
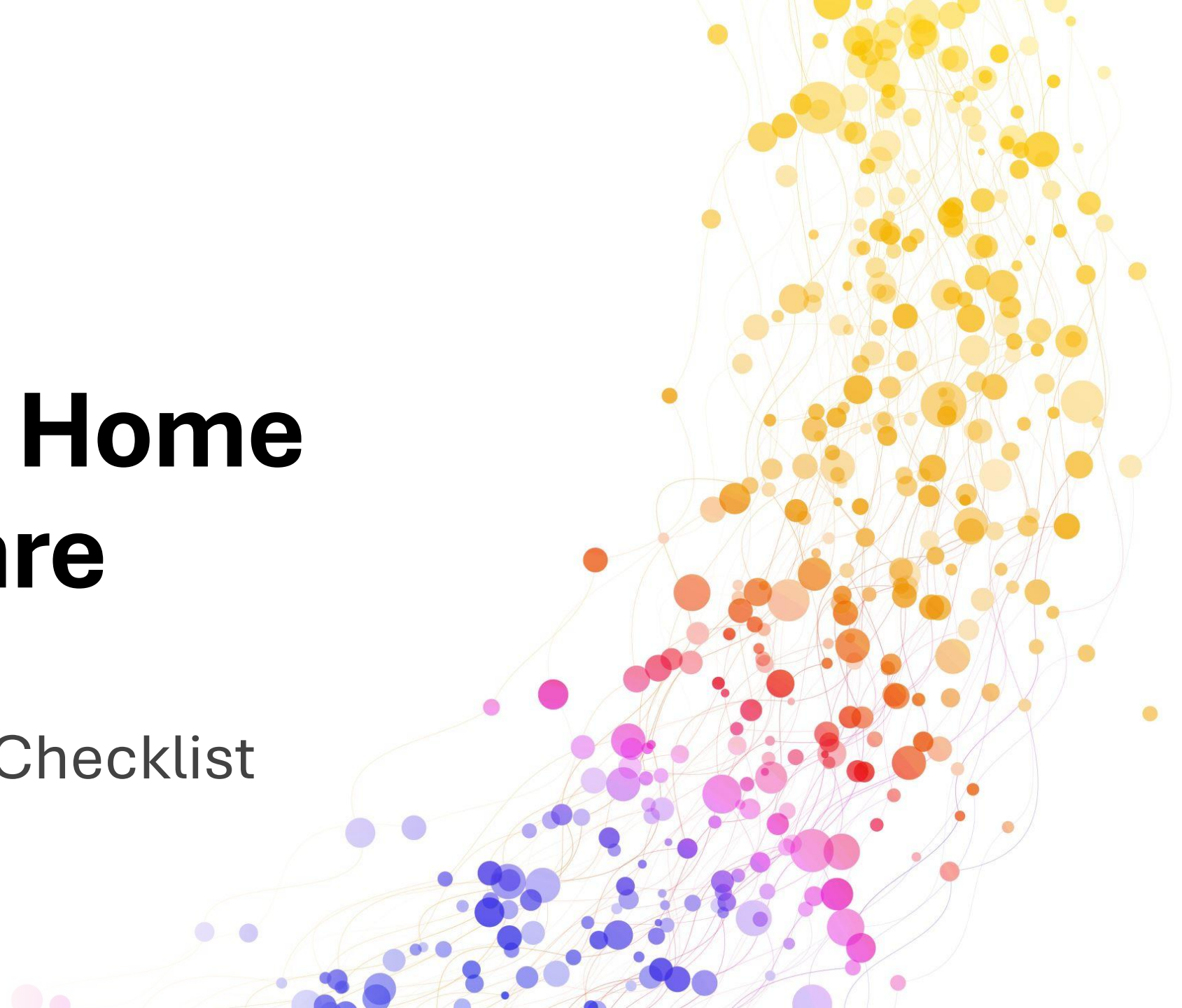




Securing Home Healthcare

 A Practical
Cybersecurity Checklist



Brian Boulanger

Vice President of Information Technology



Board Member





UNDERSTANDING THE RISK

- **92%** of healthcare organizations experienced at least one cyberattack in past 12 months (*compared to 88% in previous year*)
- Nearly **70%** of those attacks disrupted patient care
- Healthcare is the **#1** Target for Ransomware in 2025 (*increase from 2024*)

- # HIPAA Wall of Shame (HHS Breach Portal)

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf							
U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information							
>	McLaren Health Care	MI	Healthcare Provider	2192515	10/20/2023	Hacking/IT Incident	Network Server
>	Harris Eye Care	MI	Healthcare Provider	6267	08/08/2023	Hacking/IT Incident	Network Server
>	IVF Michigan, P.C.	MI	Healthcare Provider	9383	07/18/2023	Hacking/IT Incident	Network Server
>	John N. Evans, DPM	MI	Healthcare Provider	15512	06/03/2023	Hacking/IT Incident	Network Server
>	Vickers Engineering, Inc.	MI	Health Plan	857	12/20/2024	Hacking/IT Incident	Network Server
>	Continental Cafe Holdings, LLC Health Plan	MI	Health Plan	5039	11/27/2024	Hacking/IT Incident	Network Server
>	Detroit Chassis, LLC	MI	Health Plan	958	11/21/2023	Hacking/IT Incident	Network Server
>	Huron Inc. Health Plan	MI	Health Plan	750	11/08/2024	Unauthorized Access/Disclosure	Network Server
>	Detroit Wayne Integrated Health Network	MI	Healthcare Provider	3347	10/18/2024	Hacking/IT Incident	Laptop
>	Michigan Masonic Home	MI	Healthcare Provider	500	11/08/2024	Hacking/IT Incident	Email
>	University of Michigan/Michigan Medicine	MI	Healthcare Provider	57891	09/26/2024	Hacking/IT Incident	Email
>	Michigan Masonic Home	MI	Healthcare Provider	500	09/16/2024	Hacking/IT Incident	Email



UNDERSTANDING THE RISK

- **Change Healthcare (Feb '24)**
 - Cybersecurity Incident (Ransomware)
 - Outage: ~2+ Months
- **Ascension (May '24)**
 - Cybersecurity Incident (Ransomware)
 - Outage: 37 Days
- **McLaren Health Care (Aug '24)**
 - Cybersecurity Incident (Ransomware)
 - Outage: 20 Days



UNDERSTANDING THE THREAT

- **RANSOMWARE 101:**
 - **Ransomware:** a type of malicious software designed to block access to a computer system or data until a ransom is paid.
 - **Double Extortion:** a ransomware tactic where attackers not only encrypt data but also threaten to leak it if the ransom isn't paid.



UNDERSTANDING THE THREAT

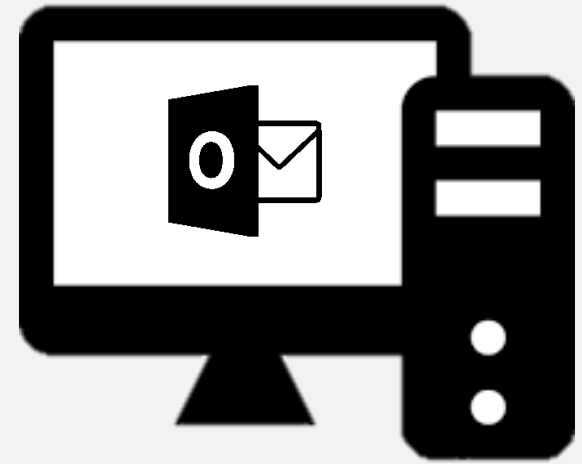
- RANSOMWARE
 - #1 Cause: HUMAN ERROR
 - Around 90% of ransomware attacks start with an EMAIL
- Focus for this presentation:
 - A. Training Employees
 - B. Preparing for 100% Human Error ← Let's start here!

ALONG CAME RANSOMWARE...

MALICIOUS EMAIL



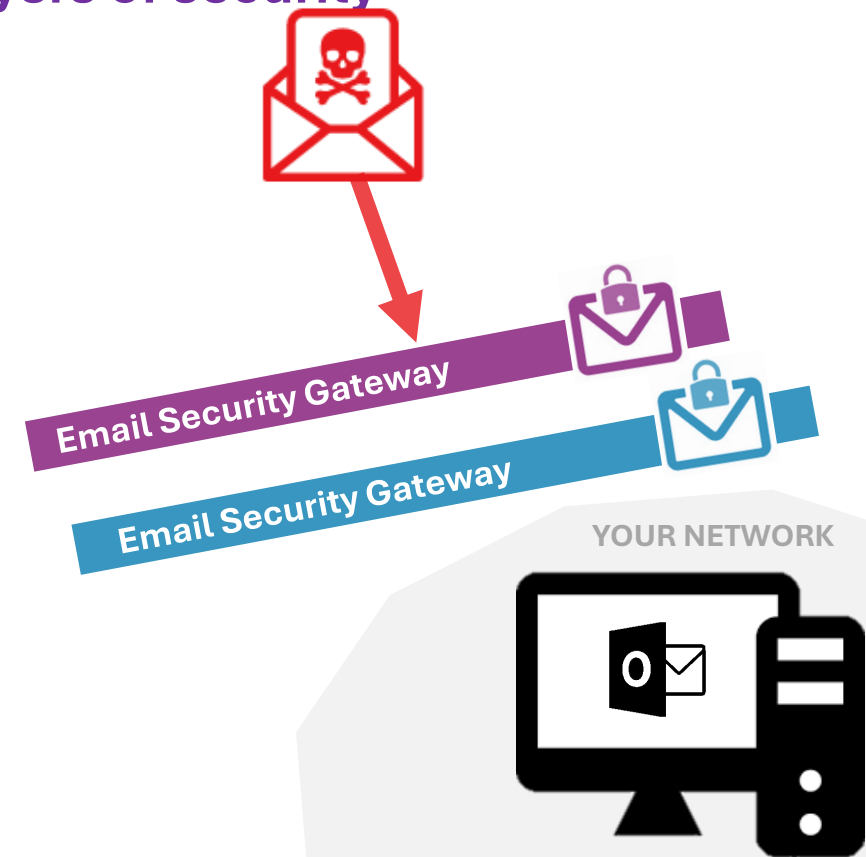
YOUR NETWORK





EMAIL SECURITY GATEWAYS

- “**Secure Email Gateway (SEG)**” – Device/Software that filters and monitors incoming and outgoing emails.
- “**Defense In-Depth**” – approach of using multiple layers of security to guard against failure of a single component.
- Incorporate 2 Layers / 2 Gateways.
- If you have them, are the settings optimized?
 - ✓ Turn on Advanced Phishing Protection
 - ✓ Hard block common malicious attachments
 - ✓ Consider blocking if DMARC is not configured/matching
 - ✓ Connect Realtime Block Lists (RTBL)
 - ✓ Send outbound email traffic through it as well
 - ✓ Turn on Data Loss Prevention (DLP) settings



EMAIL SECURITY GATEWAYS

- ✓ If you don't have one, get one.
- ✓ Ensure all settings are turned on/optimized.
- ✓ If you have 1, consider a second.
 - This is an area to invest!

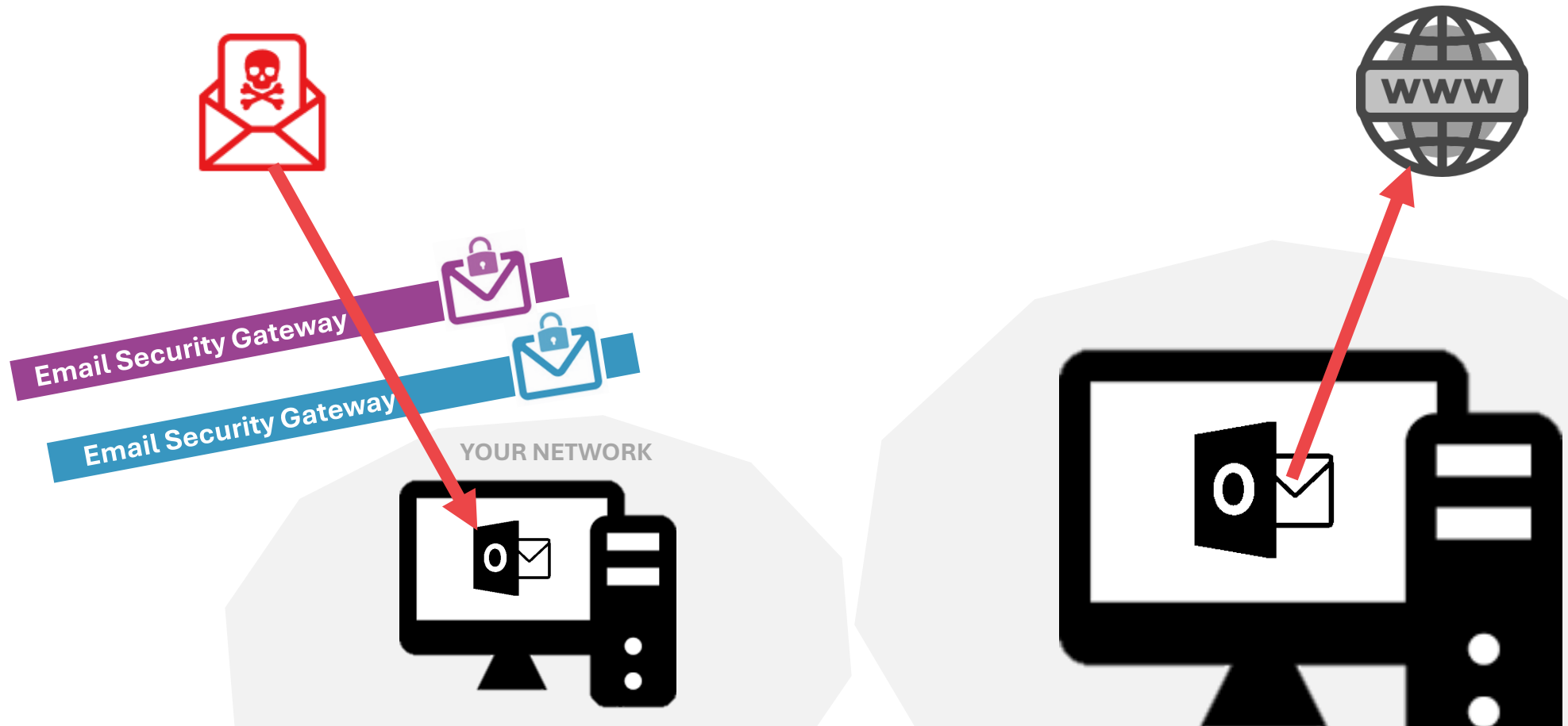
FREE TOOLS

- Microsoft “Exchange Online Protection” (*Free*)
 - Microsoft Defender for Office 365 (*Paid*)
- Barracuda Email Threat Scanner (*Free*)





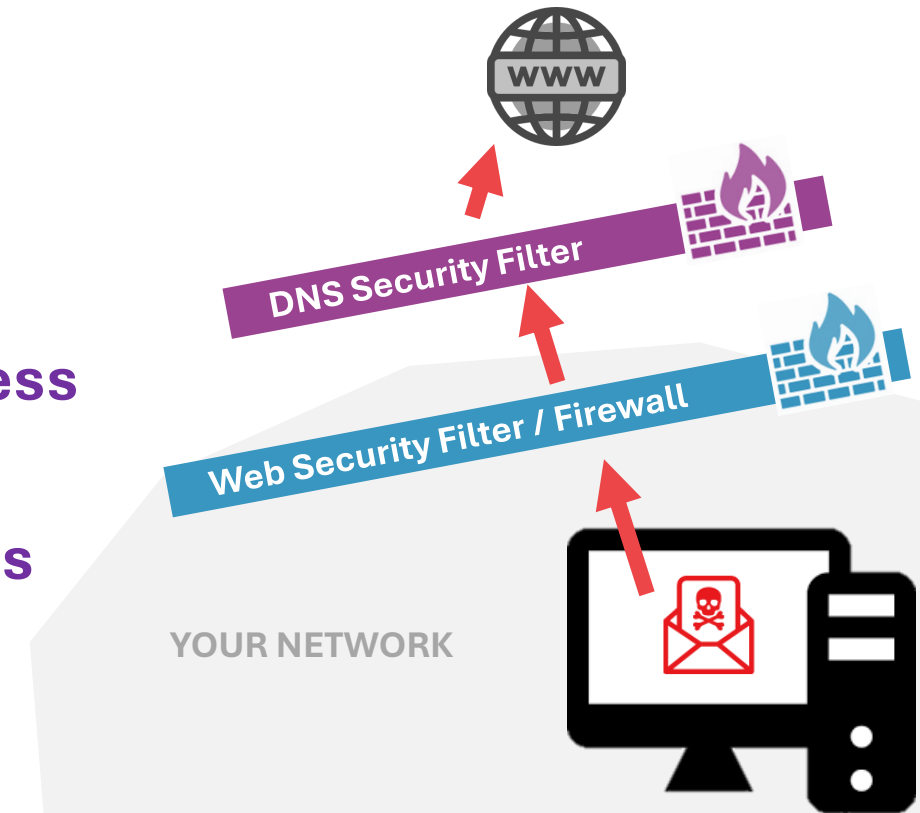
EMAIL SECURITY GATEWAYS





WEB FILTER / FIREWALL & DNS FILTER

- **Web Filter or Firewall – What's the difference?**
 - Next-Generation Firewalls (NGFW) cover Layer 7 (Application Layer)
- **Defense In-Depth:**
 - Web Filter + NGFW (Different Vendors) or
 - Web Filter + DNS Filter
- **DNS filter** = a security tool that blocks access to malicious or inappropriate websites by filtering domain name system (DNS) requests



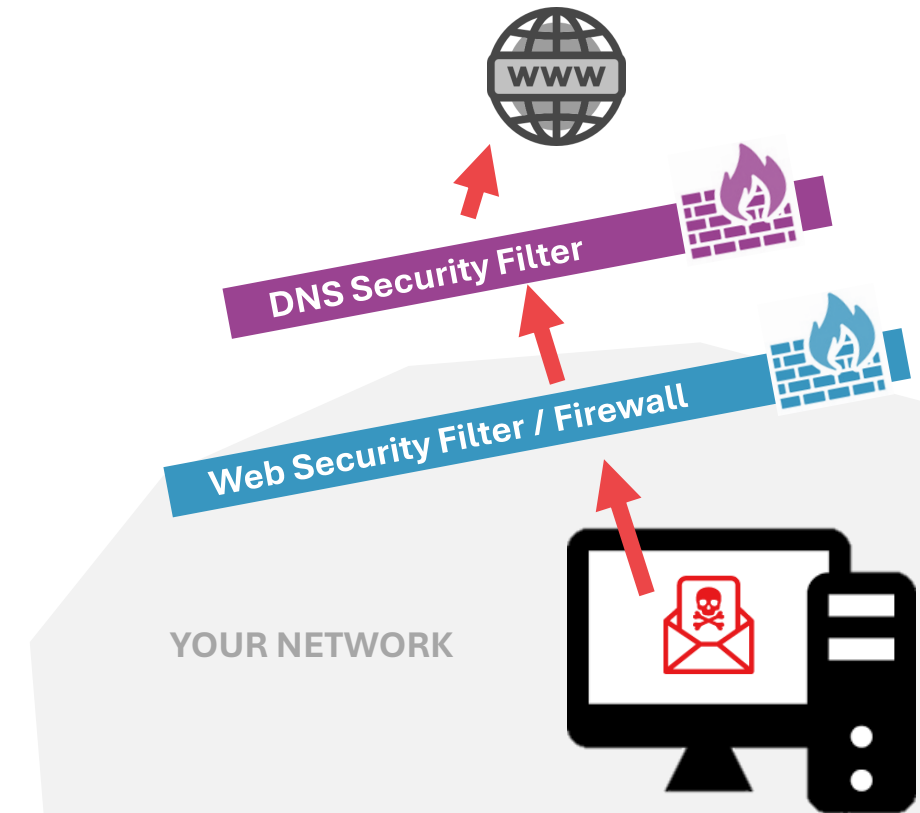


WEB FILTER / FIREWALL & DNS FILTER

☑ Have 2 outbound filters blocking Internet traffic

- FREE TOOLS?

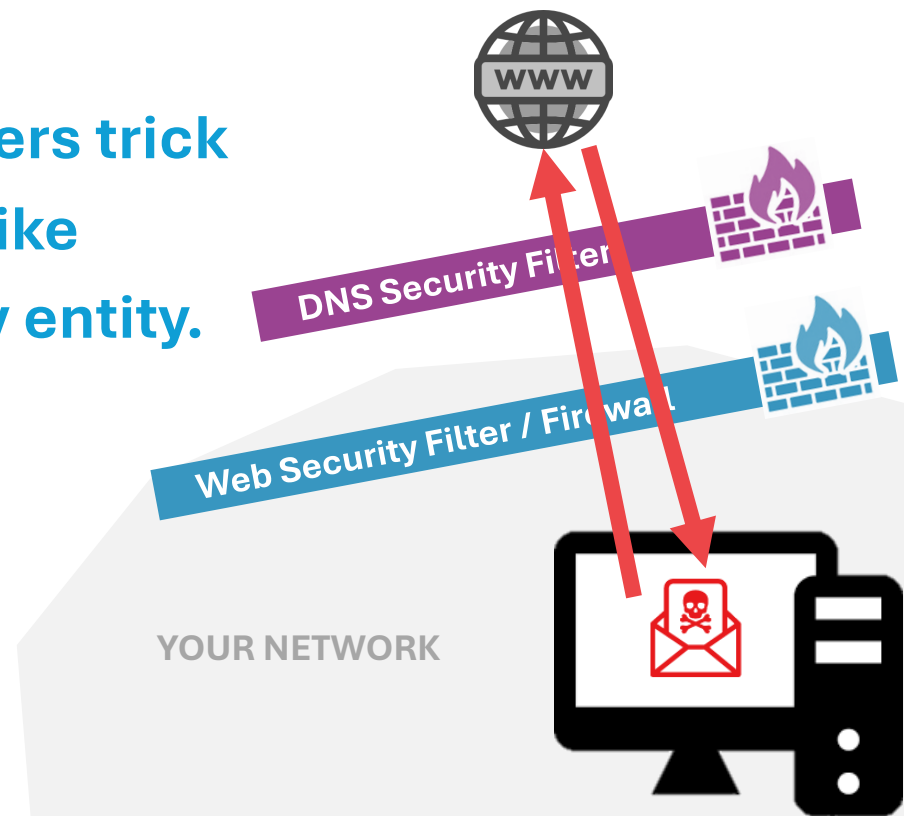
- pfSense Open Source Firewall
- OpenDNS (*Free*)
 - Cisco Umbrella (*Paid*)
- Control D Free DNS
- Quad9 Free DNS
- Windows Defender Firewall





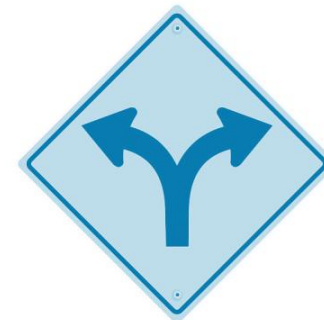
MALWARE or PHISHING?

- **Malware (Malicious Software):** Designed to damage or take control of your computer or steal your information.
 - Examples: Virus, Trojans, Ransomware, Spyware, etc.
- **Phishing:** Type of cyber attack where attackers trick people into revealing sensitive information, like passwords, by pretending to be a trustworthy entity.





REMOVE LOCAL ADMIN RIGHTS




MALWARE

- #1 **FREE** Security Measure!
 - *Because it's just a setting and a process change.*
- No one should have admin rights while surfing the web or checking email. **Period.**
- ☑ If you need elevated access, have a second account to authenticate admin functions. (Including your IT!)
- If your account can't install *anything*, then it can't install ransomware!



EDR > ANTIVIRUS



- EDR = Endpoint Detection & Response
 - AV (Antivirus): Uses signature-based detection of known threats.
 - EDR: Uses behavioral analysis and anomaly detection for advanced and unknown threats.
 - EDR: Includes broader protection with forensic tools and network-wide analysis.
-  Replace AV with EDR or XDR (Extended D&R)



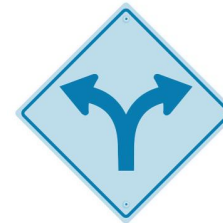
EDR > ANTIVIRUS



- **FREE TOOLS:**
 - Wazuh – Open Source XDR
 - Open EDR by Comodo
 - Most Popular Paid EDRs – SentinelOne, Sophos, CrowdStrike, Microsoft Defender for Endpoint



PATCH MANAGEMENT



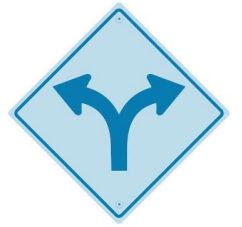
MALWARE

Approximately **60%** of ransomware attacks exploit known vulnerabilities that haven't been patched.

- **Windows (Operating System) Updates**
 - Monthly / “Zero Day”
 - Test, Force, and Ensure all endpoints get updated (servers too!)
- **Third Party Applications**
 - Web Browsers
 - All other applications



PATCH MANAGEMENT



MALWARE

- ✓ Uninstall Unneeded Software
- ✓ Force Windows Updates Monthly
- ✓ Make sure 3rd Party Applications are getting updated

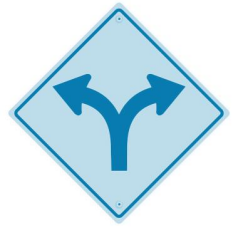
- **FREE TOOLS:**

- Action1 Free Patch Management Solution
- Windows Autopatch & Azure Update Manager (*Replaces WSUS*)





VULNERABILITY MANAGEMENT



MALWARE

- Security Evaluations

1. Vulnerability Assessment (*At least quarterly+*)
2. Pen Tests (*1-2 times a year*)
3. Gap Analysis (*Annually or after major changes*)

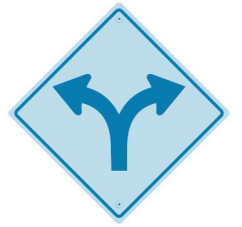
- Vulnerability Scanners

- ☒ Scan both On-premise and External
- ☒ Have teams reviewing & resolving results





VULNERABILITY MANAGEMENT



MALWARE

- **FREE TOOLS:**

- Netwrix Free Auditing Tools
- Qualys SSL Labs
- OpenVAS Vulnerability Assessment Scanner
- CISA's Cyber Hygiene Services
- F12.net Free Gap Analysis & Dark Web Scan



IF PHISHING ATTEMPT...

Over 90% of successful ransomware attacks start with phishing emails.

- *Scenario: successful phishing attempt, aka credentials have been shared....(or acquired)...*

Now what?



PHISHING





MFA MFA MFA



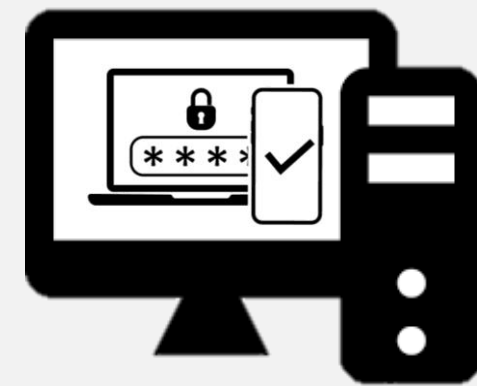
PHISHING

- **Multi-Factor Authentication (MFA)** – process requiring users to provide 2+ verification factors to gain access.
 - Something you KNOW (password / PIN)
 - Something you HAVE (phone / token / smart card)
 - Something you ARE (biometric: fingerprint / facial recognition)



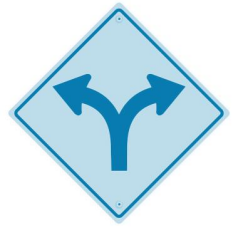
MFA EVERYTHING!

- Anything accessible from the Internet,
including email!





MFA MFA MFA



PHISHING

☑ If you have MFA, Increase Security Requirements.

- Not all MFA is created equal:

Phone Call < Text Message < Email < Auth App

< Authenticated Push < Biometrics < Security Token

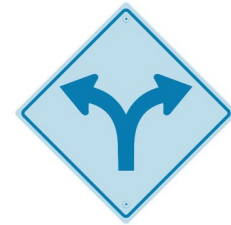
☑ Enable Single Sign-on (SSO) whenever possible

- Compliments MFA (SSO + MFA = 🗝️)
- Easier for end user + Easier to manage security





MFA MFA MFA



PHISHING

- **FREE TOOLS:**

- **Duo Free**

- **Advanced Features (*Paid*)**

- **Microsoft Authenticator**

- **Google Authenticator**

- **Authy by Twilio**

- **privacyIDEA**





PRINCIPLE OF LEAST PRIVILEGE



PHISHING

- The security concept that recommends giving users the minimum level of access necessary to perform their tasks.
 - No one should have access to everything. If you can access and edit everything, then everything is gone if ransomware is installed.
-
- ☑ Minimize Admins with full access.
 - ☑ Reduce default access for all users.
 - ☑ Set stricter access for external vendors.



INTRUSION DETECTION



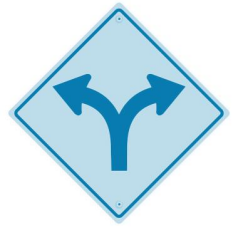
PHISHING

It takes organizations an average of **204** days to identify a data breach.
(Many breaches can go unnoticed for *over six months!*)

- Next Generation Firewall with IPS & IDS
 - IPS = Intrusion Prevention System
 - IDS = Intrusion Detection System
- Do you have alerts? Who's getting them, reviewing them?
 - SIEM = Security Information & Event Management
 - SOC = Security Operations Center



INTRUSION DETECTION



PHISHING

- **FREE TOOLS:**

- **Employees – the Prepaid IDS!**

- Does your staff know how/where to report something?

- ☒ Setup a special email address for all security threats to be sent to.

- Snort IDS (from Cisco)
 - Suricata IDS
 - Zeek IDS
 - OSSEC IDS





INCIDENT RESPONSE PLAN

- Do you know who to call first?
- Do you have Cyber Insurance?
- Do you have a Business Continuity Plan?

- ☑ Make Incident Response Plan, Business Continuity Plan & Disaster Recovery Plan, if you don't already have.
- ☑ Have routine table-top exercises simulating these plans.





INCIDENT RESPONSE PLAN

- **FREE TOOLS:**

- Security Risk Assessment Tool by HealthIT.gov
- Michigan's DTMB Sample IRP's
- SANS Security Policy Templates
- Use ChatGPT to help write your policies!





DATA BACKUPS

Over **55%** of ransomware cases are resolved using backups.

While 78% of users claim to back up their data, only 33% do so regularly.

- Arguably the #1, most important defense against ransomware.
 - If files get encrypted (i.e. locked), you can restore from backups.
- Are you backing up files and records? How often?
- Are you testing your backups + restoring them?
- 3-2-1 backup strategy:
 - 3 Copies of data
 - 2 different storage types
 - 1 off-site or in cloud



DATA BACKUPS

- ✓ Backup software and servers, not just files, daily.
- ✓ Test restoring backups regularly.
- ✓ Follow 3-2-1 Backup Strategy

- **FREE TOOLS:**

- Veeam Backup & Replication Community Edition
- EaseUS Todo Backup Free





OTHER MEASURES

- ✓ Turn on Windows Firewall on all PCs
- ✓ Mobile Device Management (MDM) System on Company Cell Phones
- ✓ Network Segmentation throughout, especially IoT devices
- ✓ Incorporate a Cloud Security Gateway
- ✓ Enable SSO when able
- ✓ Limit & Secure Wi-Fi networks
- ✓ Close ports and protocols on public IPs
- ✓ Limit 3rd party access
- ✓ Require strict security protocols for 3rd party vendors
- ✓ Enforce Security-related Group Policies for Windows:
 - ✓ Lock Computer, Force Password Policy, etc.
- ✓ Encrypt everything, wherever possible
- ✓ Never use unsupported operating systems
- ✓ Turn on BitLocker to encrypt all Windows hard drives
- ✓ Strong VPN for remote access
- ✓ Secure remote access to applications
- ✓ Only use secure browsers
- ✓ Restrict users from checking personal email

TRAINING STAFF



TRAINING

82% of data breaches involve human-related security weaknesses, such as phishing attacks and social engineering.

92% of employees state that workplace training *positively impacts* their engagement and commitment to their roles.

PHISHING TESTS



TRAINING

- **Most practical way to train against Ransomware!**
- **TIPS:**
 - Phish your employees regularly – consider monthly
 - Explain the test to all employees (show example & how it could have been identified as phishing)
 - Re-test until the end user passes
- **Positive Reinforcement:**
 - Incentivize Passing (rewards & recognition)
- **Negative Reinforcement:**
 - Provide Warnings, Counseling & Additional Training upon Failing



PHISHING TESTS



TRAINING

☒ **Don't let users access personal email**

- **FREE TOOLS:**

- Phish Insight by Trend Micro
- CanIPhish
- KnowBe4 (Freemium)
- Infosec IQ Free Phishing Risk Assessment
- Gophish Open-Source Phishing Framework
- Microsoft's Attack Simulation Training (*Included with some O365 licenses*)



SECURITY TRAINING



TRAINING

- Do you have a cybersecurity training course?
- **Microlearning**: delivering educational content in small, focused segments that are easy to digest and understand.
- Take advantage of Free Options, as part of an overall microlearning strategy.
- For Ransomware, focus on Phishing & Passwords



SECURITY TRAINING



TRAINING

- **FREE TOOLS:**

- Wizer Security Awareness Training
- Amazon Cybersecurity Awareness Training
- Jigsaw (Google) Phishing Quiz
- Federal Trade Commission Resources
- SANS Security Training
- CyberSecure My Business



PASSWORD HYGIENE



TRAINING

Weak or stolen credentials account for nearly **50%** of ransomware incidents.

- **2 primary causes for Compromised Passwords are:**
 - Weak Passwords (easy to guess or crack)
 - Stolen Passwords (acquired or leaked from a data breach).
- **What Makes a Good / Strong Password?**
 - Long (Passphrases > Password)
 - Easy to remember
 - Unique



PASSWORD HYGIENE



TRAINING

- **How to fend against Stolen Passwords?**
 - Don't re-use passwords
 - Never have the same password for multiple accounts
 - Check your passwords with Free Tools!
- **FREE TOOLS:**
 - Delinea Weak Password Finder Tool
 - Have I Been Pwned
 - Password Strength Checker by Security.org



RESOURCES!

- Scan below for list of resources referenced in this presentation:



rebrand.ly/securitytools



QUESTIONS?