

CYBER SECURITY THREATS AND SAFEGUARDS IN HEALTHCARE

PRESENTED BY TODD SORG, COO & CISO AT CIT



www.cit-net.com | info@cit-net.com | 651.255.5780

TODAY'S AGENDA



1 WHAT IS THE CURRENT THREAT LANDSCAPE?

2 HOW TO RECOGNIZE ATTACKS

3 WHAT CAN WE DO ABOUT IT?

CIT TIMELINE

Founded May 1, 1992



MidAmerica Bank Building Woodbury 1992



More Than **5** Employees



Christenson Ave. West St Paul 1995

Ventura Drive Woodbury 1998



More Than **10** Employees



Cabling Services late 1990's

App/Dev Services late 1990's



More Than **25** Employees



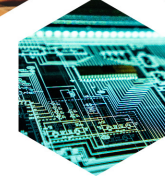
Managed Services 2003

Security Services 2015



More Than **50** Employees

SOC 2 Type I Compliant 2018



SOC 2 Type II Compliant 2020

More Than **75** Employees



Designated Autism-Friendly Workplace 2021

Clare Lane NE Rochester May 2021



More Than **100** Employees

ABOUT ME



TODD SORG
CHIEF OPERATING OFFICER & CISO

- Senior technology executive with over 25 years of experience in IT operations and Cybersecurity.
- In my current role, I focus on helping develop and mature the security programs for organizations in the healthcare, finance, manufacturing, and education industries as part of the small and medium-size business markets.



THE THREAT LANDSCAPE

- 🛡️ Ransomware
- 🛡️ Phishing
- 🛡️ Supply chain
- 🛡️ Data breach












WHY HEALTHCARE?

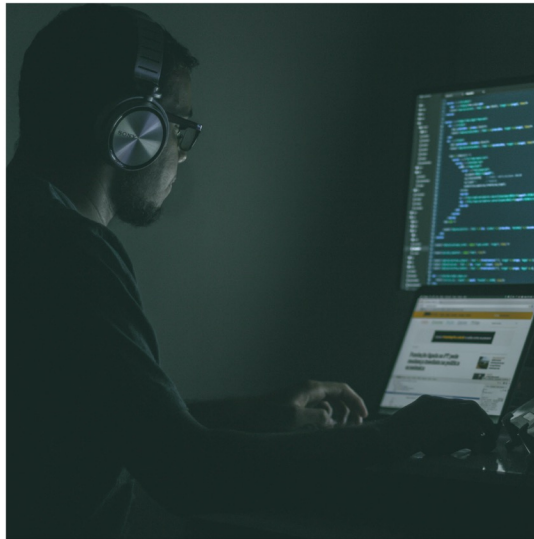
- Social Security & credit card info
- Personally Identifiable Information (PII)
- Insufficient security controls
- Security control friction
- Mobile technology increases risks

Who's at Risk? Knowbe4

The top three industries by organization size

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
 34.0% Healthcare & Pharmaceuticals	 42.3% Hospitality	 52.4% Energy & Utilities
 32.9% Education	 35.7% Energy & Utilities	 51.6% Insurance
 31.2% Not For Profit	 35.6% Healthcare & Pharmaceuticals	 47.5% Banking

NOT IF



BUT WHEN

HEALTHCARE CYBERSECURITY ACT 2022

In 2021, 46 million Americans had their health information breached as a result of a cyberattack – Bill Cassidy press release

- Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS) to define how to improve cybersecurity processes in hospitals and health systems
- An analysis of how identified cybersecurity risks specifically impact Healthcare and Public Health Sector assets, including the impact on rural and small and medium-sized Healthcare and Public Health Sector assets
- All Medical equipment owned, leased, or relied on
- How you protect and respond
- Must find, train and retain cybersecurity expertise



WHAT IS PHISHING?

Emails that attempt to entice individuals to reveal personal information or sensitive data.

SPEAR PHISHING

- Attack on a specific user or organization designed to look legitimate
- Sent to a small number of recipients
- Communications appear to come from a trusted source

WHALING

- Attack on high-ranking individuals within an organization
- Communications appear to come from a trusted source

**88% OF ORGANIZATIONS
WORLDWIDE EXPERIENCED SPEAR
PHISHING ATTEMPTS IN 2019** (Proofpoint)



PHISHING TECHNIQUES



- **HYPERLINKS**
 - Malware
 - Credential harvesting
 - Disguised as attachments
- **ATTACHMENTS**
 - Malware
 - Macros
 - Fake invoices
- **POSING AS TRUSTED USERS/ORGANIZATIONS**
 - Domain spoofing
 - Display name spoofing
 - Typo squatting
- **BUSINESS EMAIL COMPROMISE**
 - To other employees
 - To vendors/business affiliates
- **OPEN SOURCE/SOCIAL MEDIA**
- **CURRENT EVENTS/HOLIDAYS**
- **REQUESTS FOR UNTRACEABLE ITEMS**



SPOTTING A PHISH

- Unexpected messages
- Unknown senders
- Sent outside of normal business hours
- Messages that attempt to instill a sense of urgency
- Hyperlinks, message content, and/or tone seems strange or out of character
- Poor grammar/spelling
- Offering something too good to be true
- Displayed hyperlink URL mismatched to actual hyperlink URL

EXAMPLE OF DISPLAY NAME SPOOFING

From: Christopher Taylor <exc.personal112@gmail.com>

Sent: Thursday, August 8, 2019 8:58 AM

To: [REDACTED]

Subject: RE:

This message was sent from outside of the organization. Please do not click links or open attachments unless you recognize the source of this email and know the content is safe.

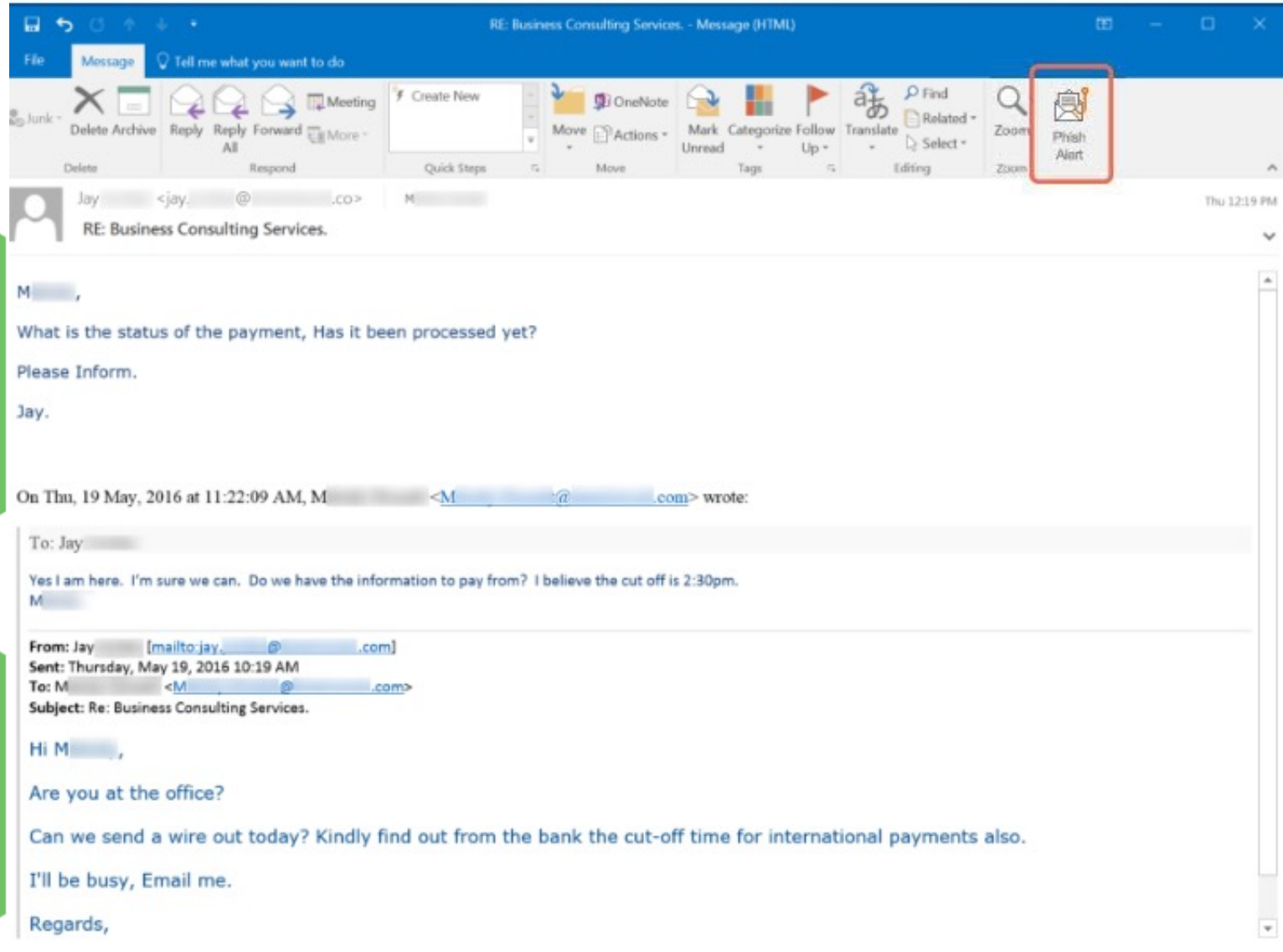
[REDACTED]

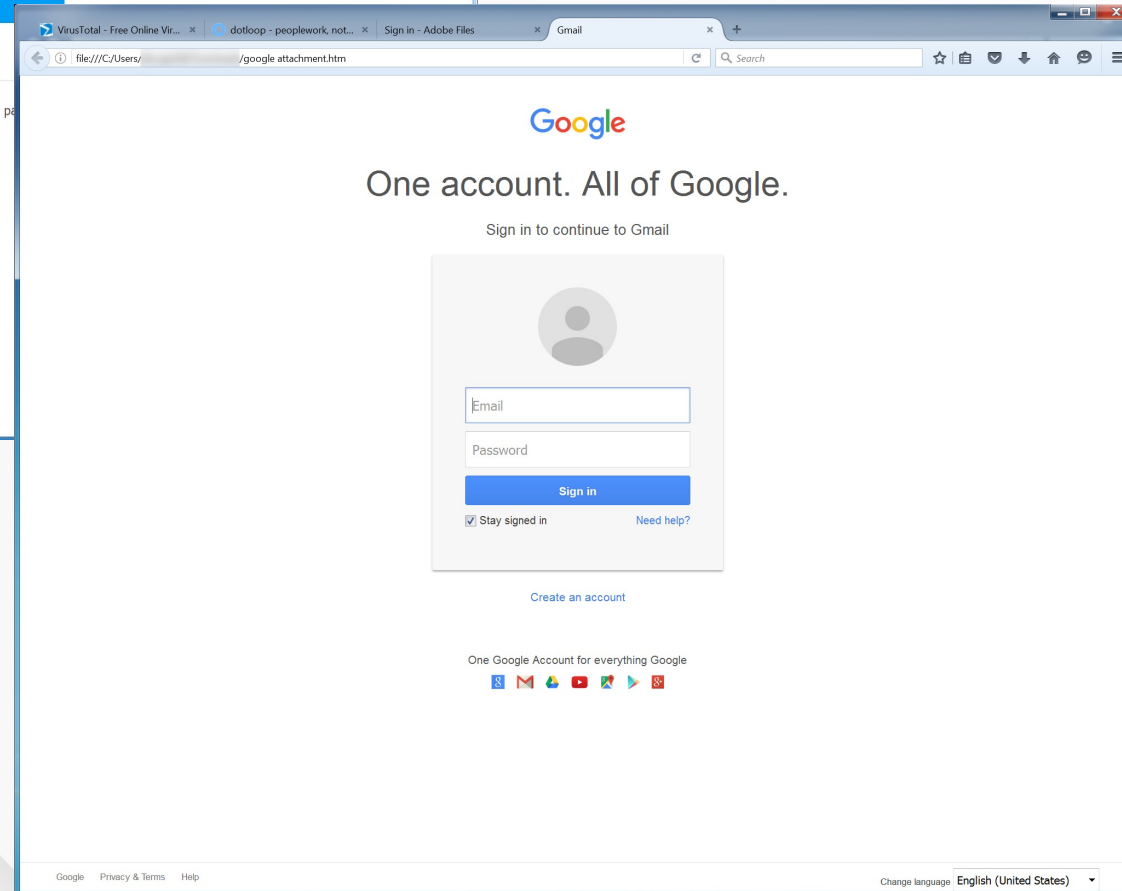
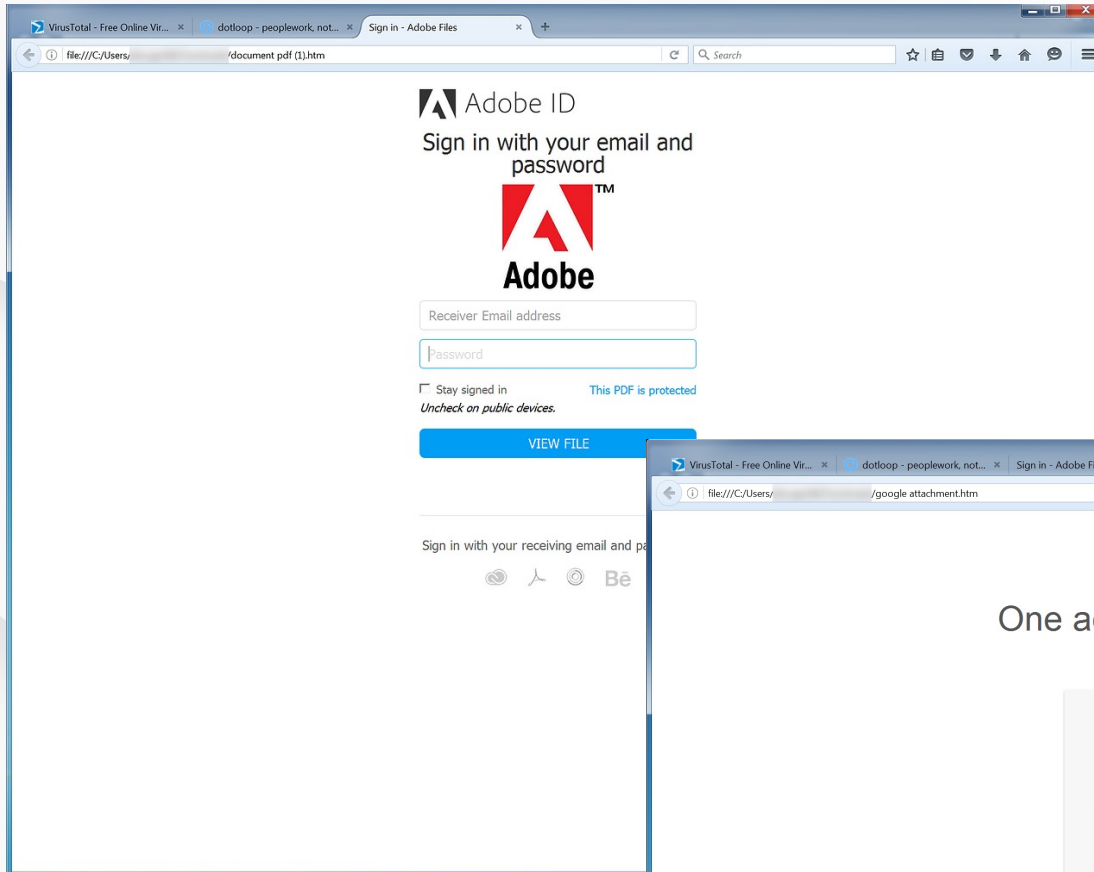
I'm having a busy day and I trust I can count on you to keep this as a surprise. I'm looking forward to surprise some of the staff with Gift cards, for hard work and dedication and I want this to remain between you and I pending when they received it. I need you to make a purchase on my behalf, I'm considering Target, Walmart or Best Buy Gift Card since we have them almost everywhere. Let me know when you get this.

Regards,
Christopher Taylor.

94% OF MALWARE IS DELIVERED VIA EMAIL

(CSO ONLINE)





From: Chase [.com](#)>
Sent: Wednesday, September 25, 2019 11:02 AM
Subject: Corporation

This message was sent from outside of the organization. Please do not click links or open attachments unless you recognize the source of this email and know the content is safe.

 ACI AIA Document13.pdf
155 KB

Review the approved ,
Let me know if there is anything else you need

<https://app.box.com/s/tngs4vj7dlhichnq3uzujtpa0cmummy8w> of the organization
Click or tap to follow link.

 ACI AIA Document13.pdf
155 KB

EXAMPLE OF IMAGE WITH EMBEDDED LINK DISGUISED AS ATTACHMENT


From: Cheri [.com](#)>
Sent: Thursday, September 19, 2019 8:54 AM
Subject:

This message was sent from outside of the organization. Please do not click links or open attachments unless you recognize the source of this email and know the content is safe.

 PYMNT_ADVICE.pdf
6 KB

Review the approved ,
Let me know if there is anything else you need
Cheri

<https://app.box.com/s/sto015sgdggf4tgewaqr7ek7c48u5911> of the organization
Click or tap to follow link.

 PYMNT_ADVICE.pdf
6 KB

PHISHING PSYCHOLOGY EVOLUTION



 Urgency

 Plausibility

 Familiarity

 Confidentiality

IDENTIFY - GOVERNANCE

Policy & Procedures, Hardware & Software Asset Management



PROTECT - ADMINISTRATIVE AND TECHNICAL CONTROLS

Data encryption, User training, & Access Management



DETECT - DETECTION OF INTERNAL AND EXTERNAL THREATS

Anomalous Threats, Vulnerability Detection & Continuous Monitoring



RESPONSE - ABILITY TO RESPOND TO DETECTED THREATS

NDR/EDR/XDR, Geo Filtering, Migrations Efforts, etc.



RECOVER - BUSINESS CONTINUITY & DISASTER RECOVERY

Data Backups, Disaster Recovery Plan & Tabletop Exercises



FOLLOWING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) FRAMEWORK MEANS:

- Ensuring your technical resources and people are secure
- Creates the foundation for achieving compliance for your industry-specific regulations
- Deploying a complete set of tools to create a handcrafted solution
- Continuous monitoring of your security controls



WHAT DOES THAT LOOK LIKE?

- On-going Simulated Phishing Attacks
- Cybersecurity Awareness Training
- Enable Multi-factor Authentication
- Endpoint Detection & Response (EDR)
- Dark Web Monitoring
- Annual Security Reviews & Scans
 - Active Directory Review
 - Firewall Review
 - Email Review
 - Internal & External Vulnerability Scans
- Ensure Proper Patch Management is in place
- Develop and implement an Incident Response Plan
- Security Information and Event Management (SIEM)



ENDPOINT DETECTION & RESPONSE (EDR) VS ANTIVIRUS



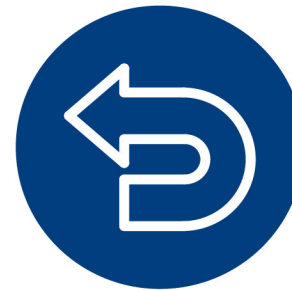
IDENTIFY



PROTECT



DETECT



RESPOND



RECOVER



EDR



**ANTI
VIRUS**

QUESTIONS?



THANK YOU!



WE MAKE TECHNOLOGY
WORK FOR BUSINESS