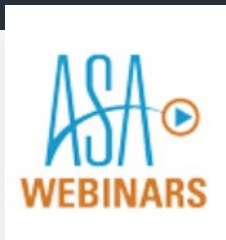


Welcome to Today's Webinar

Cybersecurity: Protecting Your Staffing Business Against Online Threats

Thursday, Sept. 19, 2024, 2 p.m. Eastern time

Please note that the audio will be streamed through your computer—there is no dial-in number. Please make sure to have your computer speakers turned on or your headphones handy.



American Staffing Association

A screenshot of a Zoom meeting control bar. The bar is dark grey with a white background for the menu. On the left, there are three icons: a hand for 'Raise Hand', two speech bubbles for 'Q&A', and a 'CC' icon for 'Live Transcript'. A mouse cursor is hovering over the 'Live Transcript' button. A dark grey menu is open over the 'Live Transcript' button, containing three options: 'Show Subtitle' (highlighted in blue), 'View Full Transcript', and 'Subtitle Settings...'.

CC
Live Transcript

Show Subtitle
View Full Transcript
Subtitle Settings...

Raise Hand Q&A

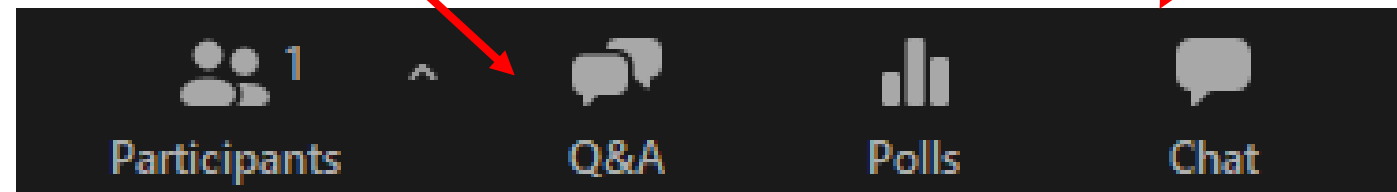
Ask a Question, Engage With Other Attendees

Q&A

Type your questions for the panel into the Q&A box

Chat

Start a conversation—say hello. Engage with panelists and other attendees.





ASA Certification Continuing Education

Today's webinar qualifies for 1.0 CE hour

- **Live webinar:** **NEW as of April 2024**—CE credits earned from attending this program are *automatically* added to your online CE Status within three business days.
- **On-demand viewers:** Submit this earned CE using the online submission form at *americanstaffing.net*.

- This program is valid for **PDCs** for the SHRM-CP® or SHRM-SCP®.

Activity ID: 24-2DGDQ



USE PROMO CODE:

“40WEBPS”



ASA **Staffing
Pro Stacks**SM

americanstaffing.net/pro-stacks



Our Presenters Today



Edward Foley

Senior Vice President, Risk Management
Summit Financial Group



Daniel Metcalf

Managing Partner and Co-Founder
Cyberfin



Michael O'Brien

Executive Vice President
Amwins Insurance Brokerage

Cyber Security: Protecting Your Staffing Business Against Online Threats

The #1 Financial Risk to a Business



HIGHLIGHTS

- HOW Cyber – crimes effect staffing firms and what to look out for.
- Cyber Myths Debunked
- Valuable tips to create and sustain resiliency.
- Current Cyber Insurance Market Conditions
- Silent Cyber: What is it: How to insure it.



Presenters

Edward J. Foley Senior Vice President, Risk Management, Summit Financial Group

Ed is a seasoned insurance executive with over 35 years of experience in sales, operations, claims, and risk management. Currently, he serves as Senior Vice President of Risk Management at Summit Financial Group. In this role, Ed's responsibilities include evaluation of first and third-party cyber loss exposures and to correspondingly secure optimal insurance solutions for businesses across various industry verticals, including the staffing and overall contingent labor sectors.

Throughout his career, Ed has earned a variety of industry credentials, including the Chartered Property and Casualty Underwriter (CPCU), Associates in Risk Management (ARM), Registered Professional Liability Underwriter (RPLU), and Cyber Professional Liability Practitioner (CPLP) designations.



Daniel Metcalf is the Managing Partner and Co-Founder of CyberFin.

Dan has become known as the "Geek" at CyberFin, specializing in solving business challenges related to technology in the insurance and financial services industry. Since 2016, Daniel has focused on consulting and delivering Cyber security services to financial institutions and regulated professional services organizations. Daniel has successfully made these services accessible to businesses of all sizes, not just large enterprises. Dan is a cybersecurity expert well-equipped to outline the essential steps that today's staffing and recruiting firms need to take to protect their digital assets and maintain robust security measures.



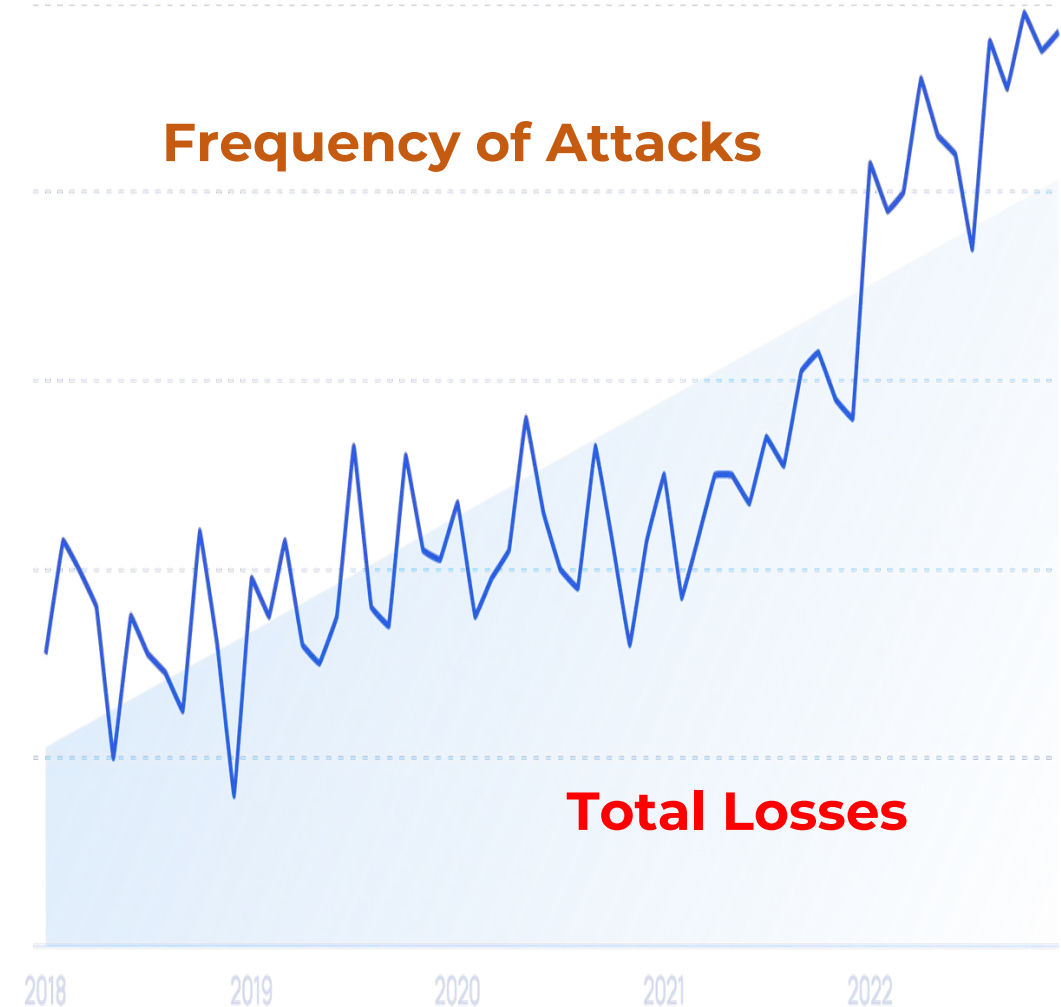
Michael O'Brien, Executive Vice President Amwins Insurance Brokerage

Mike is a 25-plus year insurance veteran specializing in a broad variety of insurance products, including Management Liability, Technology Errors and Omissions Liability, and Cyber first- and third-party Insurance products, serving a cross-section of business and industry. He is Executive Vice President at Amwins Insurance Brokerage, the largest excess and surplus line insurance brokerage in the United States, where he has worked for more than 21 years and currently leads a team whose focus includes representing multiple carriers offering Cyber Insurance products and services.

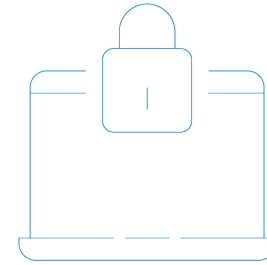
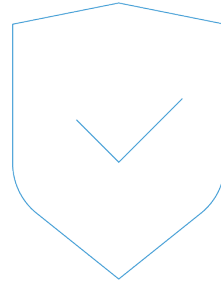
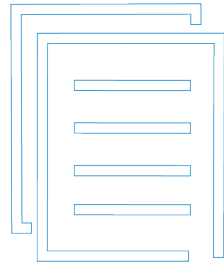
Cyber Attacks are Growing in Intensity

#1 Financial Risk to a Small and Medium Sized Business in 2024

- Cost of a breach is up **50% since 2021 - \$3MM**
- **61% of SMBs** hit by an attack in '23
- **50% lost customers** and data due to a breach



How did we get here?



Lack in time, resources and knowledge



Security

Productivity

Compliance

...Tends to Look More Like This

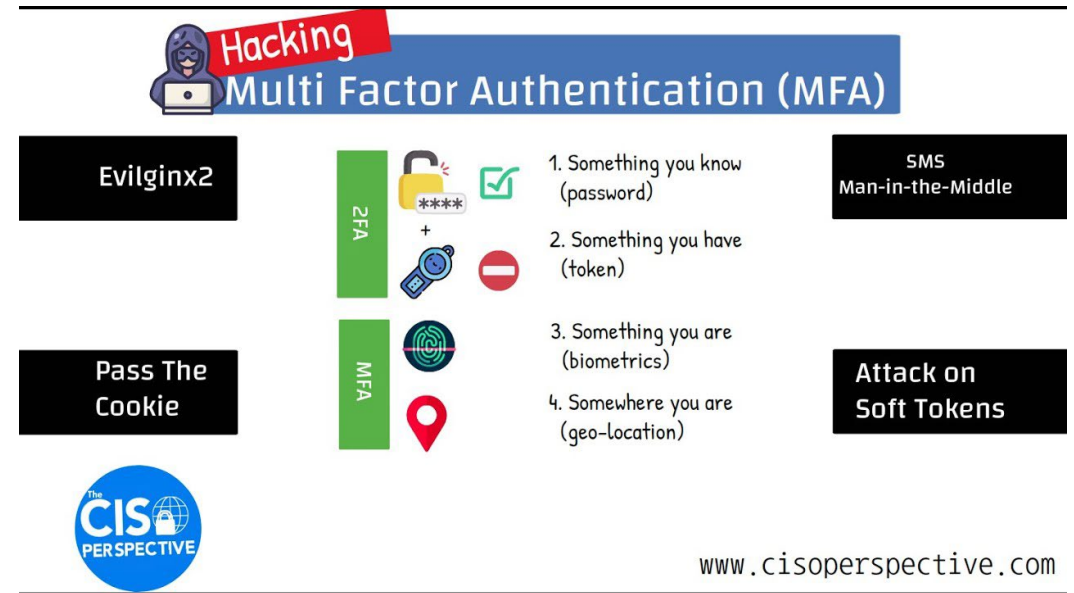


Lack of Security Infrastructure



Checking the “IT Security” Box

48% of breaches would not have been prevented by Multi-factor authentication



Data is the New Gold



“DATA IS THE NEW GOLD”

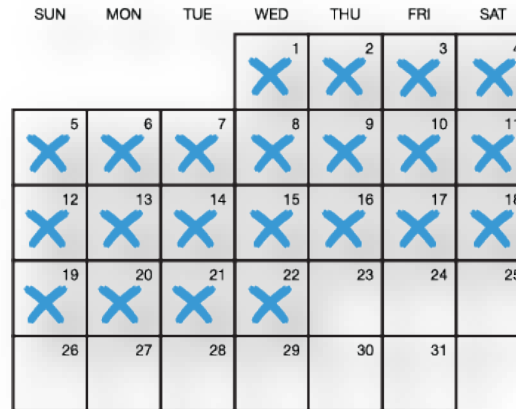
It's Where The Money Is



Cyber Crime – The Aftermath



Average downtime for a ransomware attack¹



22 Days



Fines for Non-Compliance

FINRA – Not to exceed

\$2500 per consumer

HIPPA: **\$50 per consumer up to \$1.5MM per incident/yr**

State Commerce Department Average:

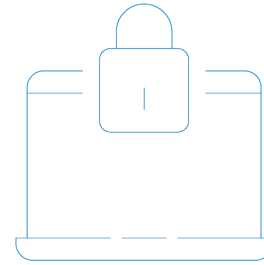
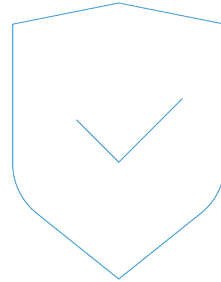
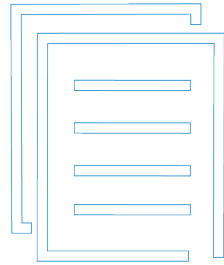
\$154 per record

1000 records = **\$150,000**

Insurance is highly regulated at the federal level through HIPAA, alongside the 13 states that have state privacy laws, in addition to the 50 states that have data breach notification laws.

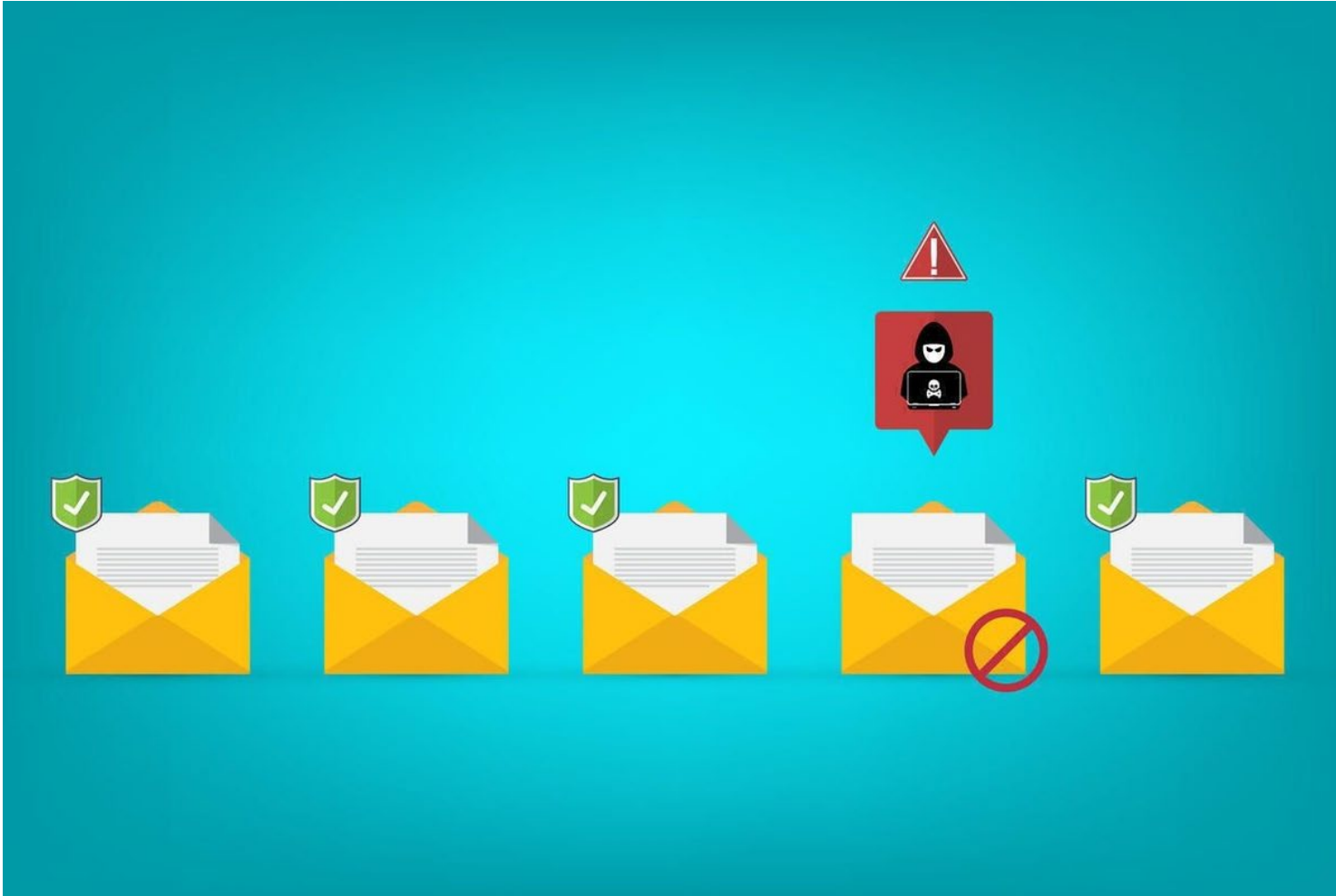


How do Criminals Make Money?





Cyber Extortion



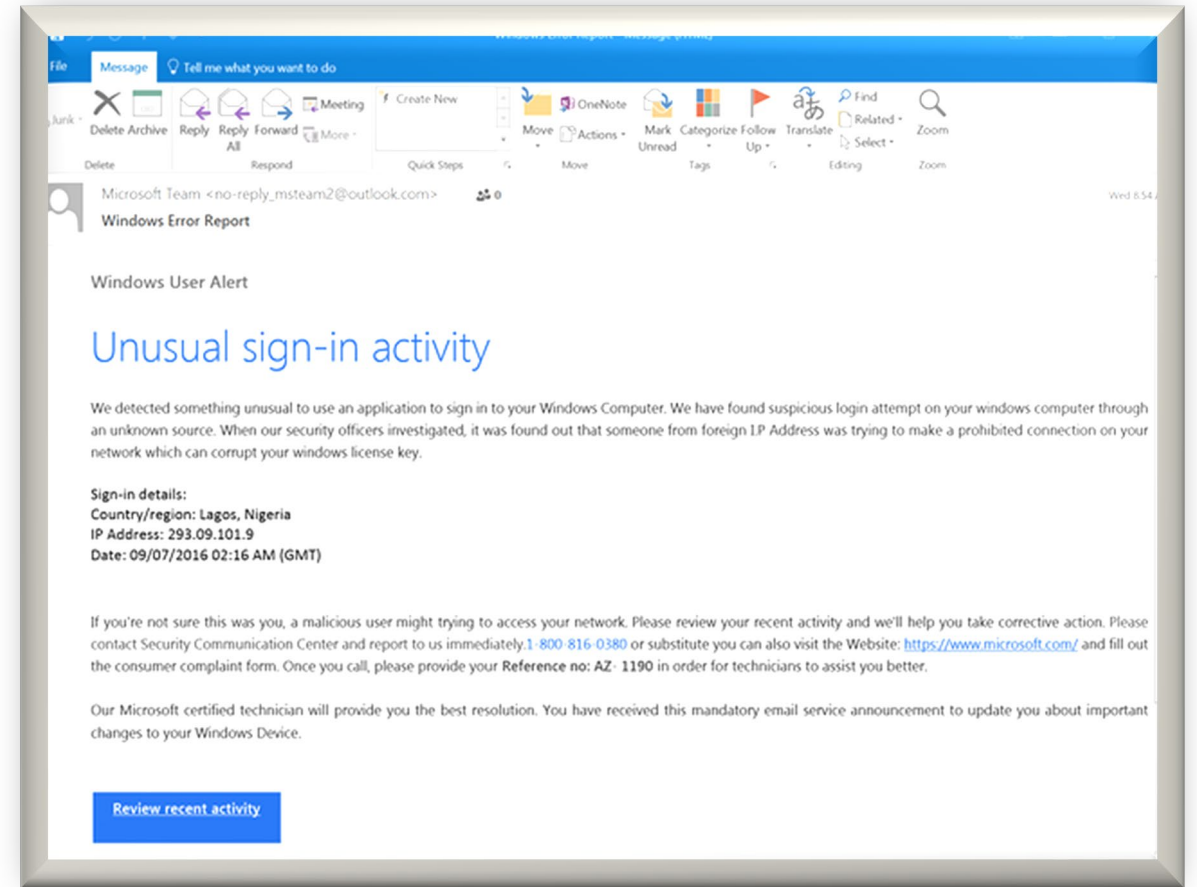
Sell Your Data on the Dark Web

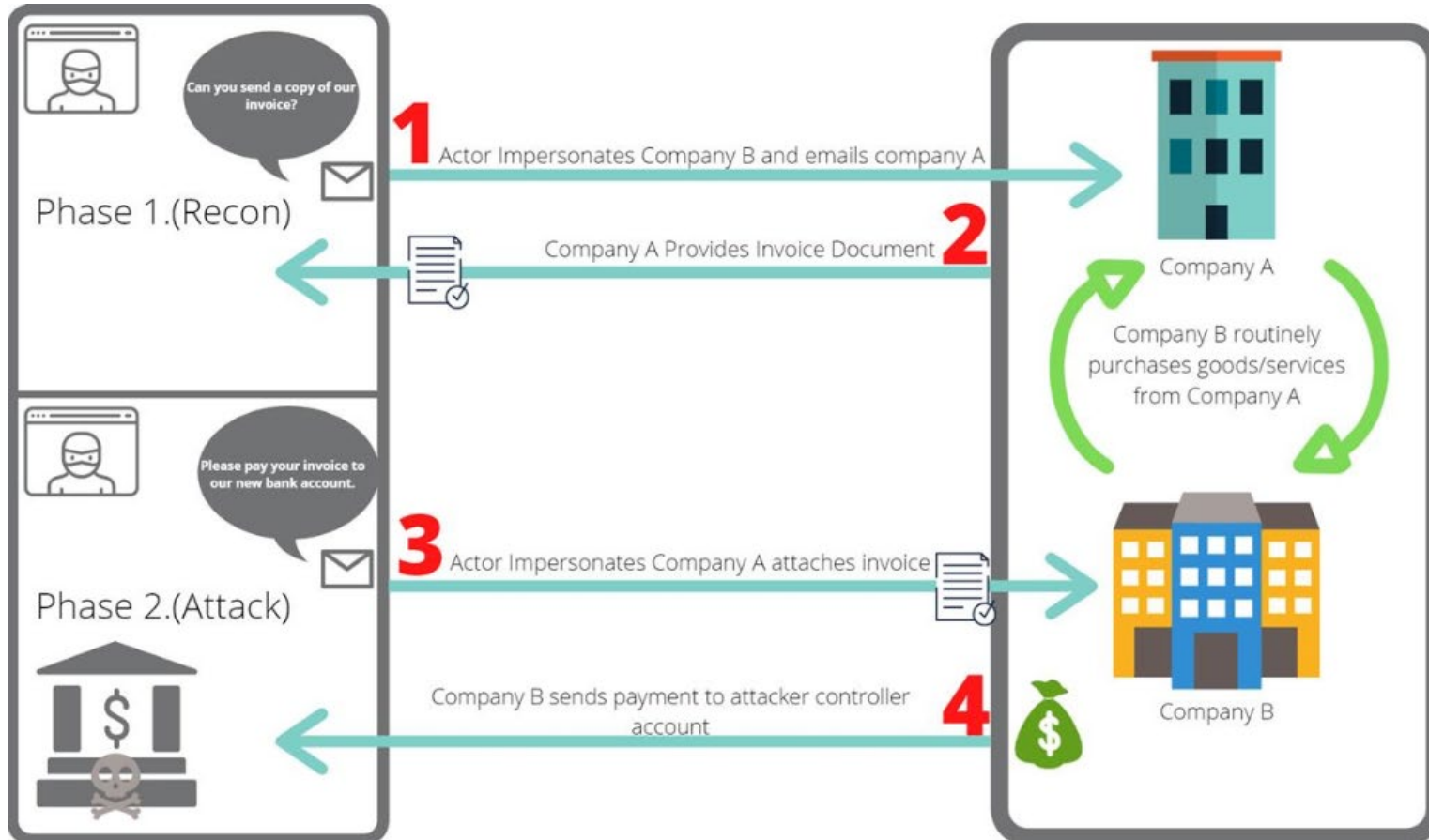
Business E-mail Compromise

Scary Story – Bankrupt Business

20 quotes to 25,000 in one month

- Received carrier site credentials
- Sold all data on dark web
- Remediation costs and fines bankrupt the Business





Invoice Manipulation

Business E-mail Compromise

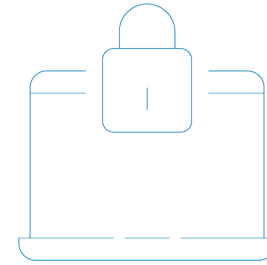
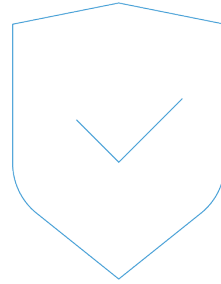


Supply Chain Attacks

“Muling”

**Access to
Bigger Phish**

Cyber Security Myths



Myth 1 – Size of Business Matters

FACT – Small & medium-sized businesses are the *PRIME TARGET*

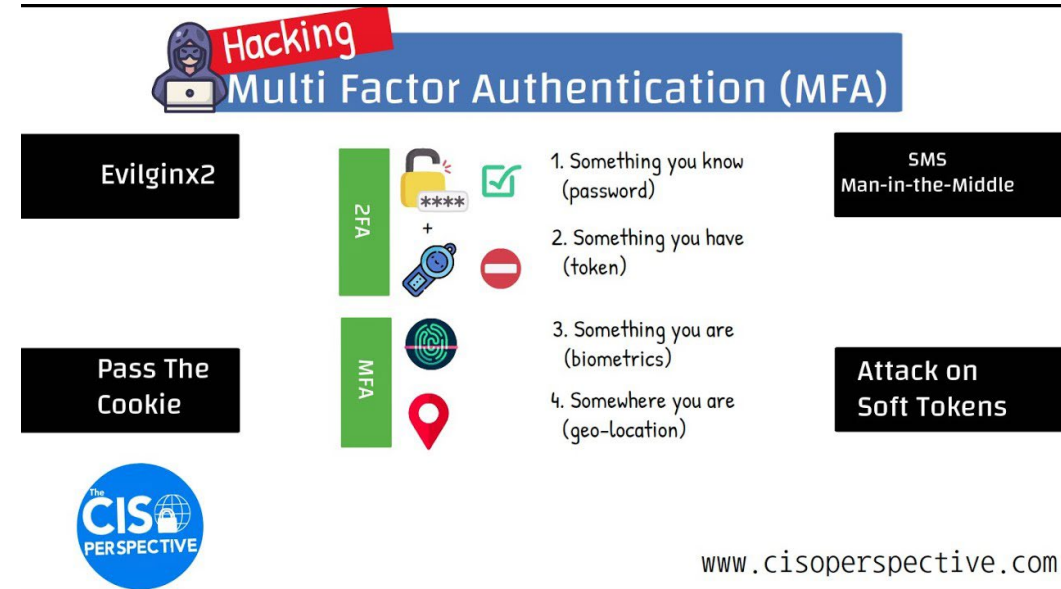
- **Access** to sensitive data
- **Mobility** of the data are how businesses makes money
- **Multiple attacks** are run at once
- **Weak** security infrastructure and expertise
- **“It’s where the money is”**



Myth 2 – MFA and Anti-Virus is Enough

FACT – Cyber crime is 24x7 and complex

- **Advanced Threats** are beyond anti-virus and able to trick users into provide MFA Codes
- **Social Engineering** manipulates users to give up their credentials or pass the data on
- **Insider Threats** allow the attackers around external threat that MFA and Anti-Virus are designed for
- **Zero-Day Exploits** are unknown to vendors and have no patches or fixes



48% of breaches would not have been prevented by Multi-factor authentication

Myth 3 – The Cloud Protects

FACT – moving to the cloud you become increasingly vulnerable to attack.

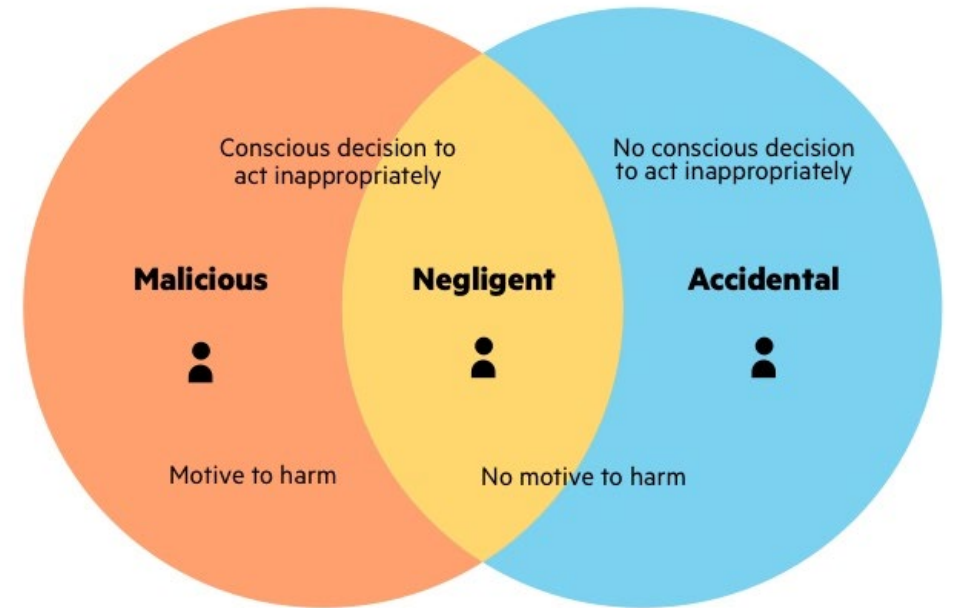
- **Increased Attack Surface** means more entry points
- **Account Compromise** leads right to environment
- **Share responsibility** of provider and customer where business-based app systems have severe gaps
- **Compliance and Legal risks** are focused on cloud requirements



Myth 4 – Cyberattacks are From Outside the Company

FACT – 43% of data breaches are caused by insiders

- **Oblivious insiders** unknowingly cause harm through risky and vulnerable
- **Negligent insiders** create risks by ignoring company
- **Malicious** current or former employees recruited to abuse their access
- **Third-party vendors** misuse their access and compromise the security



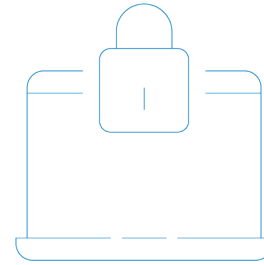
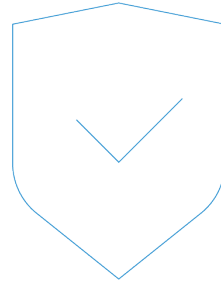
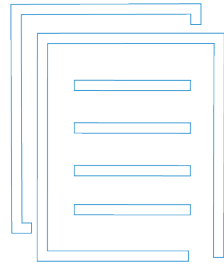
Myth 5 – It is Solely up to IT/MSP

FACT – managing cybersecurity is about risk management and requires a collaborative effort by collaborating IT and Cyber Security

- **Always-On** means share responsibility between IT and Cyber security
- **Risk management** means allocating resources and policies to mitigate
- **Culture and awareness** creates a security conscious workforce that IT is a part of
- **Compliance and legal obligations** are complicated and constantly changing



The Anatomy of an Attack



Reconnaissance



agency owner us



Home



My Network



Jobs



Messaging

No

People ▾

Connections ▾

Locations ▾

Current company ▾

All filters

About 14,000 results



Search with Sales Navigator

12 additional advanced filters



Social Engineering

Reconnaissance

RFP#0019-002-E7362BID.docx.eml  Download  Save to OneDrive

RFP#0019-002-E7362BID.docx



Timothy

To: Timothy

A new RFP Documents file has been shared with you from

[RFP#0019-002-E7362BID.docx](#)

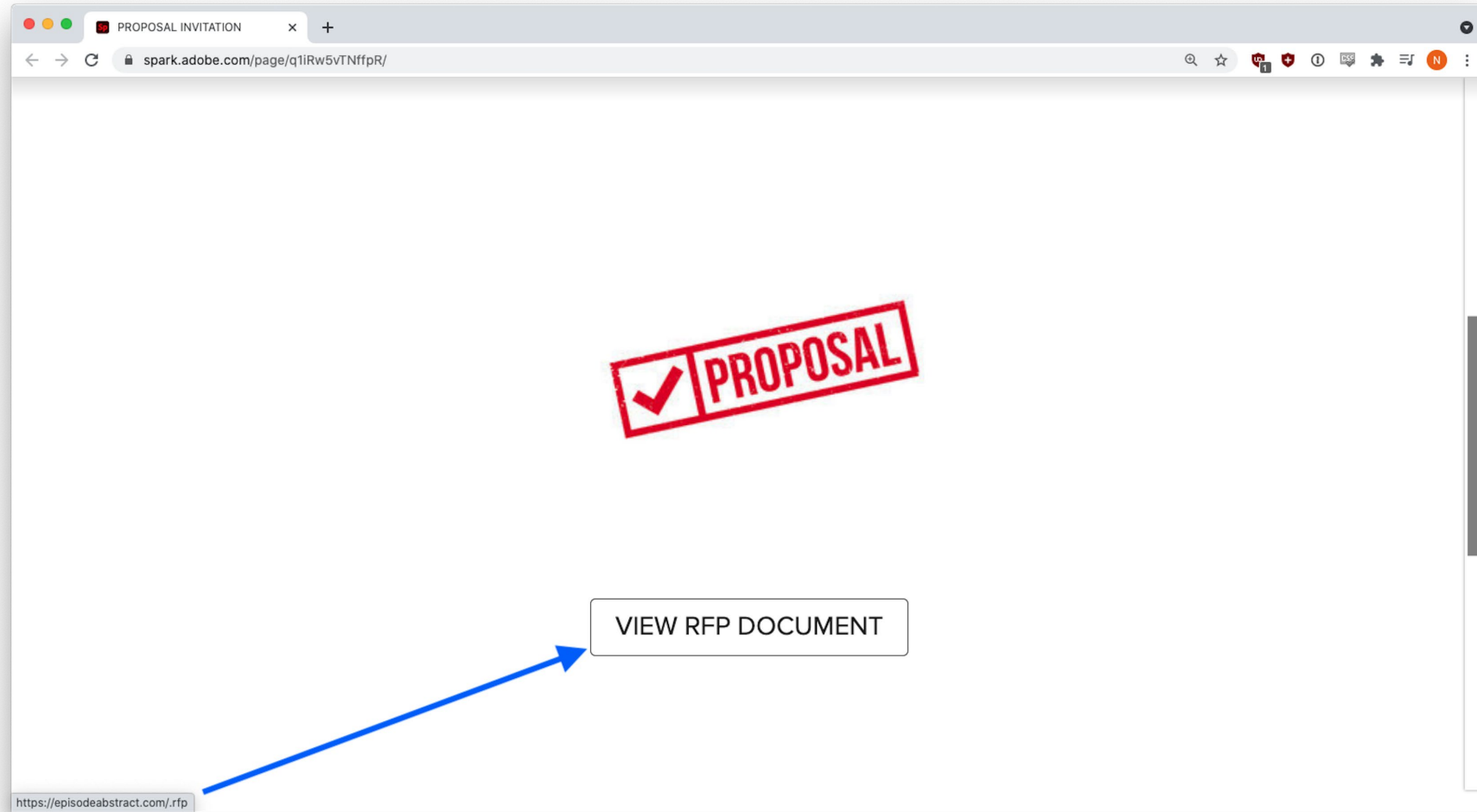
Please study Documents properly for the contract meeting presentation. [Click here](#) to download attachments.

 Reply

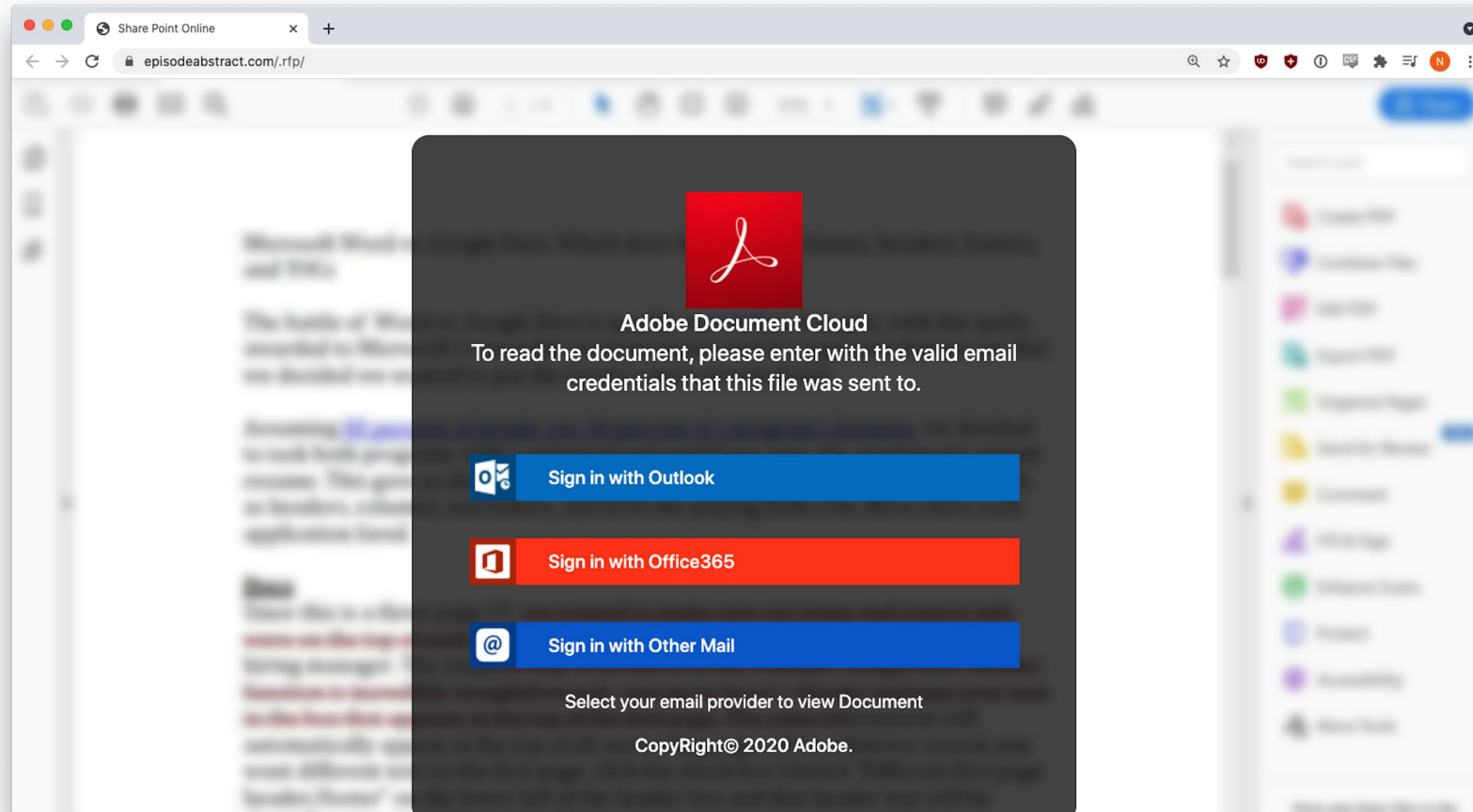
 Forward

Spear Phishing

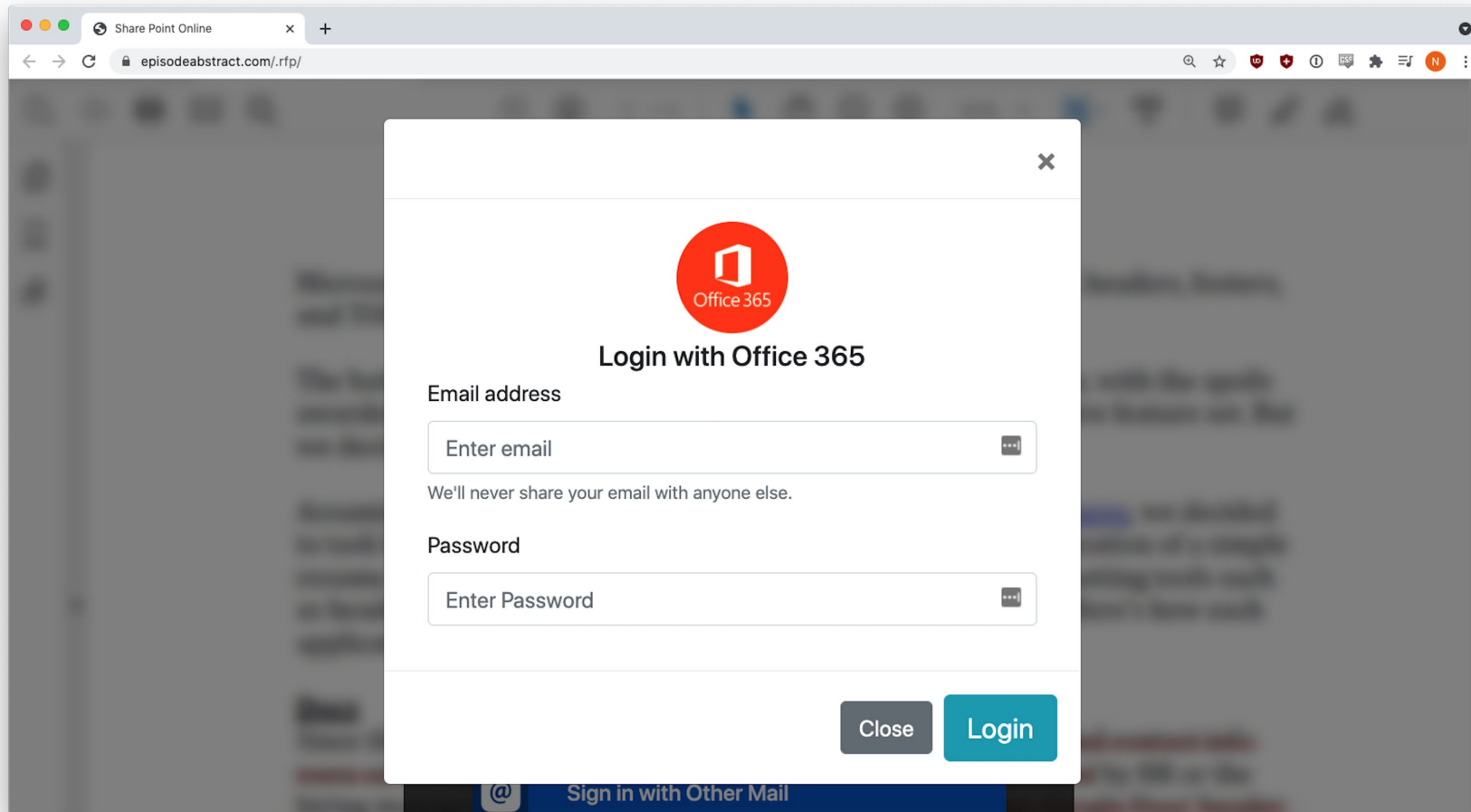
The Trick



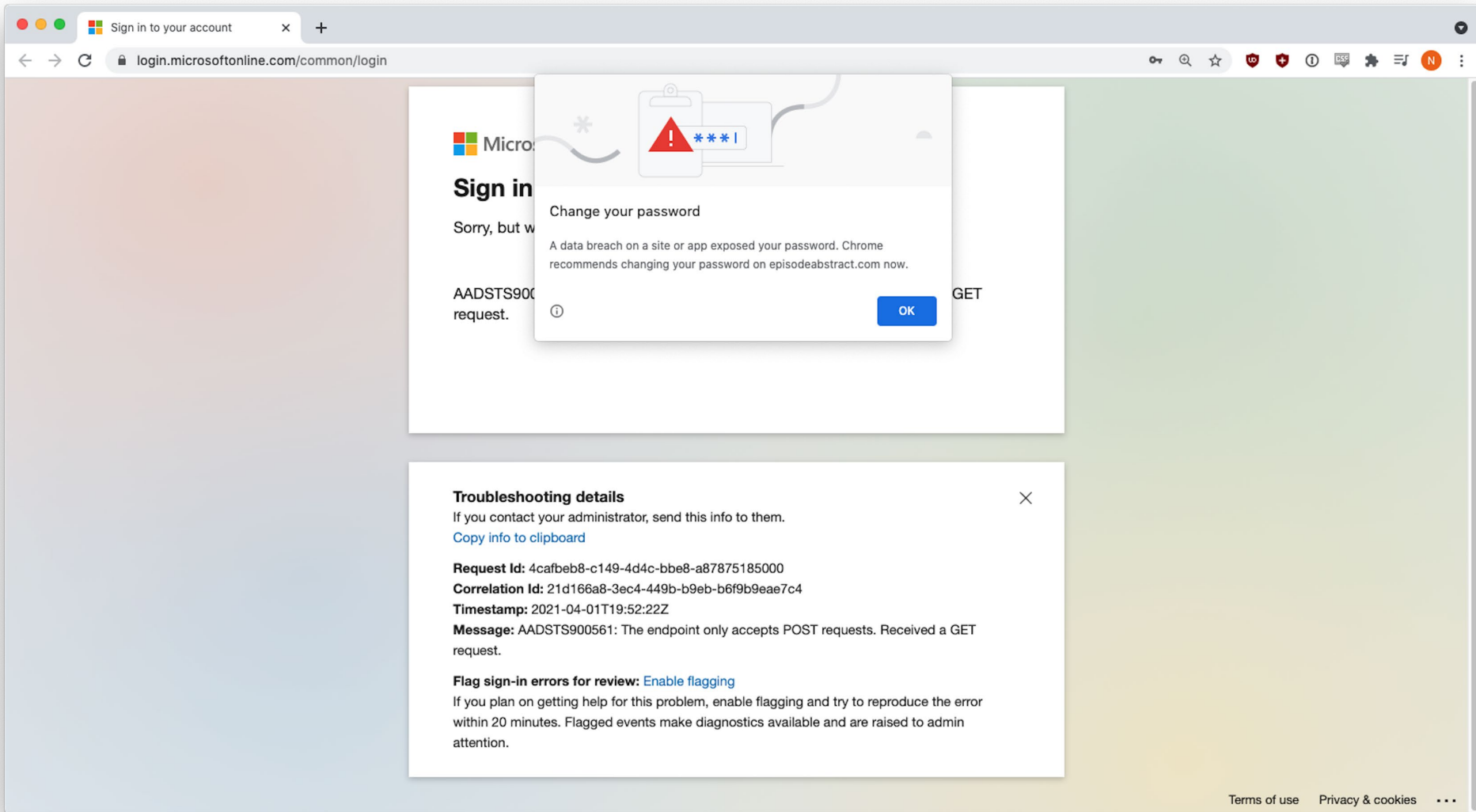
Typo squatting



Credential Harvesting Form

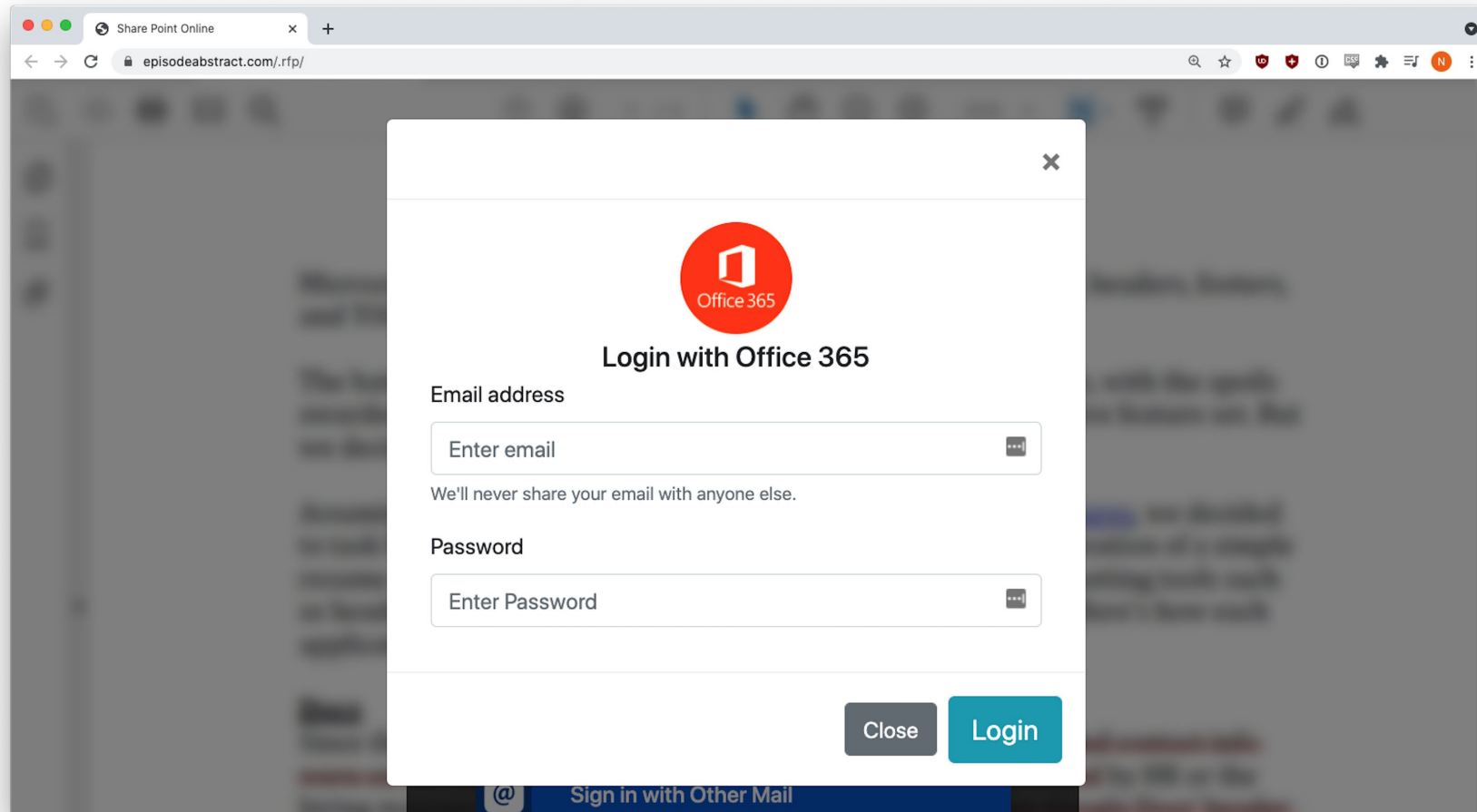


Credential Harvesting Form



Real Microsoft Account

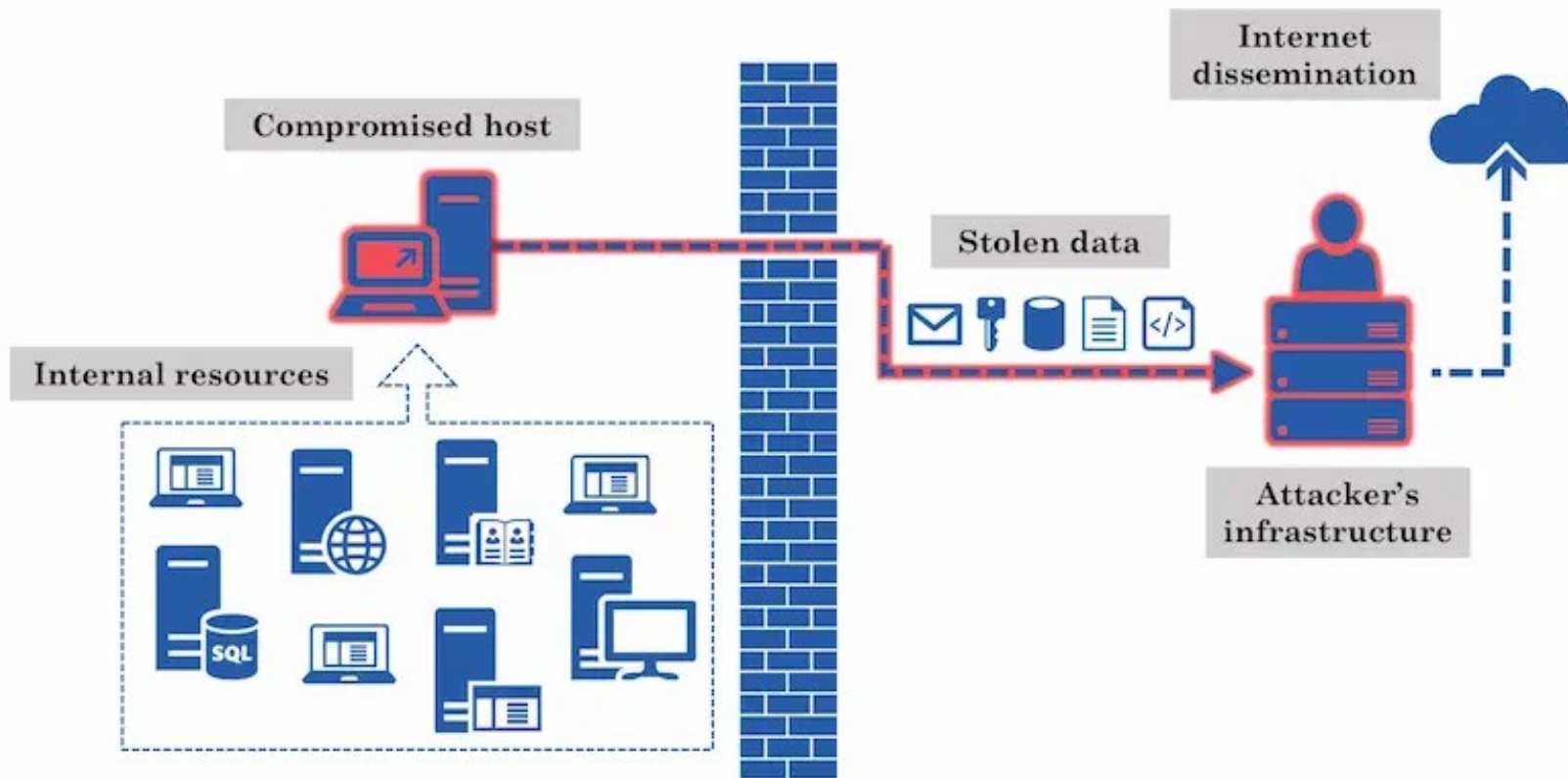
The Trick



The image shows a browser window with a tab titled "Share Point Online" and the URL "episodeabstract.com/.rfp/". A modal dialog box is centered on the screen, featuring the Office 365 logo (a red circle with a white square) and the text "Office 365". Below the logo, the text "Login with Office 365" is displayed. The form contains two input fields: "Email address" with a placeholder "Enter email" and "Password" with a placeholder "Enter Password". A small "x" icon is in the top right corner of the dialog. At the bottom right, there are two buttons: "Close" and "Login". Below the dialog, a link with an @ symbol and the text "Sign in with Other Mail" is partially visible.

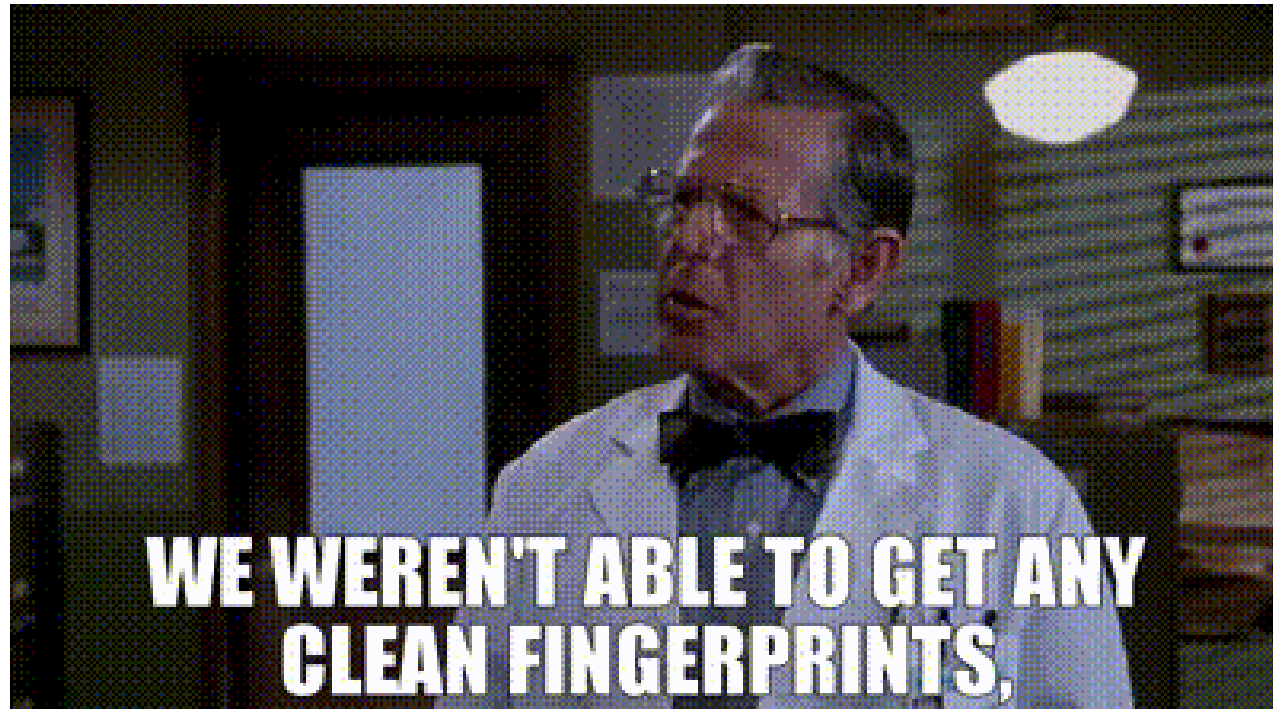
Credential Harvesting Form

Exfiltration Of Data



Attacker's Infrastructure

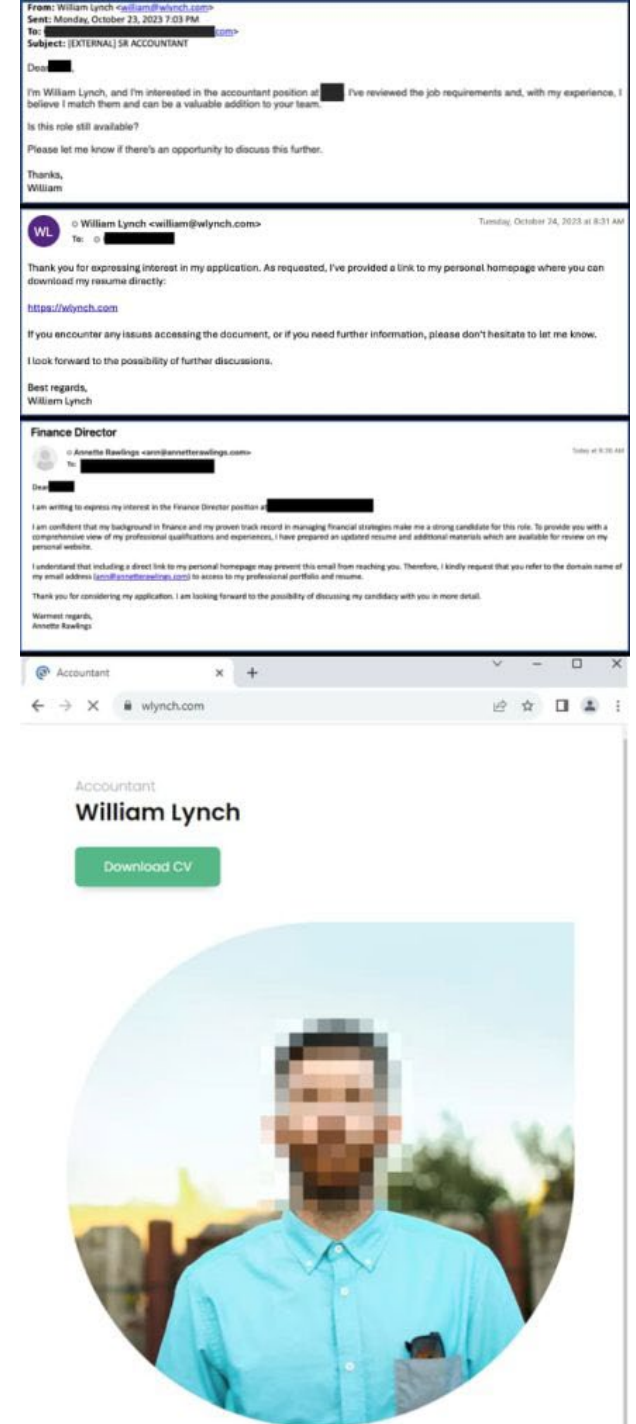
Sanitation



No visible tracks and leave a back door

Scary Story – Bad Actors Appearing as Candidate

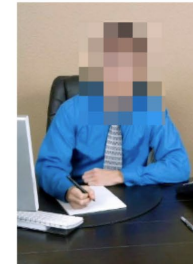
- Direct e-mails expressing interest in open job and when recipient replies the attack chain begins
- Threat actors are applying to existing jobs on LinkedIn with a embedded Malicious URL
- Threat actors are using e-mail and personal “resume websites” to run an attack



Scary Story – Contagious Interview and Wagemoles

North Korea is posing as job seekers and employers

- Contagious Interview -Threat actors pose as employers to lure software devs into installing malware during the interview process to steal cryptocurrency through their machines
- Wagemole - Threat actors seek employment with US organizations for financial gain and espionage to funnel wages for weapons programs



BLOCKCHAIN & PYTHON & CHATBOT ENGINEER

Profile

Passionate Full Stack & Blockchain Developer offering 8+ years of relevant experience in Blockchain, ML and Robotic.

I have experience developing DeFi, DEX, DApp, Trading Bot, Token, autonomous systems and artificial intelligence. I am fluent in Solidity, Web3.js, Python and JavaScript ,and have worked on a variety of projects as a consultant, helping clients achieve their goals. I am also keen on several JavaScript and Python web frameworks like Vue, React, Django and Flask

I am a life-long learner and is looking forward to working on exciting and challenging projects. I am continuously trying to improve, learn more and gain new experiences.

With a strong attention to detail and accuracy and the important ability to function well in a team setting.

Looking for a Blockchain Developer job within a forward-moving company.

Details

Phone: +140
Email: @gmail.com
Telegram: @s
Discord: N 7

<https://www.linkedin.com/in/>
7777
<https://github.com/Kin>

Skills

Fast Learner

Hard worker

Computer Skills

Team Player

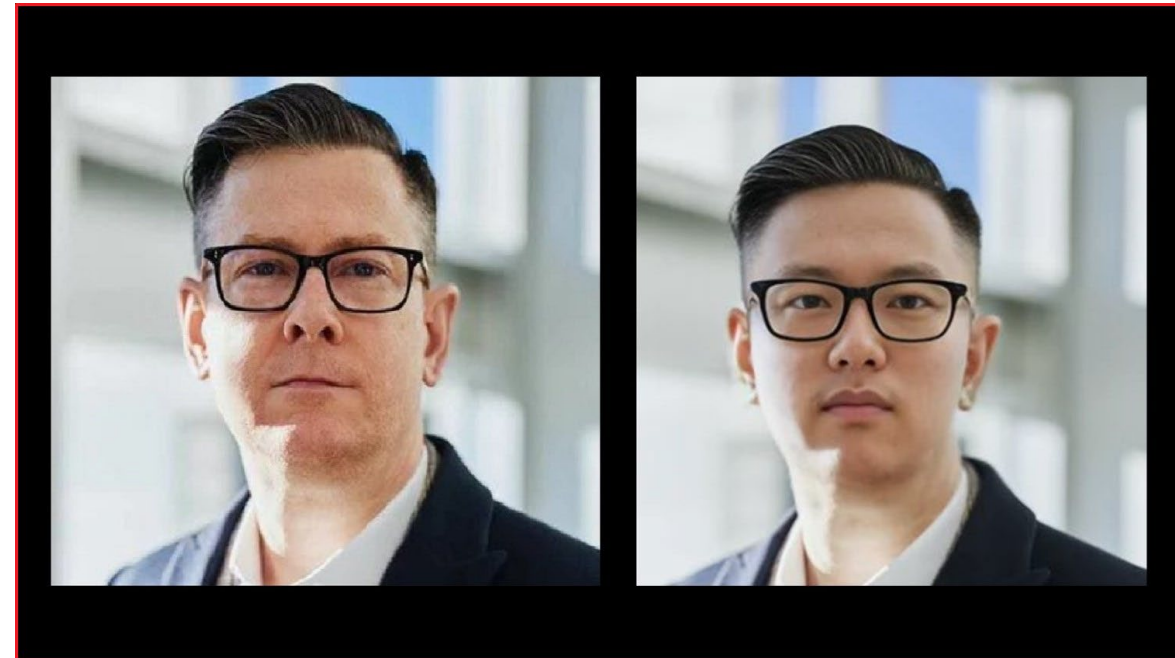
Excellent Communication Skills

Leadership and Teamwork

Scary Story – Deep Fake Gets Into Security Company

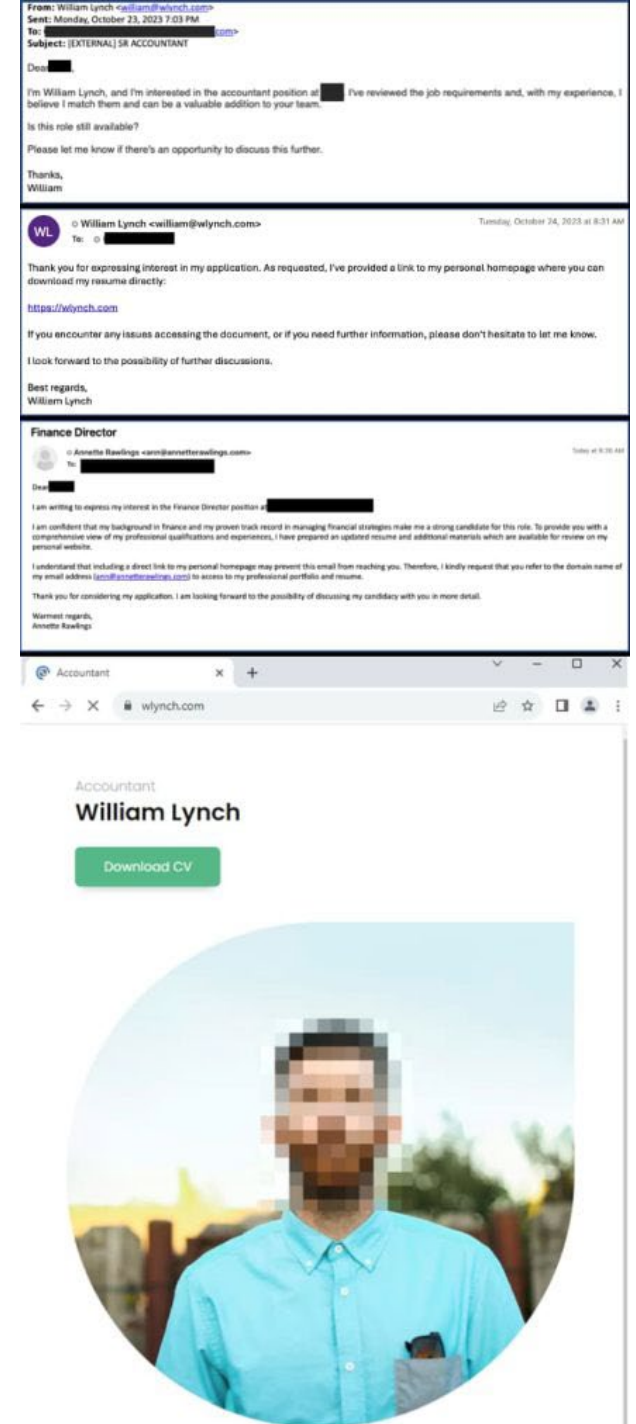
North Korea uses AI deepfake to get into KnowBe4

- 4 interviews were carried out
- Sent a Mac computer to the remote worker where the threat actor downloaded malware.

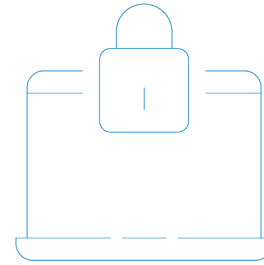
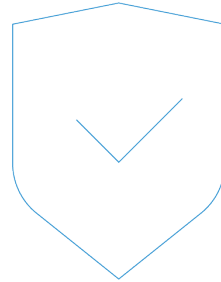
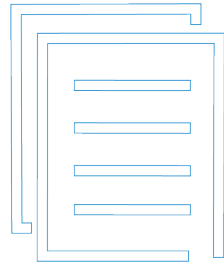


Scary Story – Bad Actors Appearing as Candidate

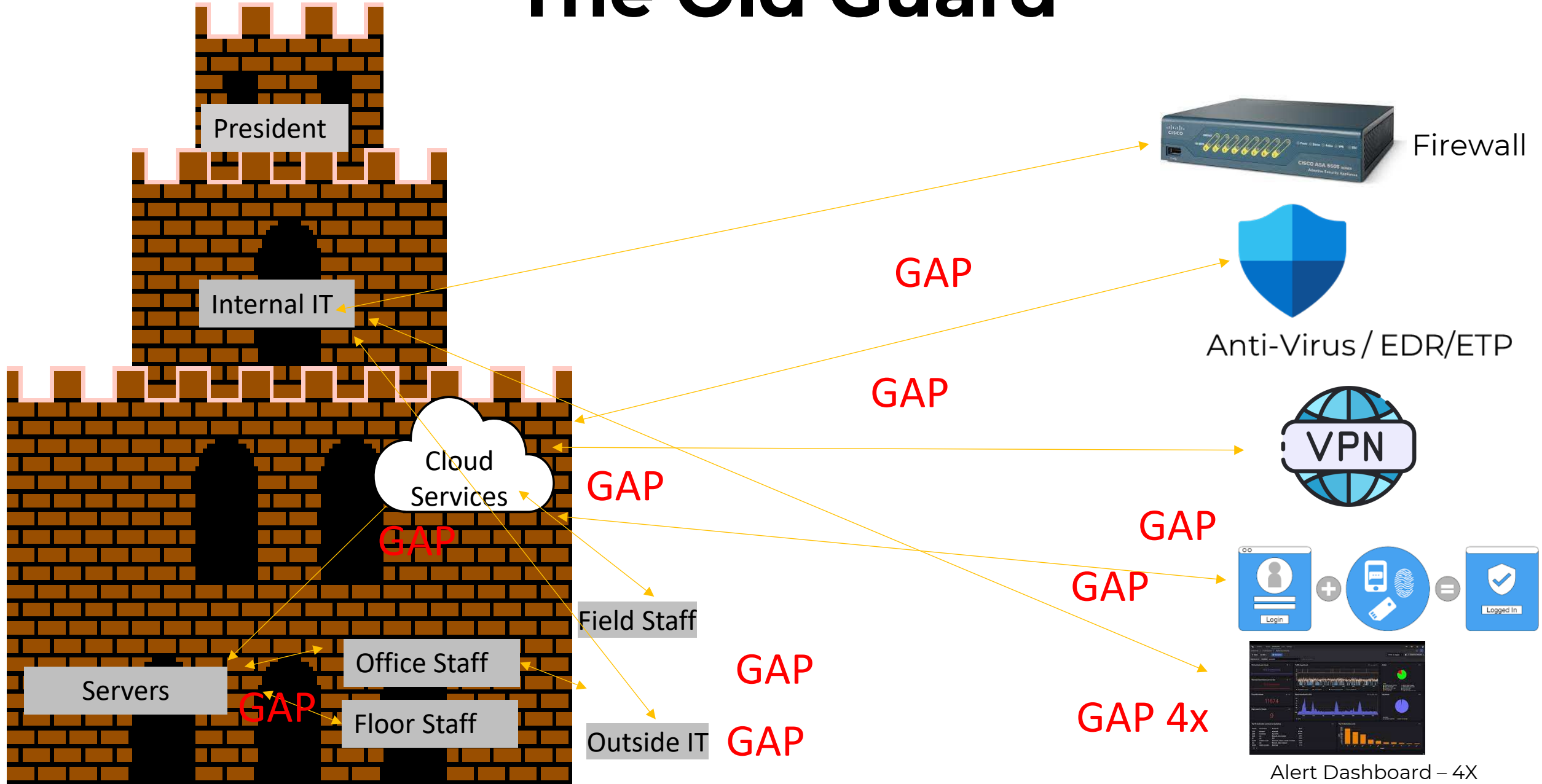
- Direct e-mails expressing interest in open job and when recipient replies the attack chain begins
- Threat actors are applying to existing jobs on LinkedIn with a embedded Malicious URL
- Threat actors are using e-mail and personal “resume websites” to run an attack



Cyber Security Tips



The Old Guard



Eliminate the Gaps in Your Cyber Security

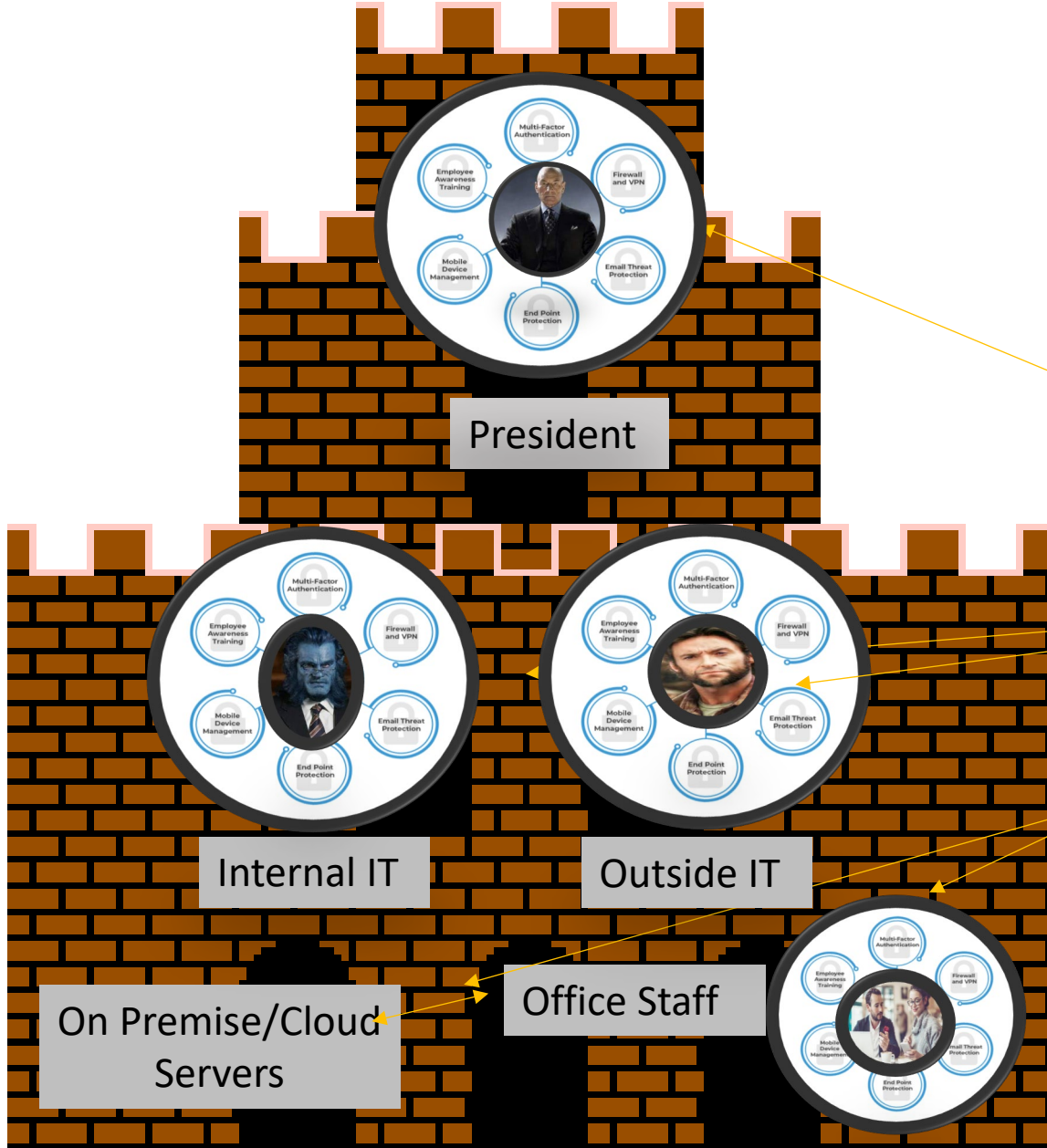


- A multi-layered user-based security approach
- All-in-one cyber security management software plus 24x7 SOC & SIEM plus threat hunting
- Comprehensive “Stand Alone” Cyber Liability Insurance



The New Guard

Managed Layered Security by User



Security Operations Center (SOC)



Security Information & Event Management (SIEM)

24 x 7 x 365

Create and require complex passwords With Multi-Factor Authentication

- 14+ characters
- Numbers, Upper and Lower Case
- Add Two Factor to e-mail, cloud and remote access

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Tip #1 – Don't Underestimate Cyber Criminals

FACT – Looking less attractive to criminals lowers their R.O.I.

- **Password** lengths, complexity and two factor slow the bad guy down to maybe move on
- **Off-domain back ups** create the ability to recover data quickly reducing extortion demands
- **Monitor your network regularly** for updates and patches closes outside vulnerabilities



Back up
your data



Practice password
hygiene



Monitor your
network regularly



Enable two-factor
authentication

Tip #2 – Separate Business & Personal

FACT – Bad guys are looking for hybrid users vulnerabilities more than in office

- **Business only devices** both in the office and out of it
- **Home office security** as an extension of the field office lowers the attack surface in both places
- **Business only e-mail boxes and log-ins** eliminates known vulnerabilities of free products and allows for security software install – **eliminate @gmail, @yahoo, @outlook, @live, @aol, @myspace addresses**



Tip #3 – Mind the Gaps

FACT –A layered security approach by end user lowers your attack surface

- **Prevents** all kind of attacks not just external attacks
- **Protects your cloud/virtual** environment by treating it like a on-premise environment
- **Trusts No One** inside your organization with security protocols inside the company too
- **24 x 7 monitoring and remediation** reduces the time and impact of an attack



Cyber Insurance – Current Market Conditions

- Expanding capacity and growing risk appetite
- Large influx is Insurtech's that are well funded
- Reductions in premiums ranging from 10% to 25%
- Risk Management Scans
- Embedded Managed Detection and Response offerings (MDR)

“What If” my temporary contributes to an attack of my client’s system (Silent Cyber)

- Temporary Firms cyber liability coverage will likely only cover liability arising out of an attack on their system – not clients.
- Temporary Firms Professional and General Liability Policy may or likely will have Cyber Exclusions precluding coverage.
- Alternative Solution: Secure a cyber umbrella policy with difference in conditions coverage provided

CYBERUP

- Example of a modern Cyber Umbrella Policy
- Protects insured's against "Silent Cyber" incidents.
- True Umbrella coverage with full drop - down capabilities
- Would likely respond and provide coverage where a temporary employee contributes to a cyber attack on a temporary firm's client system.



Thank you



Edward Foley

Senior Vice President, Risk Management
Summit Financial Group

efoley@yoursummit.com



Daniel Metcalf

Managing Partner and Co-Founder
Cyberfin

dm@cyberfin.net



Michael O'Brien

Executive Vice President
Amwins Insurance Brokerage

Michael.obrien@amwins.com

ASA Certification Continuing Education

Today's webinar qualifies for 1.0 CE hour

- **Live webinar:** **NEW as of April 2024**—CE credits earned from attending this program are *automatically* added to your online CE Status within three business days.
- **On-demand viewers:** Submit this earned CE using the online submission form at *americanstaffing.net*.

- This program is valid for **PDCs** for the SHRM-CP® or SHRM-SCP®.

Activity ID: 24-2DGDQ



USE PROMO CODE:

“40WEBPS”



ASA Staffing Pro StacksSM

americanstaffing.net/pro-stacks





**You will now be redirected
to a brief survey**