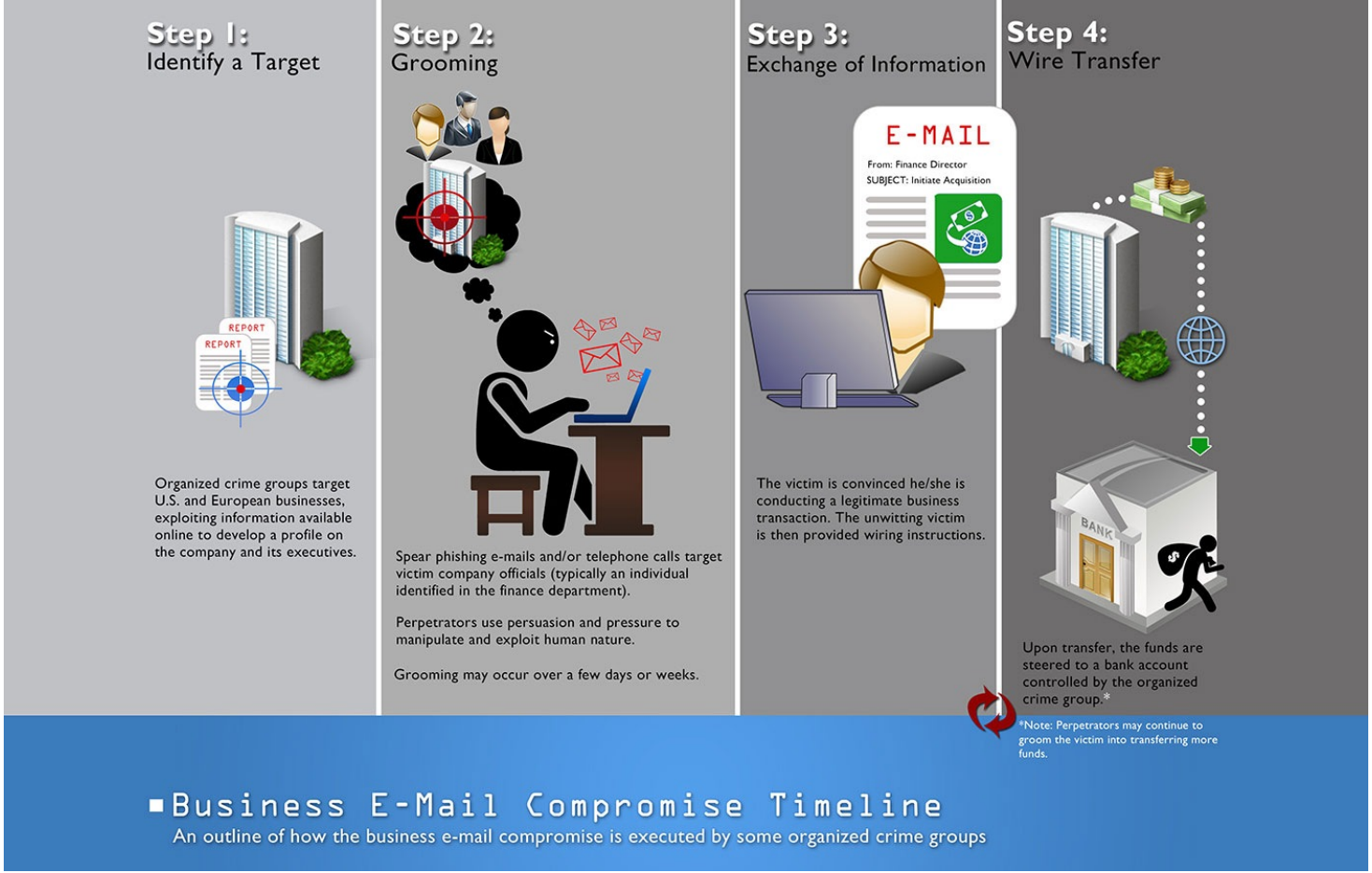
Common Cyber Attacks

- Email Compromise
- Ransomware

- Both of these are facilitated by Social Engineering
  - Phishing
  - Phone calls

What is Business Email Compromise?

- Fraudsters impersonate employees or vendors via email in an attempt to steal money
  - Fake vendor invoice
  - Exec asks staff to “buy gift cards”
  - Update direct deposit account
  - Etc.
- Malware often not needed



https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

How attackers perform BEC

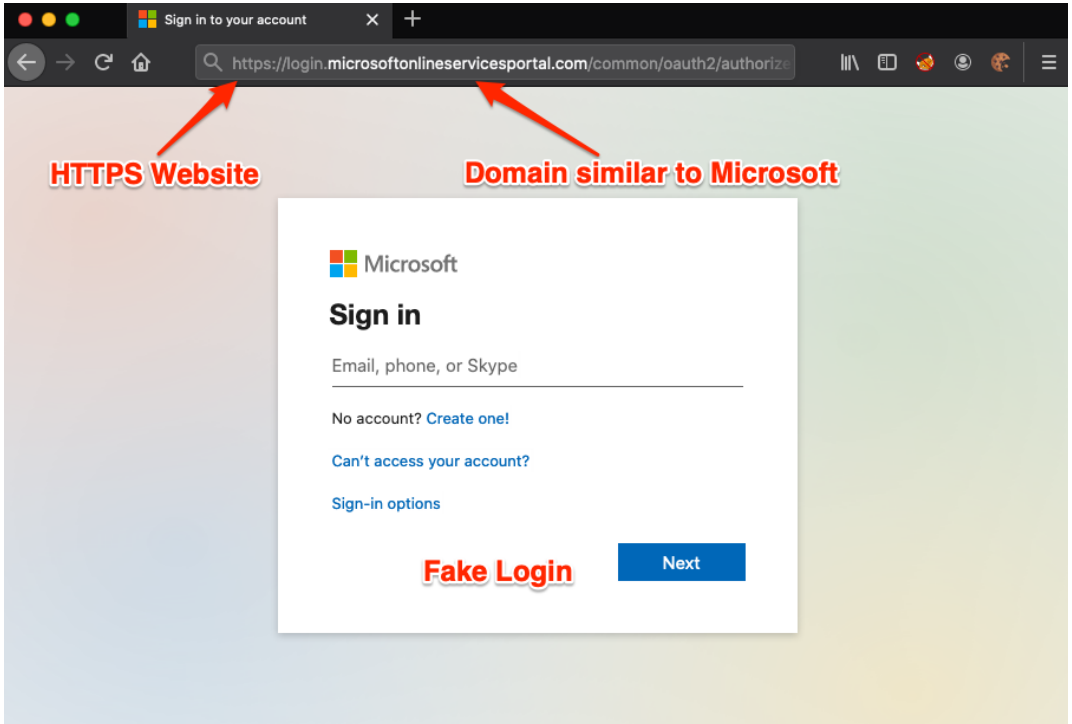
- Email spoofing
- Domain impersonation
- Name dropping
- Compromised email

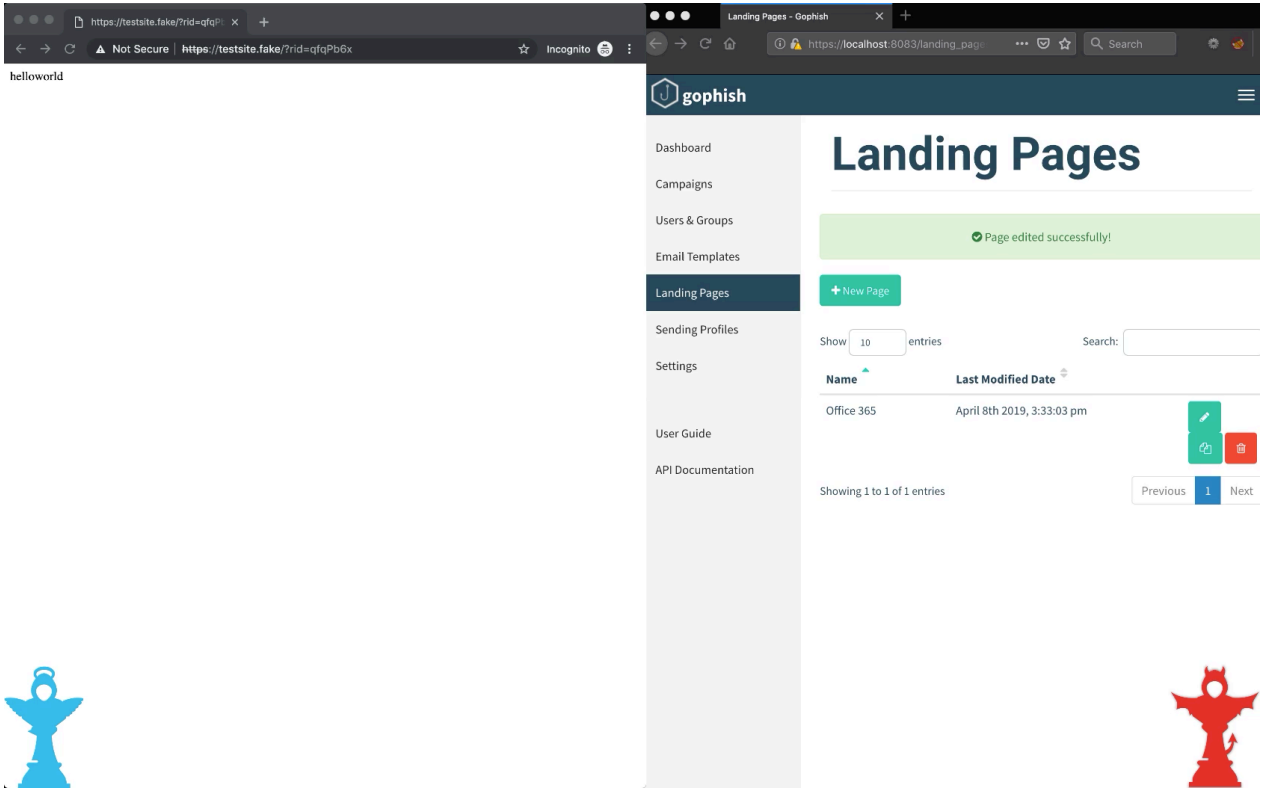
Exchange Online / Office 365

- Email is accessible from anywhere in the world
  - No longer need to find where you “are” on the Internet

- Easy to steal passwords and try logging into Office 365
  - Fake websites and password guessing tools

Fake Login Portal





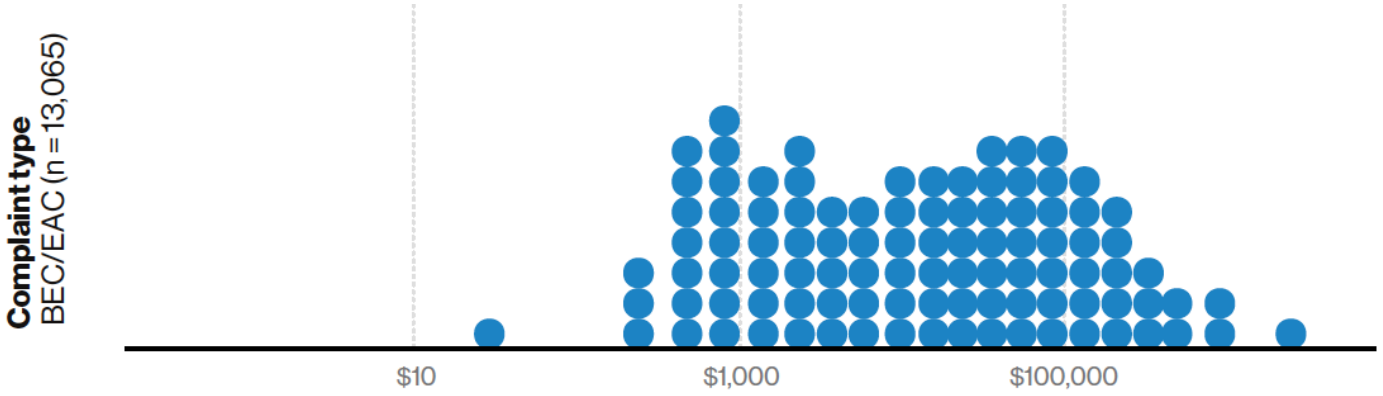
Password Guessing

```
[DBUG] Opening SSH connection to root@1.2.3.4
[DBUG] /usr/bin/ssh root@1.2.3.4 -D 33482
[DBUG] Waiting for /usr/bin/ssh root@1.2.3.4 -D 33482
[DBUG] Proxy: socks4://127.0.0.1:33482
[INFO] Spraying 2 users against https://login.microsoft.com at Sun Sep  6 17:19:01 2020
[INFO] Command: ./trevorspray.py -e bob@evilcorp.com alice@evilcorp.com -p Fall2020! asdf --ssh root@1.2.3.4
[SUCC] bob@evilcorp.com : Fall2020! - NOTE: The response indicates MFA (Microsoft) is in use.
[WARN] Invalid email or password. email: alice@evilcorp.com could exist.
[INFO] Finished spraying 2 accounts at Sun Sep  6 17:19:03 2020
[SUCC] bob@evilcorp.com : Fall2020!
[DBUG] 2 valid emails written to /trevorspray/log/valid_emails.txt
[DBUG] 1 valid user/pass combos written to /trevorspray/log/valid_logins.txt
```

https://github.com/blacklanternsecurity/TREVORspray

Cost of BEC

- Exploitation of cloud-based email has cost US businesses 2.1+ billion



Lots of claims around $40K

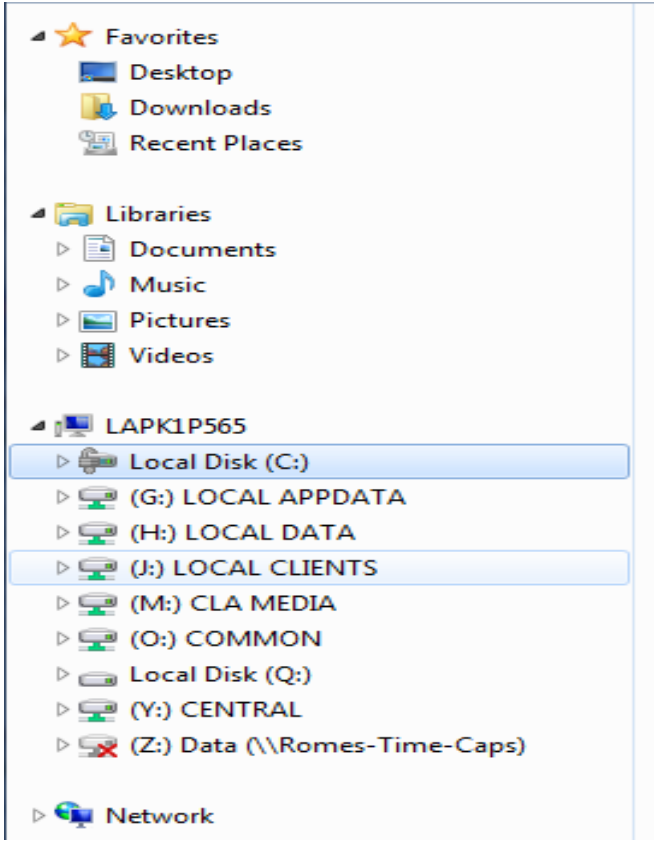
50% of victims recover money

Where are the attackers?

- Complaints filed with the FBI
  - 85% of victims and subjects in the same country
  - 56% in the same state
  - 35% in the same city

Ransomware

- Malware that encrypts your files/system and makes them unusable



Ransomware

- Attack on the **Availability** of network data
- Easier to do than exfiltration of the data
- Uses strong encryption to render victims' files unreadable
- Payments are often in Bitcoin
- Cyber criminals attempt to delete host and network backups
- User credentials are used for network access
- Many variants and constant evolution

In the News

University Pays $457K After Ransomeware Attack

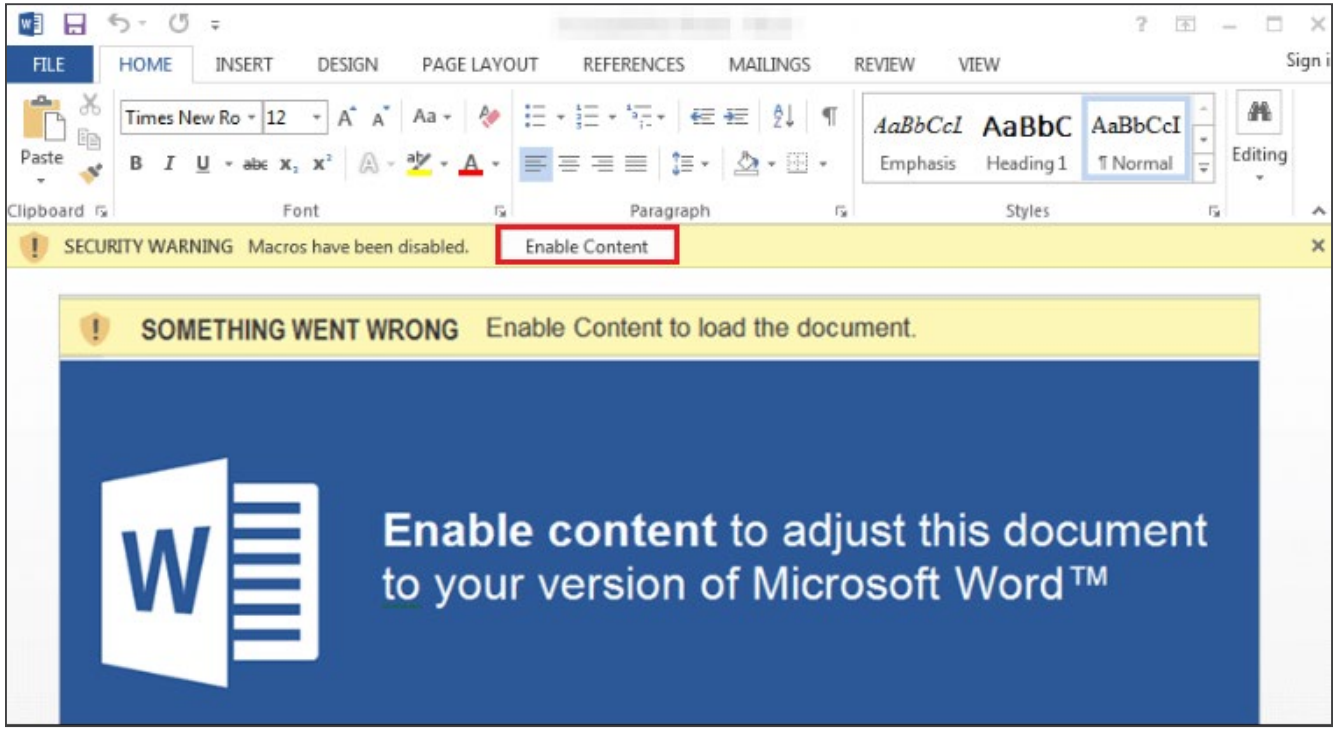
Ransomeware attack: University had data protection but it wasn't used on affected systems

University Dodges A Bullet As Fake COVID-19 Survey Leads To Ransomeware Attack

Ransomware Delivery

- Stealing remote login credentials and then deploying ransomware
- Delivering ransomware via email attachments
  - Office documents
  - HTA files
  - ZIP files

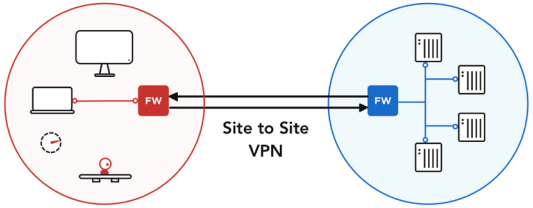
Office Malware

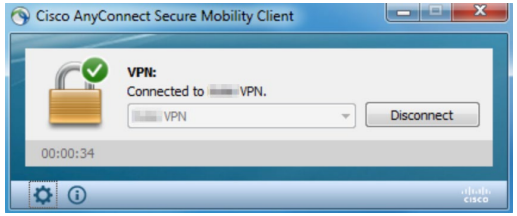


Securing Remote Access

Remote Access

- Remote access solutions
  - VPN
    - ◊ Site-to-Site
    - ◊ Client-Access
  - Applications





CITRIX

vmware Horizon

Remote Desktop Services Default Connection
RemoteApp and Desktop Connection

Remote Access Security Concerns

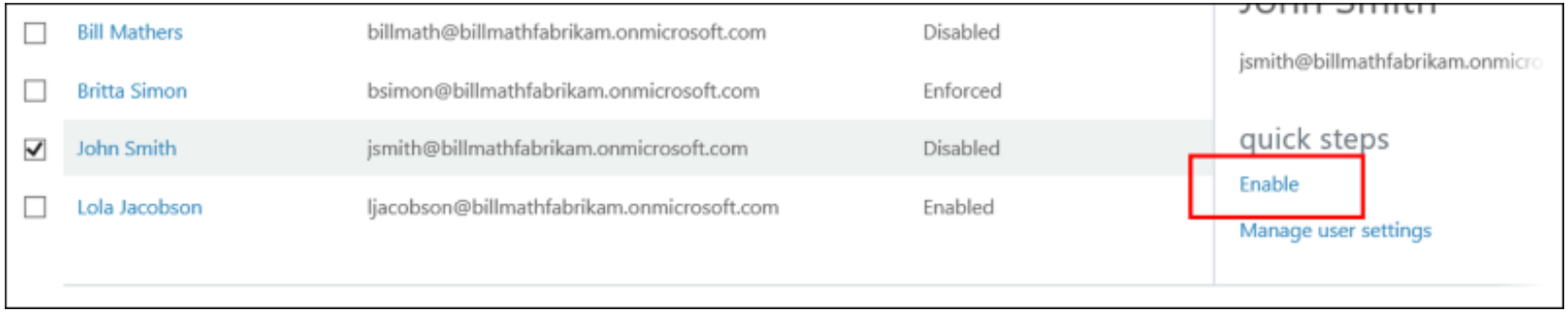
- Is it exposed to the entire Internet
- How is access controlled
  - Username + password
  - Multi-factor
- Can it be accessed from unmanaged devices
- How is monitoring and logging configured

Remote Access Security Best Practices

1. Limit types of remote access technologies
   - Use firewall rules/access controls lists to limit remote access to sensitive data
   - Don’t expose RDP to the Internet…just don’t…
   - Limit remote access to sensitive data to managed devices

Remote Access Security Best Practices

2. Enable multi-factor authentication on as many accounts as you can



Remote Access Security Best Practices

3. Configure robust logging/auditing
   - Daily/weekly reports of who has connected to VPN
     - Who (name/username)
     - When (date/time)
     - Where (source IP address/geolocation)

Other Cybersecurity Controls

Security Best Practices

1. Update policies and procedures to reflect current environment
   - Remote access policy
   - Password reset processes
   - Etc.

Security Best Practices

2. Harden email/spam filter
   - Block emails that impersonate your domain
   - C-level protections (based on name of employees)
   - Enable mailbox auditing
   - Retain logs for access/logins
   - Configure SPF, DKIM, DMARC on email server

Security Best Practices

2. Harden email/spam filter (cont.)
   - Disable legacy email protocols
   - Disable automatic email forwarding
   - Restrict logins geographically (only allow US logins)
   - You can restrict access to managed/company owned devices
   - Block unauthorized files (.exe, .zip, .hta, .js, etc.)

Security Best Practices

3. Document trusted phone numbers of vendors
   - Change of payments requests need to be validated through a phone call

Security Best Practices

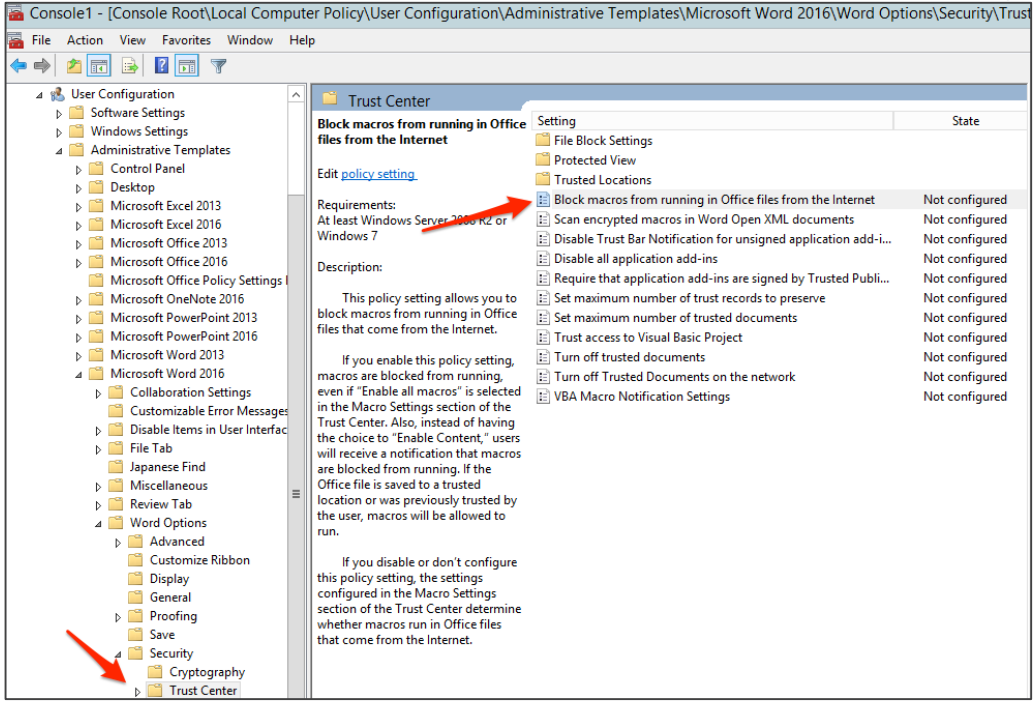
4. Train your users
   - How to review emails for suspicious content
     - ◊ Review “FROM” address closely
     - ◊ Hover over links
   - That you expect them to validate requests over the phone
   - Who to contact if they suspect they have an issue

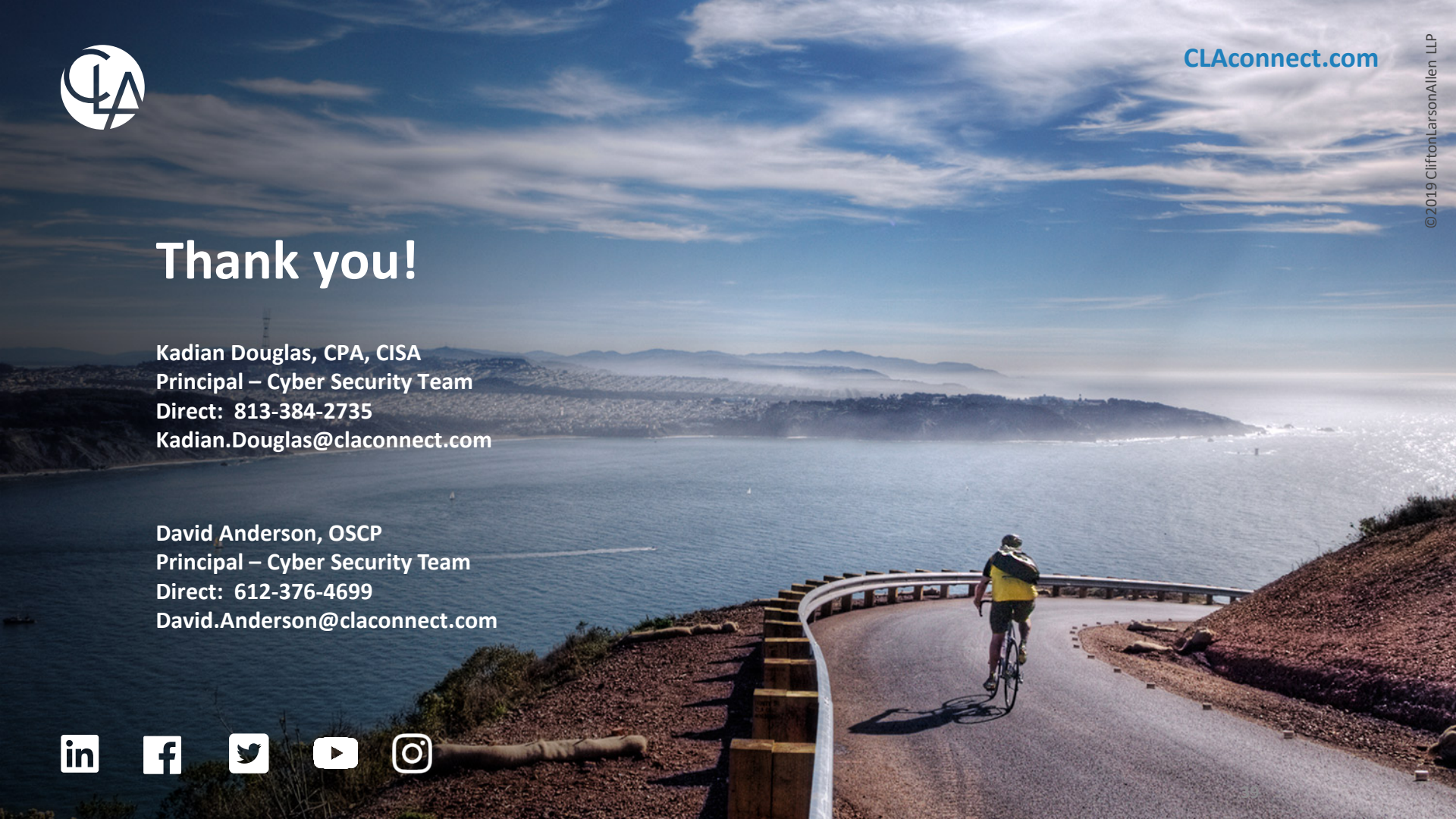
Security Best Practices

5. Have good backups
   - Keep backups isolated from network/offline
   - Test your backups and recovery procedures regularly

Security Best Practices

6. Block Office macros
   - Identify what users need macros: train them
   - Block macros for those who don't need it





CLAconnect.com

Thank you!

Kadian Douglas, CPA, CISA
Principal – Cyber Security Team
Direct: 813-384-2735
Kadian.Douglas@claconnect.com

David Anderson, OSCP
Principal – Cyber Security Team
Direct: 612-376-4699
David.Anderson@claconnect.com