



# Securing your library data

Wes Osborn

Central Library Consortium (Ohio)

# Agenda



WHY?



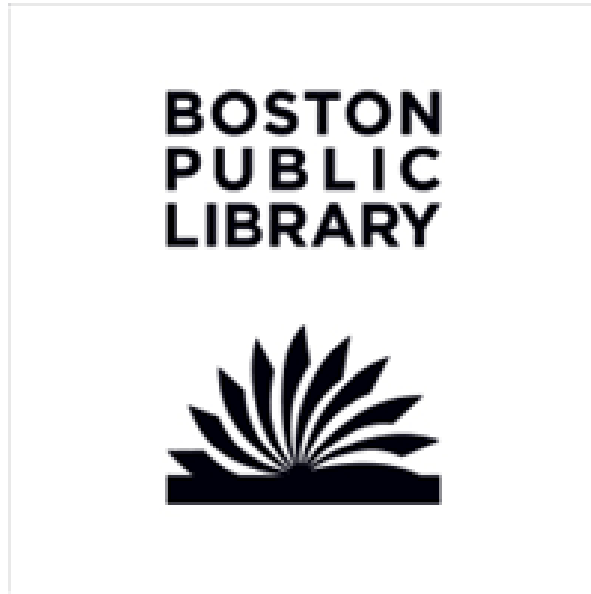
NON-TECHNICAL  
APPROACH



TECHNICAL APPROACH

# Hacking Victims since 2024

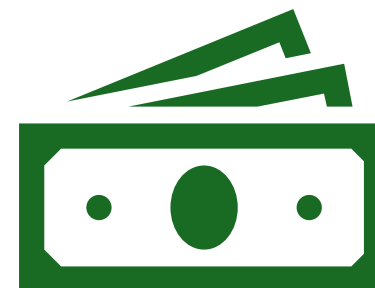
---



# There ARE Financial motives



“Libraries don’t have any money!”



But.. Attackers are hoping for an insurance payout

# Results of an attack

Systems are disabled through  
by scrambling  
the data.

Attackers will  
unscramble the  
data **for a fee.**

# Required by law



## OHIO LAWS & ADMINISTRATIVE RULES

LEGISLATIVE SERVICE COMMISSION

[HOME](#)[LAWS](#)[ABOUT](#)[CONTACT](#)[RELATED SITES](#)[GO TO](#)[Go](#)[Keyword Search](#)

(F) Develop procedures for purposes of monitoring the accuracy, relevance, timeliness, and completeness of the personal information in this system in accordance with the procedures, maintain the personal information in the system with the accuracy, relevance, timeliness, and completeness thereof, and assure fairness in any determination made with respect to a person on the basis of the information;

(G) Take reasonable precautions to protect personal information in the system from unauthorized modification, destruction, use, or disclosure;

# Avoiding the frontpage

## 77% of CISOs fear next big breach will get them fired

News Analysis

28 Oct 2024 • 3 mins

CSO and CISO

Data Breach

Incident Response

Increased pressures are putting CISOs in the hot seat, but should they bear all the blame when the inevitable comes?

**GeekWire**

NEWS ▾

JOB

EVENTS ▾

LISTS ▾

MEMBERS ▾

STUDIOS ▾

All tech-enabled systems and services are back up and running at Seattle Public Library this week, roughly three months after a ransomware attack partially crippled the institution and its 27 branches across the city. And cybersecurity experts are praising some of the steps taken to protect against future attacks.

# Required for insurance




## 5 ways to meet cyber coverage requirements (and reduce risk)

---

Insurance companies typically look for five essential cyber insurance requirements before insurance coverage. Chances are that your clients lack these security controls across their infrastructure. In that case, the following security controls can reduce the likelihood and impact while helping to qualify the business for coverage.

### 1. Multi-factor authentication

[Multi-factor authentication \(MFA\)](#), also known as two-factor authentication, is one of the

The background is a blurred photograph of a library interior. On the left, there are wooden bookshelves filled with books. The right side of the image shows a bright, out-of-focus area with warm, golden light, possibly from a window or a lamp, creating a bokeh effect. The overall tone is warm and scholarly.

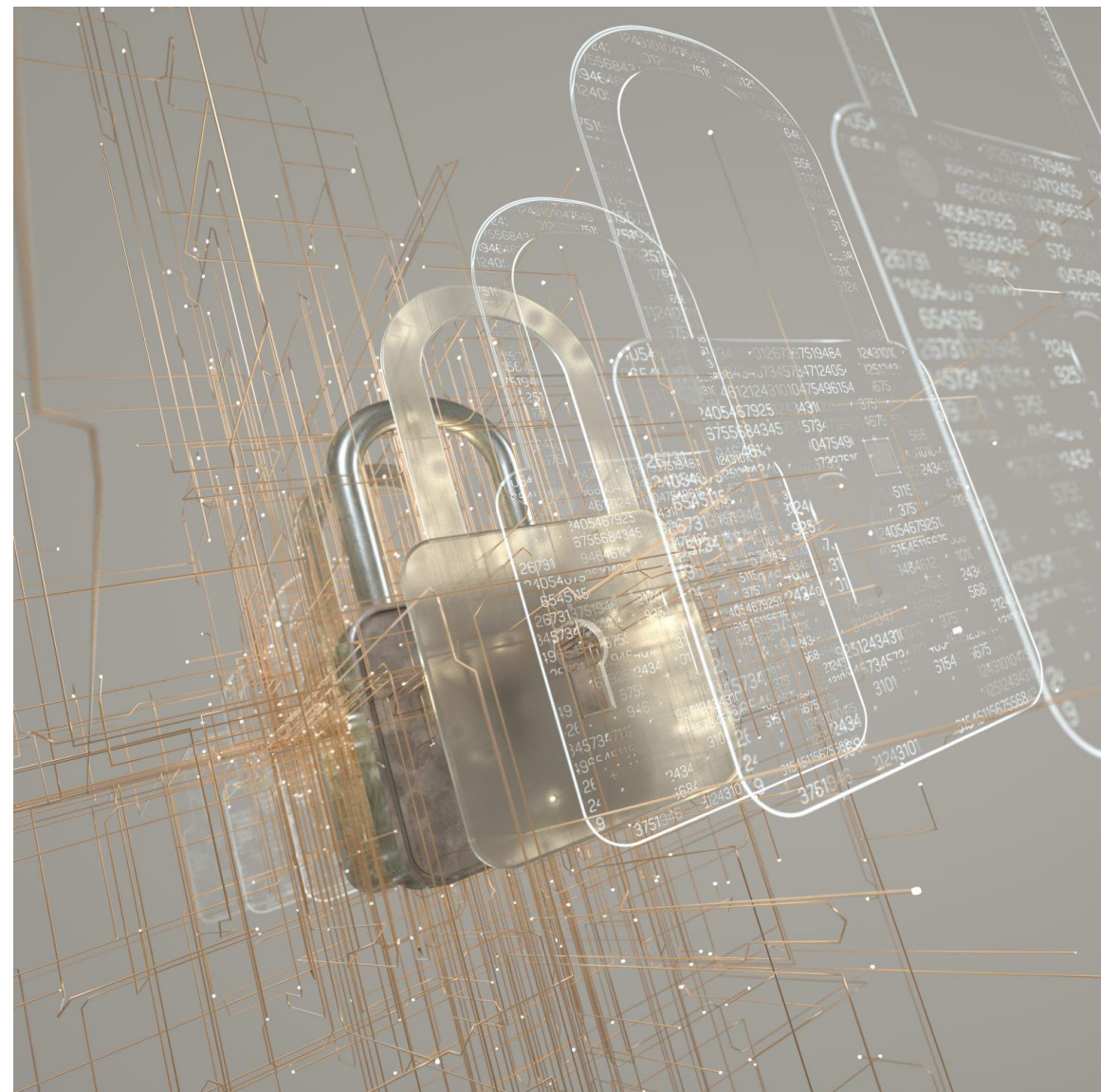
Libraries have a history of  
taking privacy seriously

For data to be  
private, it must  
be secure

There is a strong link  
between the two



# Non-technical security approaches



# Central Library Consortium Security Policy (and related documents)

Knowledge Base clc-policy



Security Policy and its related documents, persons and companies with access to CPI data generated or stored by CLC shall be known as Applicable Individuals.

## Overview

Applicable Individuals will protect CPI data contained within CLC's systems from unauthorized disclosure, modification or destruction, whether accidental or intentional. The CLC and its member libraries will comply with this policy and the Ohio Revised Code Chapter 1347 regarding the duties of state and local agencies for maintaining personal information systems.

In addition to the requirements outlined in this policy, libraries that accept credit cards, will comply with the latest Payment Card Industry Data Security Standard within the Cardholder Data Environment.

The most current version of this policy and any related rules or procedures are available on the CLC Knowledge Base site or upon request from the CLC office (ORC 1347.05 ¶B).

## Practice

As defined in ORC 1347.01 ¶H, the libraries of the CLC constitute a combined system in order to enable collaboration. CPI data within the combined system will be accessed, handled, shared and disposed of as described in the [CLC Security Practice Rules](#) ORC 1347.15 ¶A (1). The CLC will maintain a [CLC Incident Response Plan](#) <sup>4</sup> in case of any unauthorized disclosure of CPI data (ORC 1347.12). Each individual library may augment these rules with locally specific rules of their own. Libraries must include disciplinary measures for unauthorized use or disclosure of CPI data (ORC 1347.05 ¶D).

# CLC Security Guideline Updates



Used ChatGPT to improve & shorten it



Included vendor personally identifiable information (PII) sources



Entire packet available for download:  
<https://go.clcoho.org/security24>

# Contract monitoring

---



Audit their security practices (e.g., SOC 2, ISO 27001 certifications).



Look for mentions of encryption, and access controls.



Define how the service provider can use your data.



How long they will retain your data after service termination.

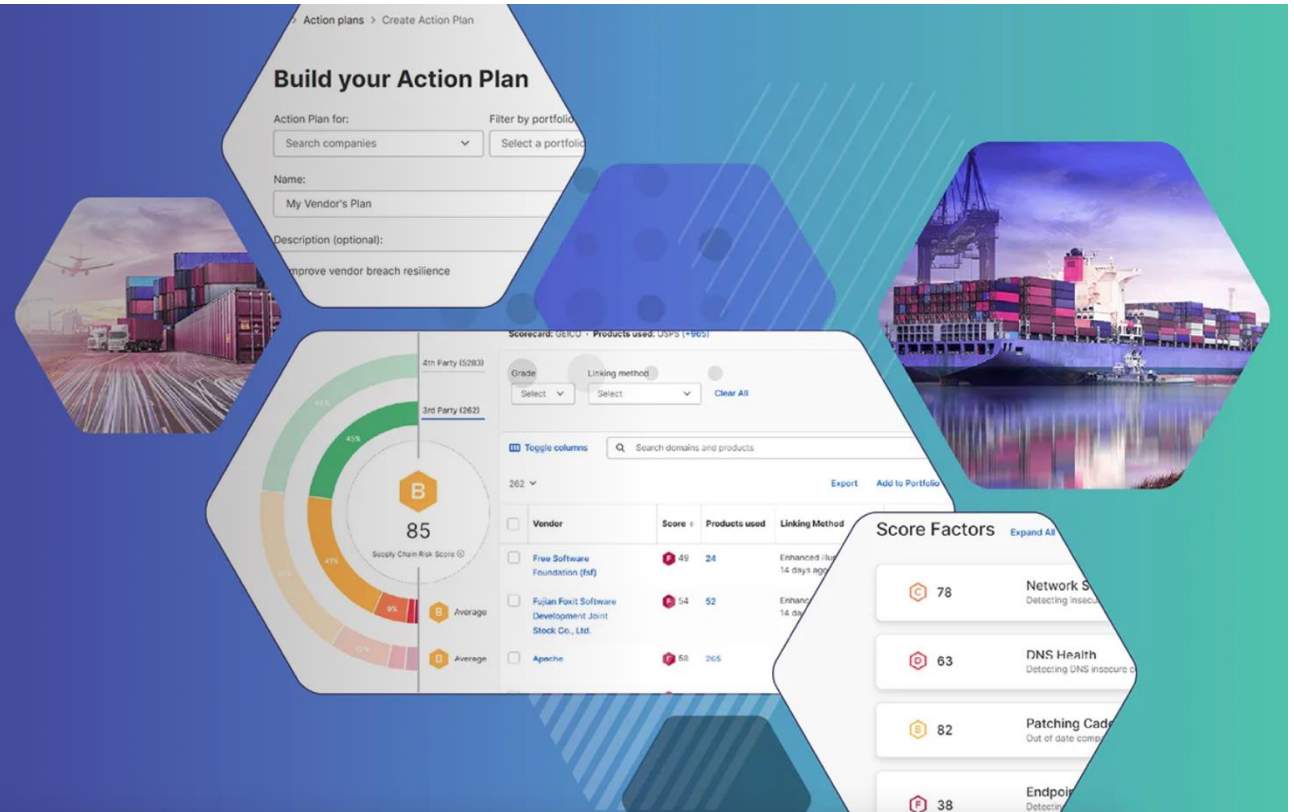
# 3<sup>rd</sup> party monitoring services - SecurityScorecard

Solutions ▶ Supply Chain Risk Management

## Secure the public sector supply chain

Illuminate risk within your supply chain and prevent third-party security breaches while keeping data, infrastructure, and the public safe

[Get a Demo >>](#)





How can we  
protect  
ourselves?

---



# Email IS the #1 attack method

---

At least 70%+ of hacks  
start via email

# Welcome back 🖐️

Log in to your account

Email / Username

wesochuck

[Skip the password; email me a login link](#)

Sign On to **Online Banking** or [select another service](#) ▼

User ID (required)

Enter User ID

Password (required)

Enter Password

☐ Remember User ID

[Forgot ID or Password?](#)

---

Don't be fooled by  
*urgent* messages

---

# Examples of false urgency

---

You will lose your account,  
unless...

---

You will be charged...

---

You have 24 hours to...

---

Someone is in jail

---



+63 948 697 1465 >

iMessage  
Tue, Mar 4 at 3:28 PM

The Toll Roads Notice of Toll Evasion: You have an unpaid toll bill on your account. To avoid late fees, pay within 12 hours or the late fees will be increased and reported to the DMV.

<https://ohioturnpike.org-ticketrxw.xin/vip>

(Please reply Y, then exit the text message and open it again to activate the link, or copy the link to your Safari browser and open it)

The Toll Roads team wishes you a great day!

The sender is not in your contact list.

[Report Junk](#)

What to  
do?

Text

Text someone  
using contact

Call

Call someone  
using contact

Email

Emailing is OK...  
just don't hit reply

# Why no reply? Which address is real?

- WOSBORN@C1COHIO.ORG
- WOSBORN@C1COHIO.ORG

# Why no reply? Which address is real?

- wosborn@apple.com
- wosborn@apple.com



Type in sensitive information  
(or use a password manager)



What should I do if I've **clicked** on an email link?

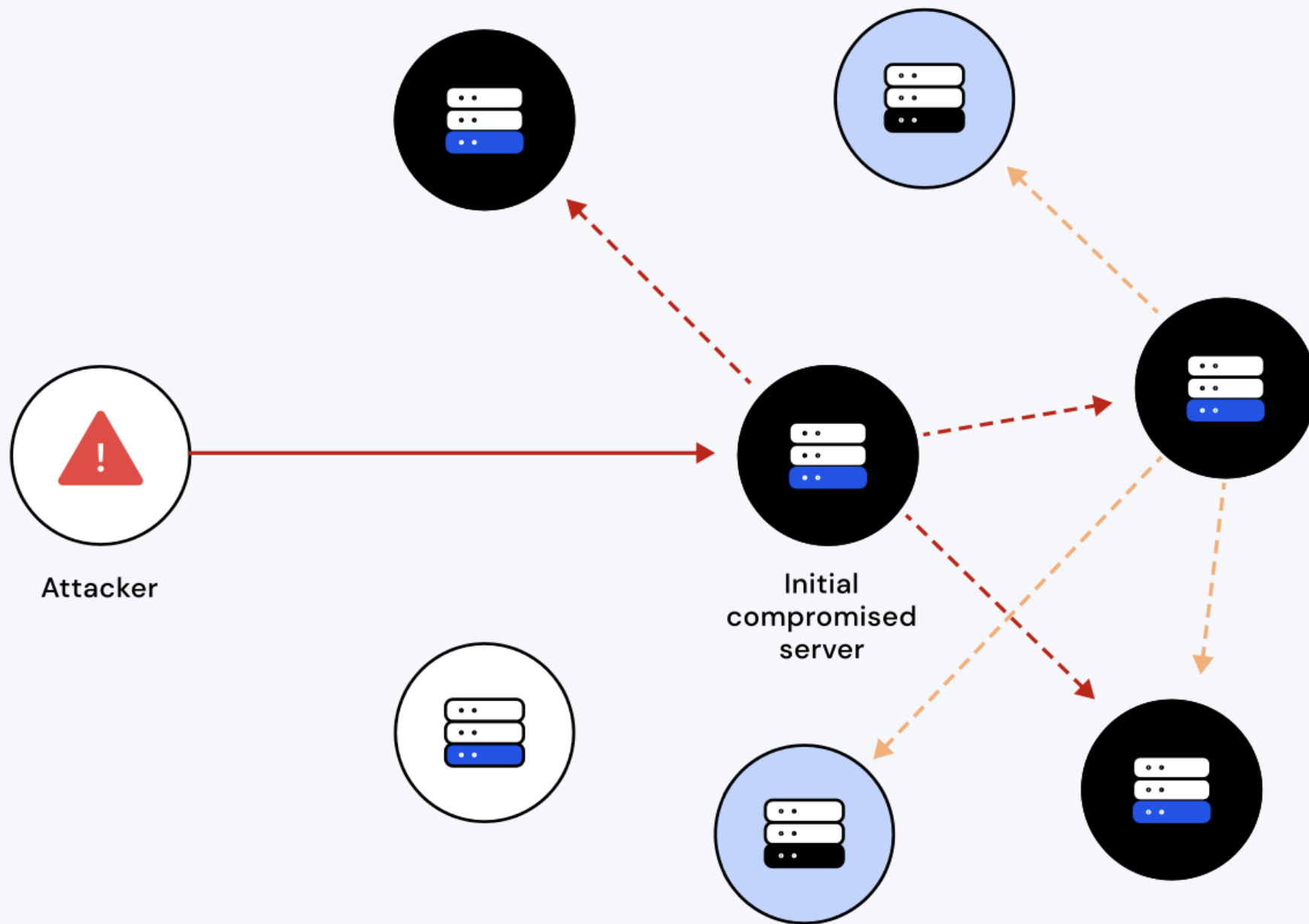
---

If all you did is click & you're on a modern patched device, you're fine

If you entered a password, other data, ran a file, or suspect something is wrong with your computer – **THEN PANIC & turn it off!**

Isn't turning off the  
computer a bit extreme







If you suspect your  
computer is  
compromised –  
turn it off

# Enable Multi-Factor Authentication (MFA)

MFA = in addition to knowing something (password) you must **have** something (phone, token, etc.) to access your account

---

Our findings reveal that MFA implementation offers outstanding protection, with over 99.99% of MFA-enabled accounts remaining secure during the investigation period.

*–Microsoft Study, May 2023*

Auto refresh : **Off**

Detection time : **Last 1 month**

Show dates as : **Local**

Risk state : **2 selected**

Detection type : **None Selected**

Risk level : **High, Medium**

+ Add filters

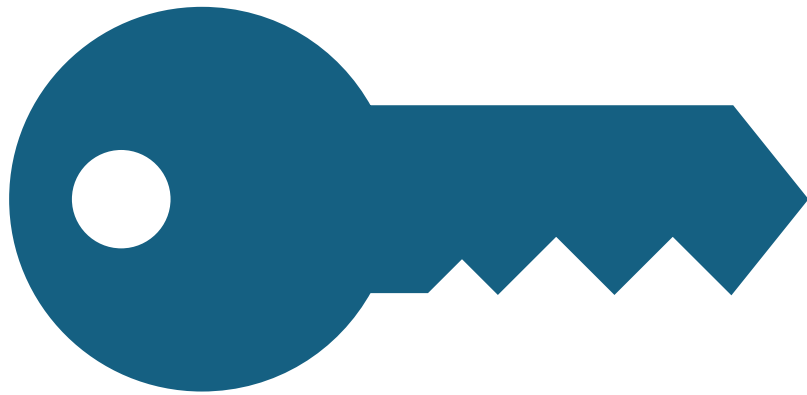
### User detections

Detection time ↑↓	User ↑↓	IP address ↑↓	Location	Detection type ↑↓	Risk state ↑
10/9/2024, 4:29:42 PM	John Doe	92.119.36.23	Buckeye, Arizona, US	Atypical travel	At risk
10/15/2024, 2:40:15 PM	Jane Smith	185.174.100.20	Los Angeles, California, US	Unfamiliar sign-in pro...	At risk
10/9/2024, 11:28:56 AM	John Doe	102.88.36.187	Lagos, Lagos, NG	Anomalous token	At risk
10/9/2024, 8:47:56 AM	John Doe	92.119.36.23	Buckeye, Arizona, US	Unfamiliar sign-in pro...	At risk
10/8/2024, 11:30:30 AM	John Doe	216.131.87.22	Miami, Florida, US	Anomalous token	At risk
10/7/2024, 3:35:24 PM	John Doe	162.253.68.218	Orange, California, US	Anomalous token	At risk
10/3/2024, 3:40:33 AM	John Doe	173.93.232.211	Pawleys Island, South ...	Anomalous token	At risk
9/29/2024, 4:31:17 PM	John Doe	64.31.13.148	Dallas, Texas, US	Unfamiliar sign-in pro...	At risk

Login  
attempts are  
always being  
made  
because  
email is so  
valuable

"Fidelity Investments: **If anyone asks for this code, STOP. It's a SCAM.** Our reps will NEVER ask for it. Only enter it online."

Take this seriously, NEVER give out SMS codes to anyone else. This is a common Facebook Marketplace "scam".



Don't reuse vendor  
passwords & API keys





# Dangers of vendors reusing credentials

If you change it  
for one vendor,  
then all vendors  
must update.

Makes it more  
difficult to track  
down potential  
abuse.

---



Time to play a game!  
Real or fake?

## Microsoft account password change

Inbox x



**Support** <support@msupdate.net>  
to me ▾

4:09 PM (26 minutes ago)



Microsoft account

# Your password changed

Your password for the Microsoft account [ethan@hooksecurity.co](mailto:ethan@hooksecurity.co) was changed.

If this was you, then you can safely ignore this email.

Security info used:

Country/region: United States

Platform: iOS

Browser: Safari

IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:

1. [Reset your password.](#)
2. [Review your security info.](#)
3. [Learn how to make your account more secure.](#)

You can also [opt out](#) or change where you receive security notifications.

Thanks,

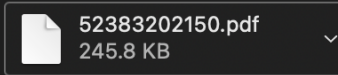
The Microsoft account team

EXTERNAL: View your Office 365 A1 for faculty invoice




○ Microsoft <microsoft-noreply@microsoft.com>

To: ✓ Wes Osborn



[Download](#) • [Preview](#)

 To protect your privacy, some external images in this message were not downloaded.

## Sign in to view your Office 365 A1 for faculty invoice

Your Office 365 A1 for faculty invoice is now available in the Microsoft 365 admin center. Sign in to view it.

[View your invoice >](#)

If you've already paid, disregard this email.

If you're set up to pay by credit card, no action is required—we'll charge your card within 24 hours of the invoice date.

To review changes made to this subscription, [go to the subscription history in the Microsoft 365 admin center](#).




### Additional resources

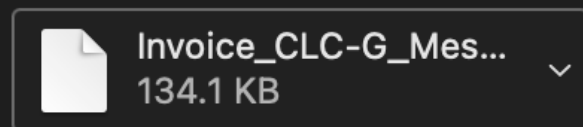
- [Learn more about your invoice](#)
- [Learn how to navigate your invoices](#)
- [Change the way you receive invoices](#)
- [Change your payment method](#)
- [Change your billing address](#)

## EXTERNAL: Unique Management invoice 6131815 – Central Library Consortium



 **tbullock@uniqueic.com** <tbullock@uniqueic.com>

**To:**  CLC Data Processing Center; **Cc:**  Wes Osborn 



[Download](#) • [Preview](#)

Caution: This email originated from outside of the organization. Do not click links or open attachments unless you

Hello!

Attached you will find the most recent invoice(s) for MessageBee notices.

Please let me know if you have any questions.

Thank you!

Teri Lynn Bullock  
Customer Service Account Manager  
Unique Management Services, Inc. | 800.879.5453

MT

○ **newsletter=zurifurniture.com@fastmortgageapprover.com** <ene...>

Tuesday, October 8, 2024 at 7:16 PM

on behalf of ○ **Mailgun Team** <newsletter@zurifurniture.com>

To: ○ CLC Data Processing Center; Cc: ○ CLC Data Processing Center ✓



# New API Key Has Been Created Successfully

If you did not make this change, please review this activity immediately.  
Unauthorized access can compromise your security.

**API Key Name:** [API-test 1 ]

**Creation Date:** Tue, 08 Oct 2024 16:15:50 -0700

**Key ID:** [ M0uy5rc4h-m3jomrdu ]

[Review Activity](#)

EXTERNAL: API Key Has Been Created Successfully



enewsletter=zurifurniture.com@fastmortgageapprover.com <ene...

Tuesday, October 8, 2024 at 7:16 PM

on behalf of Mailgun Team <enewsletter@zurifurniture.com>

To: CLC Data Processing Center; Cc: CLC Data Processing Center ✓



New API Key Has Been Created  
Successfully



Onto to the technical side

---

# Know your environment

---

Especially if you inherited it.



**purple knight**

powered by  semperis

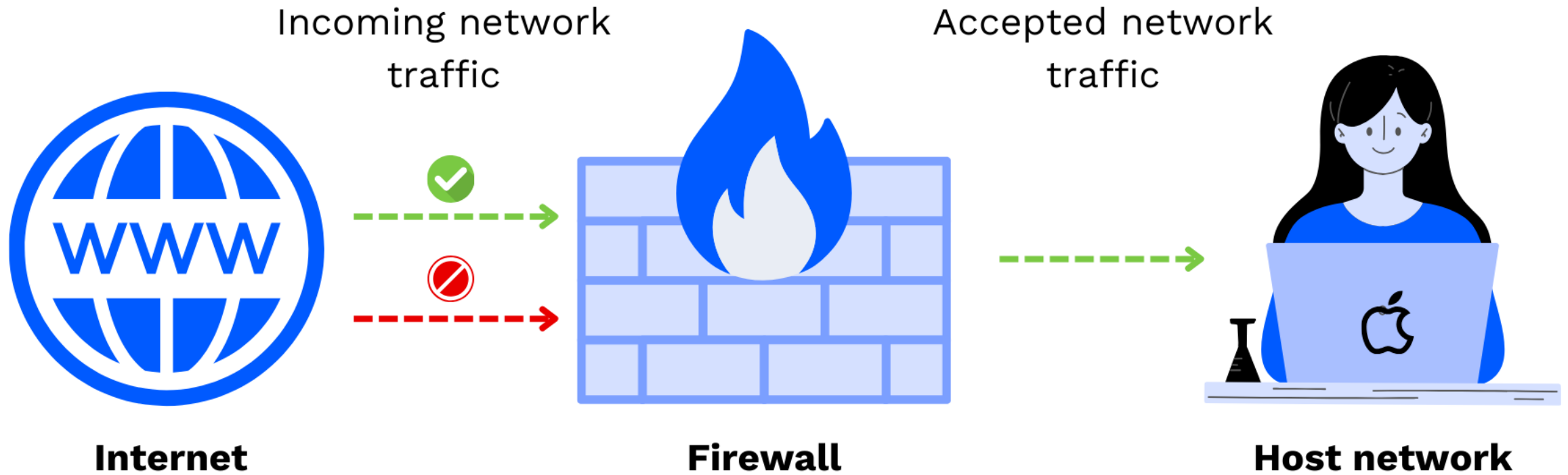
Run free Purple Knight scanning tool: Active Directory, Entra ID, and Okta vulnerabilities assessment tool



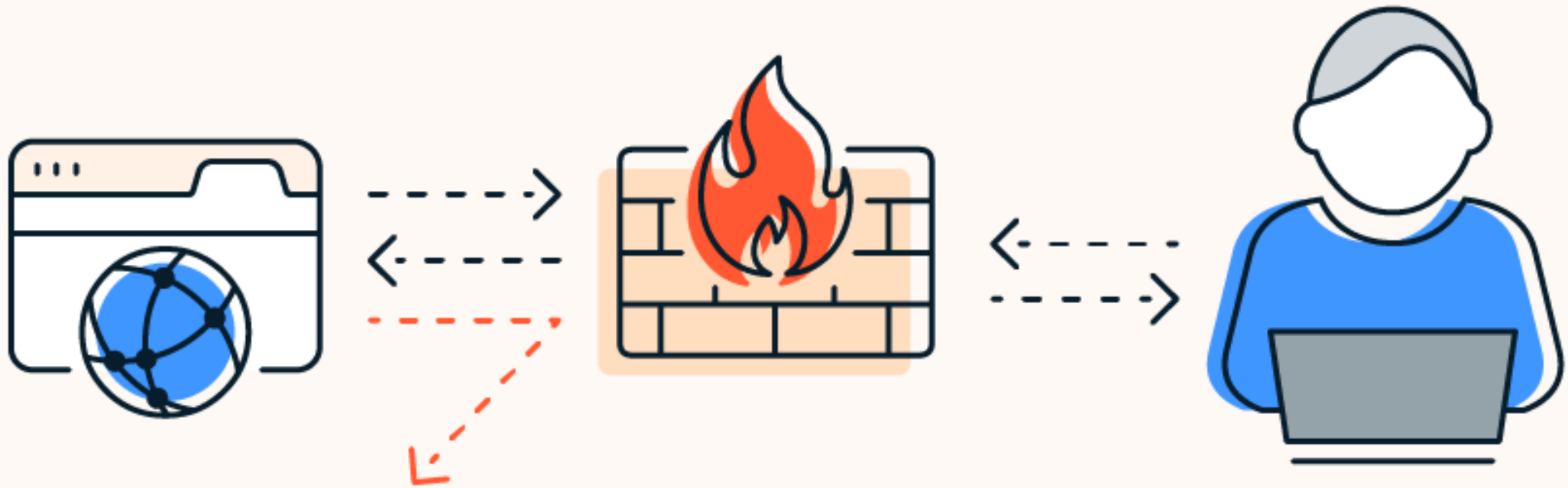
What has your firewall  
done for you today?

---

# Traditional firewall role



Should workstations allow outbound FTP?  
Block it with an egress rule.



# Other firewall options – Adjust as needed

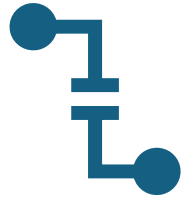
Sometimes your operating system has a firewall

Last line of defense

Sometimes just get in the way

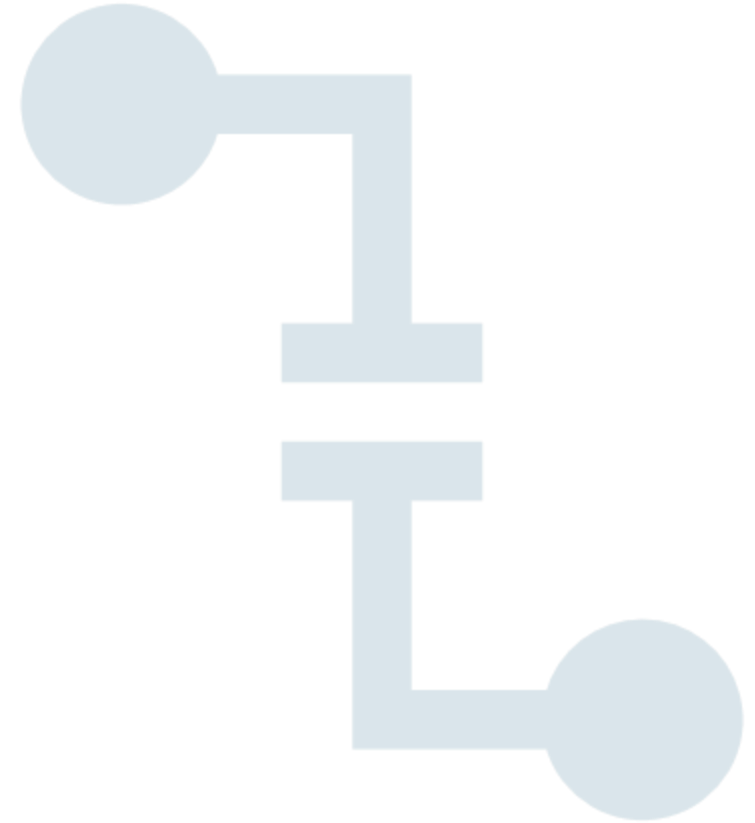
Polaris = Windows Firewall

Sierra = Limit Network Access table / iptable



# Web Application Firewall (WAF)

What you do when everything is port 80/443 traffic?



# Adding a WAF

---

Deeper inspection of the traffic

---

Can offer protection even if hosted

---

Can prevent search engine / AI bot scraping

---

Low price, self-service options  
(Cloudflare)

---

Typically requires changing DNS records

# Typical Cloudflare setup

1

Import or  
transcribe DNS  
records

2









Selectively  
enable  
Cloudflare  
proxying

3

Update name  
server (NS)  
records with  
registrar

4

Adjust settings  
as desired

<input type="checkbox"/>	must-be-proxied		required-for-redirect		
	A	www	192.0.2.1		Proxied
	must-be-proxied		required-for-redirect		
	CNAME	api2	990b420a-74d2-476d...		Proxied
	CNAME	api	990b420a-74d2-476d...		Proxied
	CNAME	authors	990b420a-74d2-476d...		Proxied
	CNAME	carousels	990b420a-74d2-476d...		Proxied
	CNAME	catalog	990b420a-74d2-476d...		Proxied
<input type="checkbox"/>	CNAME	clc-sso	990b420a-74d2-476d...		Proxied
<input type="checkbox"/>	CNAME	code	bitbucket.org		Proxied

# Self- hosted?

You've got even more  
Cloudflare options

# cloudflared reverse proxy eliminates NAT

Free for unlimited hosts

Gets all the extra protections of Cloudflare

DNS must be hosted by Cloudflare (free)

Proxies HTTP/S traffic only

←

Central Library Con...

▸

📅

Zero Trust overview

📊

Analytics

🔌

Gateway

▾

🔑

Access

▾

🌐

Networks

▴

Tunnels

Routes

Targets

👥

My team

▾

📋

Logs

▾

🔒

CASB

▾

🔒

DLP

▾

🔗

DEX

▾

✉️

Email Security

New

▾

[← Back to tunnels](#)

# clc-socc

OverviewPublic HostnamePrivate Network

## Public hostnames

+ Add a public hostname

		Public hostname	Path	Service
⋮	1	netmon-5050.clcohio.org	*	http://192.168.44.5:5050
⋮	2	netmon.clcohio.org	*	https://192.168.44.5
⋮	3	devauthors.clcohio.org	*	https://192.168.44.60
⋮	4	devapi.clcohio.org	*	https://192.168.44.60
⋮	5	leap-sso.clcohio.org	*	https://192.168.144.77
⋮	6	trainleap-sso.clcohio.org	*	https://192.168.144.162
⋮	7	devleap-sso.clcohio.org	*	https://192.168.144.87

# Secure Remote Access (VPN)



VPN access is a network backdoor



Treat with extreme caution

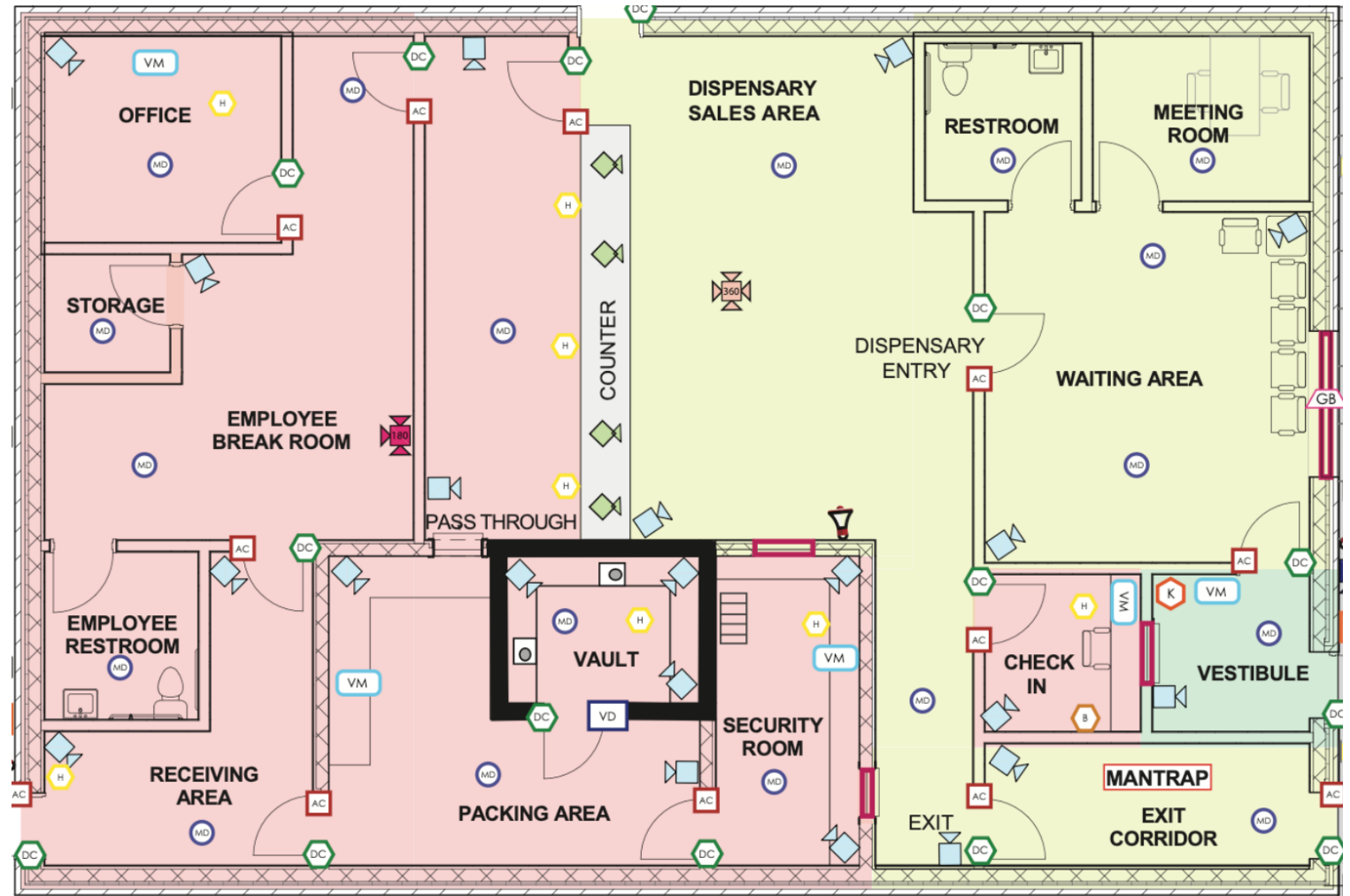


VPN should support SSO and 2FA

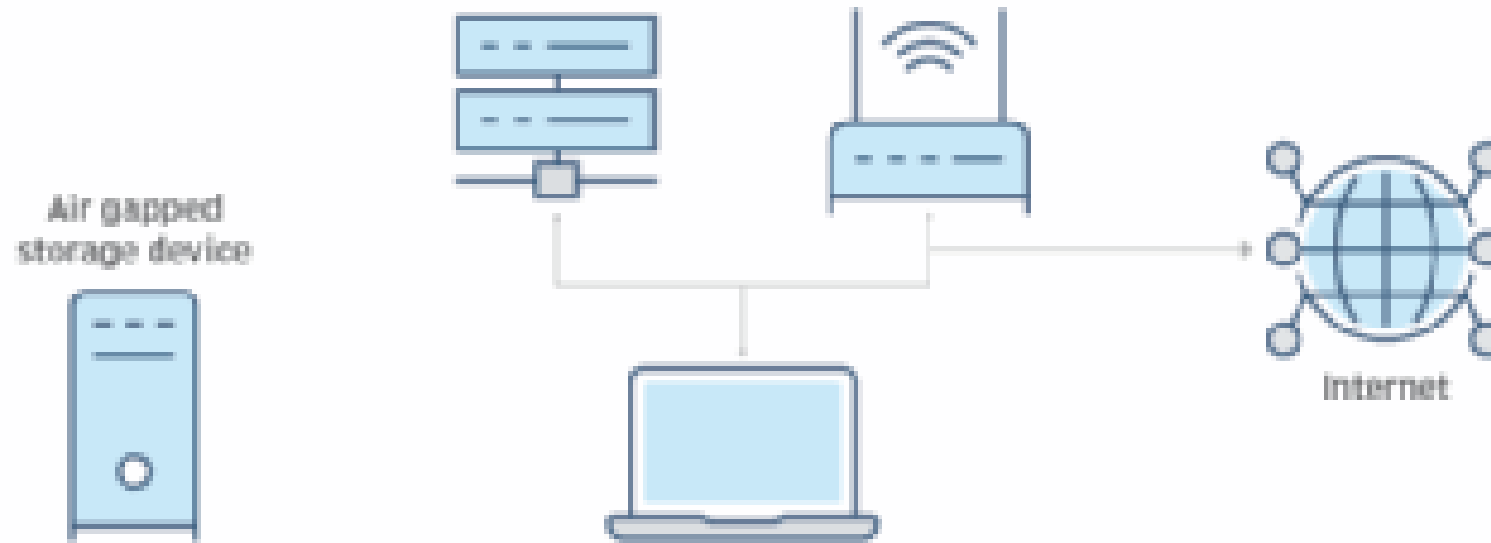


Cloudflare Zero Trust free (50 users)

# Protecting your most valuable assets



# Air gap computer network security



Do the most valuable servers need to access the Internet?





---

## Implement Single-Sign-On w/MFA

It is much easier to guard &  
monitor one door

Select a reputable vendor with  
good integrations: Okta,  
Microsoft, Google

Be careful with MFA setup

# Conditional MFA token setup

Don't allow MFA  
to be set up off  
network

Can allow  
attacker to set up  
own MFA device



# Consider *conditional* MFA



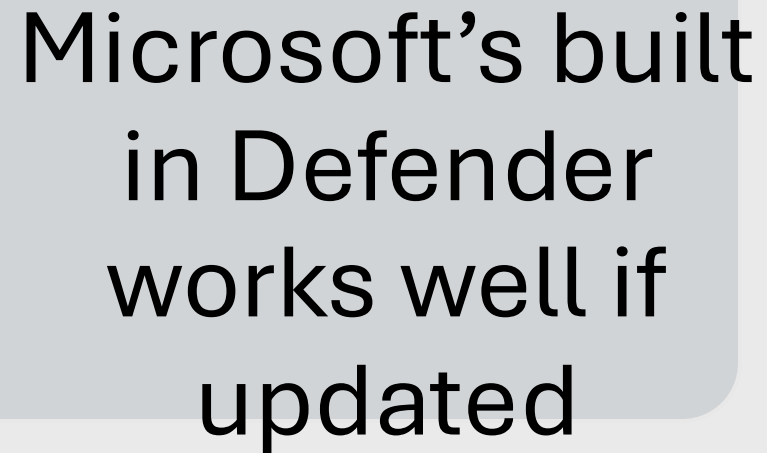
Only prompt for MFA  
outside of the building



Reduces "fatigue"  
associated with MFA

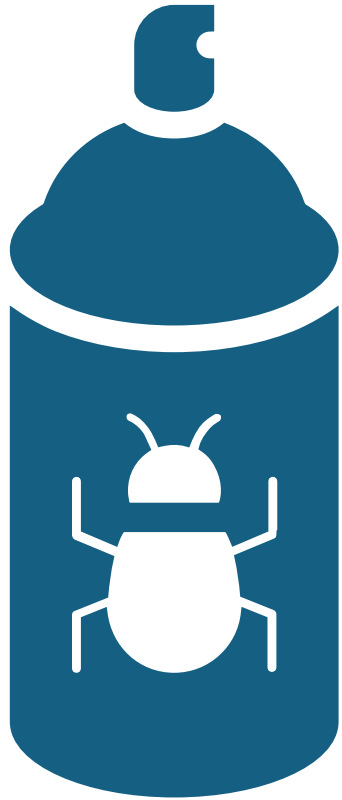


# Implement anti-malware software



Microsoft's built  
in Defender  
works well if  
updated

---



# Traditional anti-malware works by stopping known threats

There are approximately 200 new computer viruses developed each day.

How do you stop the new ones?



Only allow **known** good programs to run

Instead of trying to find & stop the bad programs

Assume everything is bad and only let **good** programs run



# Known as Allow listing

Threatlocker and Microsoft App Control are options

# Be smart about backups



MAKE SURE YOU  
HAVE THEM



STORE SOME OF  
THEM OFFSITE



CONSIDER  
IMMUTABLE BACKUPS

# Immutable Backups

---

Immutable:  
Cannot be  
changed

Protects attacker  
from making  
backups  
unusable

# Do a test restore



A restore is the only way you know you have a backup



Also helps estimate & improve your recovery time



# The Personal Touch

Do these things for yourself or your loved ones

Implement MFA on  
personal email account



Implement MFA on  
financial accounts



# Freeze your credit

Your info is probably out there, make sure no one can use it!

900+ websites & 14 billion accounts

Freezing your credit is free.



Daily **Mail**

## Major bank hit by data breach that sees social security numbers leaked

2 days ago • By Chris Melore



Washington Times

Bank of America warns customers of data breach after document handling mishap

16 hours ago • By Brad Matthews



Ya

Bank  
Breac

18 hou

# Recap



PROTECT YOUR EMAIL



DON'T BE PRESSURED  
BY URGENT MESSAGES



PROTECT YOUR  
BACKUPS

