Risks and Trends in Cybersecurity and Fraud

2020 Update

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

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

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

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

- Define cyber crime
- Identify payment fraud trends and tactics hackers are using
- Recognize how and why hackers are targeting you
- Describe recent cyber crime litigation issues
- Describe common information security weaknesses
- Explain solutions to help minimize risk

Hackers have "monetized" their activity

– More hacking

– More sophistication

– More "hands-on" effort

– Smaller organizations targeted

Current State of Affairs

Organized Crime

- Wholesale theft of personal information

Ransomware

- Holding your data hostage

Payment Fraud

- "Corporate Account Take-Over" - aka CATO
- Use of credentials to commit online banking and credit card fraud

Credential "Harvesting"

Ransomware

Ransomware

- CryptoWall, CryptoLocker, wannacry, petya, **Ryuk** etc.

- Encrypt all data, hold it "ransom" for $$

- Starting to target other operating systems, like Macs

Create Opportunities

3 Generations

1. Local machine only

2. Local machine plus network permissions

3. Local machine plus *ENTIRE NETWORK*

Payment Fraud
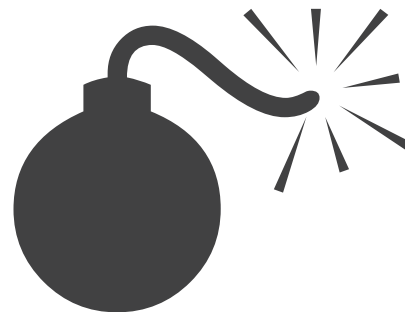
Corporate Account Takeover – 3 Versions

1. Deploy malware – keystroke logger

2. Deploy malware – man in the middle

3. Recon/email persuasion

   1. *"Whaling"*

   2. *Business email Compromise*

   3. *CEO attack*
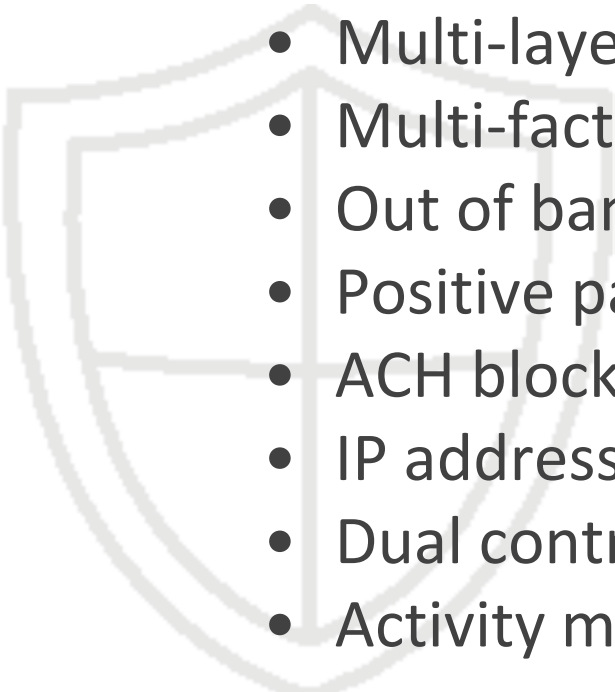
      1. *NEW – W2 attacks*

Multi-Factor Authentication Solutions

- MFA is critical

- Silver bullet?

- Text msg?

CATO Defensive Measures

- Multi-layer authentication
- Multi-factor authentication
- Out of band authentication
- Positive pay
- ACH block and filter
- IP address filtering
- Dual control
- Activity monitoring

Credential Harvesting

Credential Harvesting

- Driven by movement to the cloud

- Malware

- Social engineering

COVID "Opportunities"

1. Virus/health related news
2. Remote Work force
3. Re-opening of businesses
4. SBA funding
5. PPP programs
6. Political news

COVID "Opportunities"

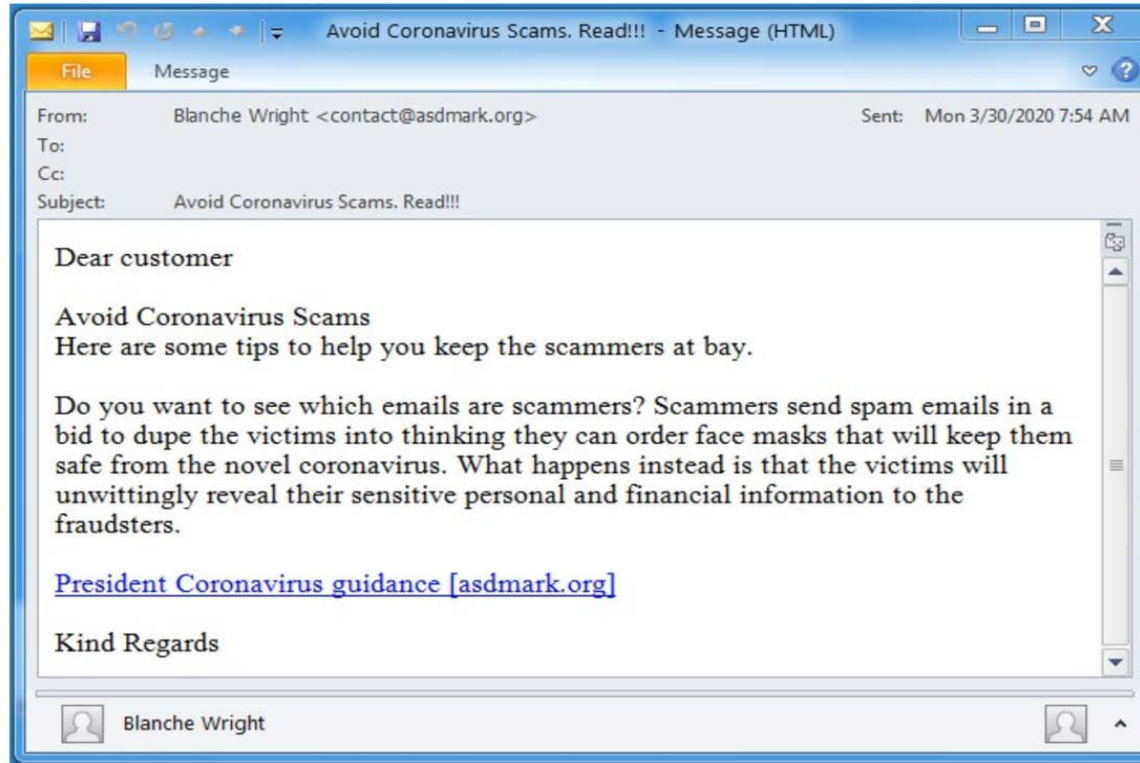Most breaches have a root cause in some form of Phishing

What is "Spear Phishing"

These templates, which use realistic-looking graphics, are designed to imitate the World Health Organization, the U.S. Centers for Disease Control and Prevention, the Internal Revenue Service, as well as government websites in the U.K., Canada and France, according to Proofpoint. The templates enable fraudsters to quickly create malicious domains to lure victims who have been sent phishing emails, according to the researchers. Of the more than 300 phishing attacks that Proofpoint has examined since January, nearly half were designed to steal either login credentials or banking information.
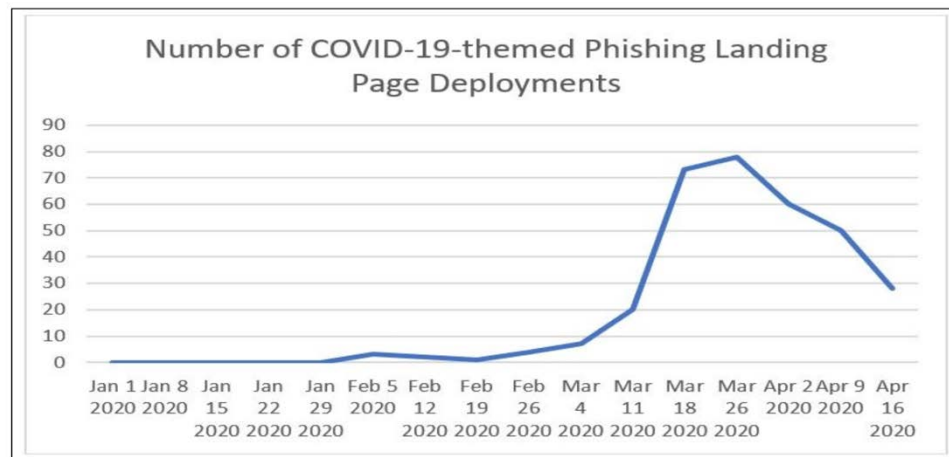
(Source: Proofpoint)

As more governments around the world offer stimulus payments and financial assistance to citizens and businesses, the lures have shifted, says Sherrod DeGrippo, senior director of threat research and detection at Proofpoint.

Example Coronavirus email - March

Avoid Coronavirus Scams. Read!!! - Message (HTML)

File   Message

From: Blanche Wright <contact@asdmark.org>   Sent: Mon 3/30/2020 7:54 AM
To:
Cc:
Subject: Avoid Coronavirus Scams. Read!!!

Dear customer

Avoid Coronavirus Scams
Here are some tips to help you keep the scammers at bay.

Do you want to see which emails are scammers? Scammers send spam emails in a bid to dupe the victims into thinking they can order face masks that will keep them safe from the novel coronavirus. What happens instead is that the victims will unwittingly reveal their sensitive personal and financial information to the fraudsters.

President Coronavirus guidance [asdmark.org]
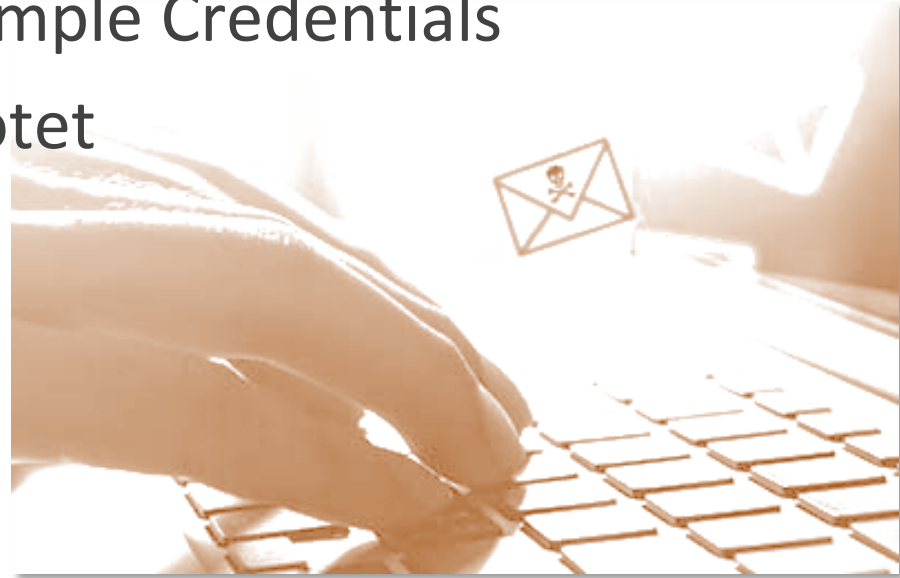
Kind Regards

Blanche Wright

Credential Harvesting

Trends Within the Trend

- RAT

- Default / Simple Credentials

- Rise of Emotet

Credential Compromise

- Guessing
- Cracking
- Sniffing (interception)
- Keystroke logging
- Browser scraping
- Social engineering
- Reuse

Tip: Build a password from a phrase.

I like to eat Oreo cookies
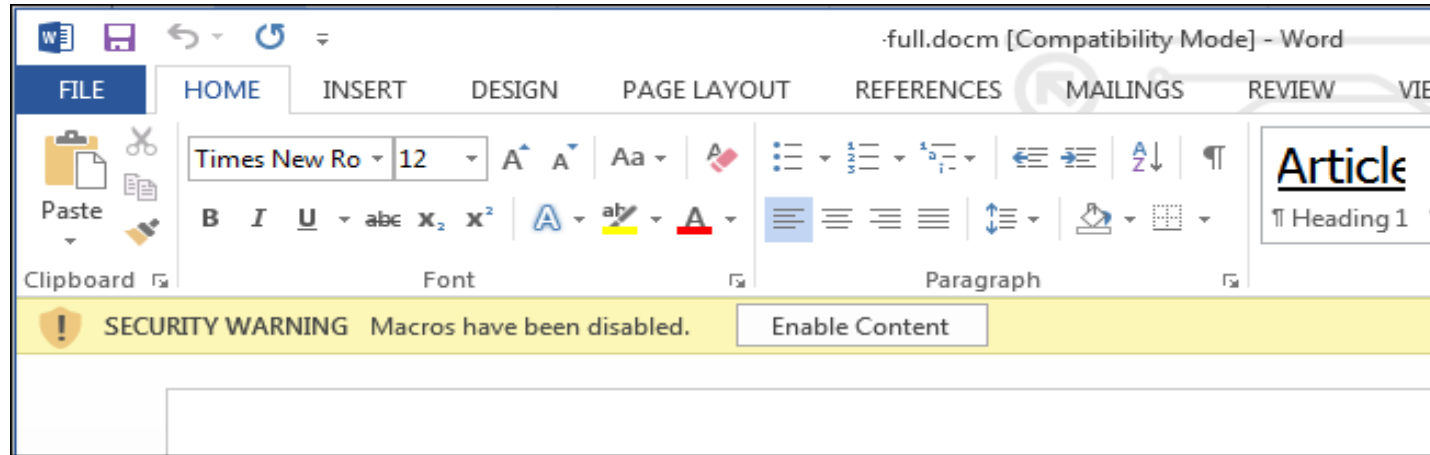   at night.

ilteocan

or, even better:

Il2eOc@n

Create Opportunities

Spear Phishing Tricks

- Malware Delivery
  - ZIP file attachments
  - Office Macros

Create Opportunities

Mitigation Keys

- Train users regarding email phishing
- Maintain current patch levels
- Remove local administrators
  - Best practice for ADMINS?
- ***Maximize relationship with the bank***
- ***Isolate the PC used for online banking***
- ***Air gap the back up media***
- Implement breach monitoring/ incident response
- Use MFA for all cloud apps

Current State of Affairs

The Cost
Global cybercrime cost business up to:
$400 **BILLION** annually

Some companies theorize it will reach:
$2.1 **TRILLION** by 2019

"There are only two types of companies: Those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again."
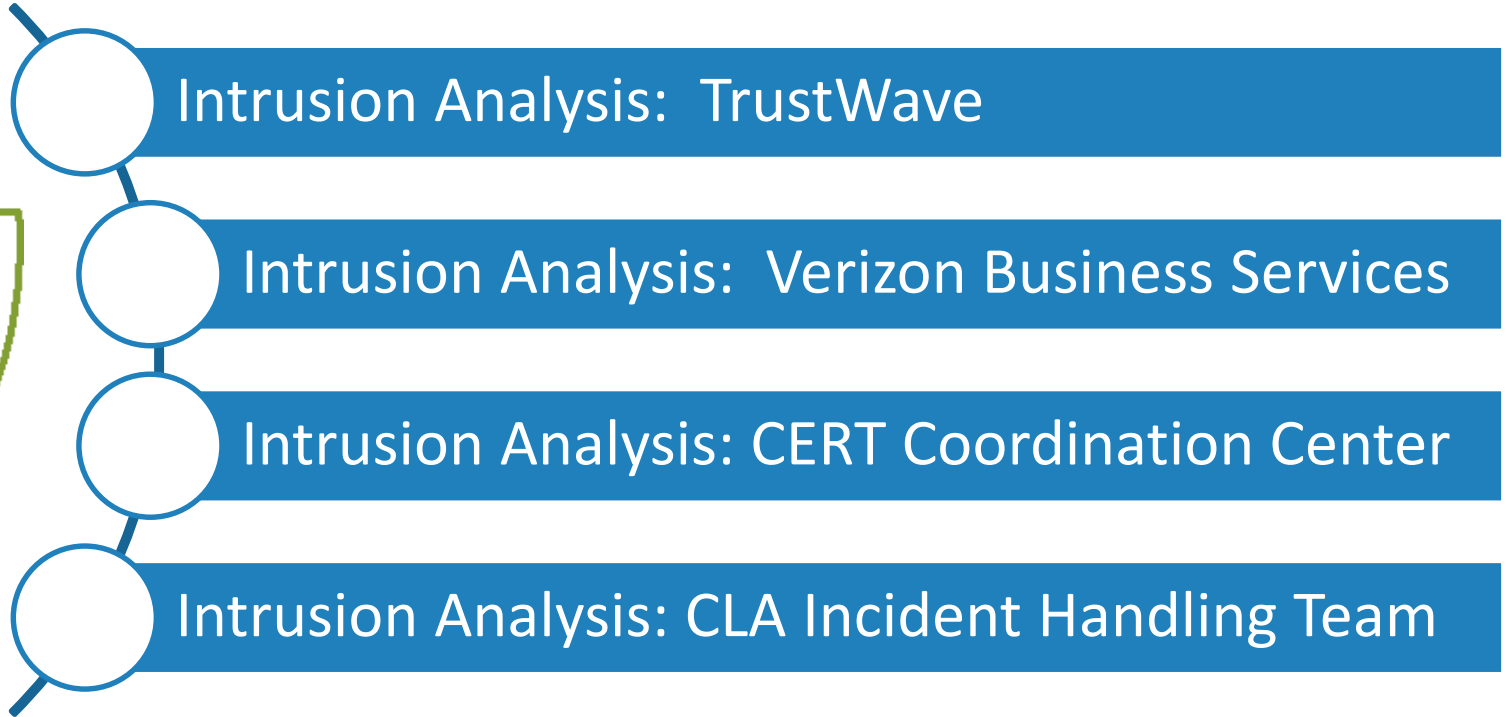
- Robert Mueller

Create Opportunities

10 Key Defensive Measures

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

96% of Attacks are Preventable!

Intrusion Analysis: TrustWave

Intrusion Analysis: Verizon Business Services

Intrusion Analysis: CERT Coordination Center

Intrusion Analysis: CLA Incident Handling Team

Strategies

Our information security strategy should have the following objectives:

- Users who are more aware and savvy
- Networks that are resistant to malware
- Relationship with our financial institution is maximized

Create Opportunities

Ten Keys to Mitigate Risk

1. **Strong Policies -**

   - Email use

   - Website links

   - Removable media
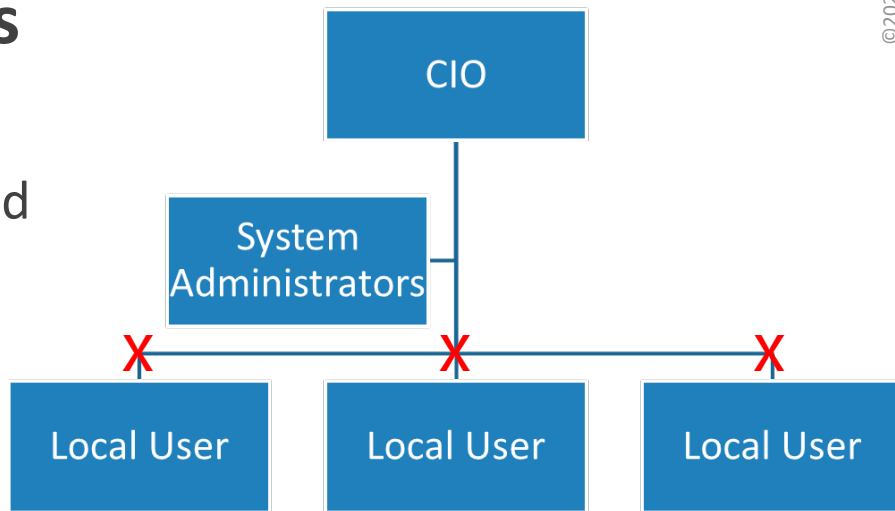
   - **Users vs Admin**

Ten Keys to Mitigate Risk

2. **Defined user access roles and permissions**

- Principal of minimum access and least privilege

- **Users should <u>NOT</u> have system administrator rights**

  - **"Local Admin" in Windows should be removed (if practical)**

Ten Keys to Mitigate Risk

3. Hardened internal systems (end points)

- Hardening checklists
- Turn off unneeded services
- **Change default password**
- **Use Strong Passwords**
- **Consider application white-listing**

4. Encryption strategy – data centered

- Email
- Laptops and desktops
- Thumb drives
- **Email enabled cell phones**
- Mobile media

Create Opportunities

5. Vulnerability management process

- Operating system patches

- **Application patches**

- Testing to validate effectiveness –
  - "belt and suspenders"

Ten Keys to Mitigate Risk

6. Well defined perimeter security layers

- **Network segments**
- Email gateway/filter
- Firewall – "Proxy" integration for traffic in AND out
- Intrusion Detection/Prevention for network traffic, Internet facing hosts, AND workstations (end points)

7. Centralized audit logging, analysis, and automated alerting capabilities

- Routing infrastructure
- Network authentication
- Servers
- Applications
- Know what "normal" looks like…

Create Opportunities

Ten Keys to Mitigate Risk

8. **Defined incident response plan and procedures**

   - **Be prepared**

   - Including data leakage prevention and monitoring

   - Application whitelisting

   - Forensic preparedness

   - Insurance

   - Practice…

Ten Keys to Mitigate Risk

9. Know/Use Online Banking Tools

- Multi-factor authentication
- Dual control/verification
- Out-of-band verification/call-back thresholds
- ACH positive pay
- ACH blocks and filters
- Review contracts relative to all these
- Monitor account activity *daily*
- **Isolate the PC used for wires/ACH**

Create Opportunities
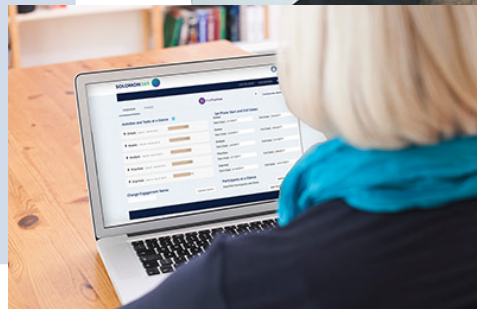
Ten Keys to Mitigate Risk

10. Test Test Test

- "Belt and suspenders" approach
- Penetration testing
  ◊ Internal and external
- Social engineering testing
  ◊ Simulate spear phishing
- Application testing
  ◊ Test the tools with your bank
  ◊ Test internal processes

Create Opportunities

Questions?

Mark Eich

Principal

Information Security

mark.eich@claconnect.com

***

(612) 397-3128

Create Opportunities