

Washington State Office of Cybersecurity

Josh Eshenbaugh



Becoming Cyber Aware



Introduction

I am a security analyst with the Washington State Office of Cybersecurity.

- Over 10 years experience in Cybersecurity
- Threat Intelligence Researcher
- Cyber Incident Responder
- Digital Forensics
- Malware Analysis
- Cloud Compliance Consultant



Objectives

What does the cyberthreat landscape look like?

Who is responsible for protecting it?

What are security best practices?

Protecting Your Home Network

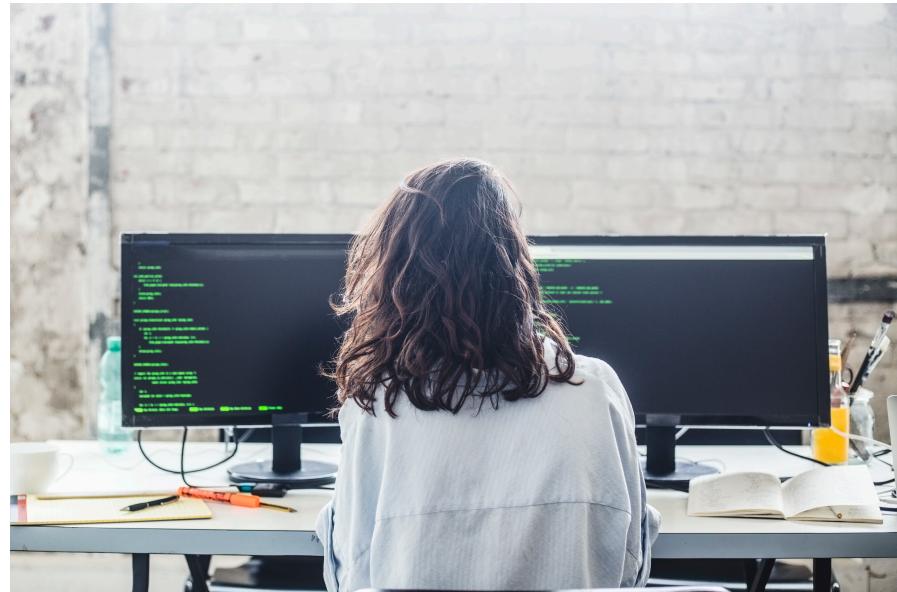
- Encryption
 - Use WPA2 or WPA3
 - Older device maybe using WEP or WPA. Try upgrading if possible
- Firewalls
 - Make sure firewalls are turned on at the device level
 - Microsoft Defender is free and comes installed and activated on most Microsoft devices.
- Wireless Access using MAC Address
 - Limit the devices that can connect to your router
- SSID Broadcasting
- Change your Wi-Fi Name and Password

Connecting to Resources at the Office

- Only connect from trusted Wi-Fi networks
- Use a VPN whenever possible. Some office may require this to connect to shared resources
 - If you must use public or untrusted Wi-Fi only do so through a VPN
- Pay close attention to your work emails for anything that is suspicious and unexpected
 - Emails are the most used source for most successful attacks

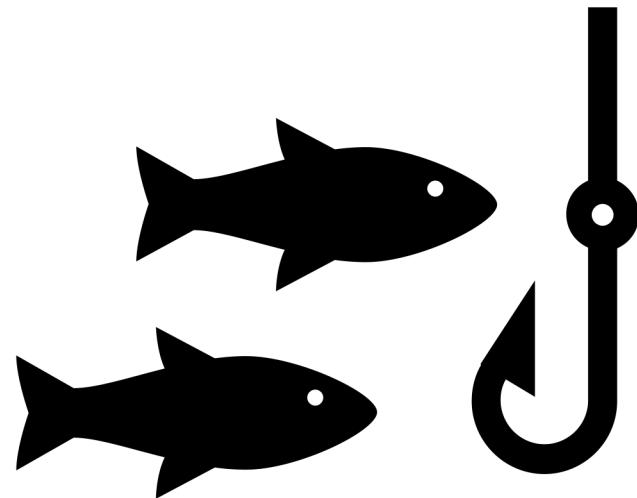
Cyberthreats

- **Phishing**
- Denial-of-Service (DoS) Attacks
- Zero-day-attack
- Trojans
- Keylogger
- **Spoofing**
- Cyberstalking
- Data Breach
- Malware
- **Ransomware**



Phishing

- The most common way computer systems become infected with malware is through phishing emails.
- It only takes one person to open an infected attachment, click on a link that goes to a malicious website, or be tricked into providing their account credentials.
- They may appear to be from people or organizations you know and trust.
- They contain information from previous emails threads so that it appears to be part of a continuing conversation.



General tips to avoid becoming a victim:

- Be suspicious of any emails that urge you to act and try to create a sense of urgency.
- Never click on links or open attachments without first making sure the request is authentic.
- Call the sender by looking up their phone number independently.
- Never call a phone number included in a suspicious email or reply to the sender.
- You can also hover your mouse over links to determine the full address.

Common types of attachments seen in phishing campaigns:

- Malicious files with innocent names, such as “invoice.”
- Office products such as Excel and Word can have malicious macros (programs that run inside of programs).
- PDF files may have a malicious link or a macro embedded.
- Files that emulate a DVD drive or a USB drive (extension .iso, .ism) can be used to automatically run a script once opened.

Common ways bad actors try to trick you:

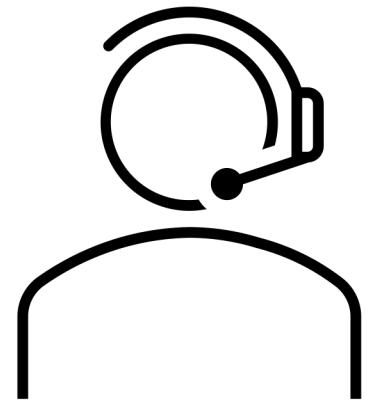
- A popular band is coming to town, are you going?
- You have an imminent deadline for sexual harassment training.
- Sense of Urgency:
 - Your password is about to expire
 - A deadline is approaching for mandatory training
 - Overdue bill
 - Your account credentials have been compromised

Phishing



Spoofing

- Disguising a communication from an unknown source as being from a known, trusted source.
- Spoofing can apply to :
 - emails
 - phone calls
 - websites
 - computer spoofing an IP address



Spoofing Example

Hello Brenda!

Let me know if you're unoccupied I'll need you to run a task expediently. I have run a survey on all employees, I want to acknowledge the dedicated staffs and appreciate them with gifts. So, I am suggesting some shopping gift cards for them. P.S: I'm busy at the moment but I will look out for your reply. Kindly let me know how soon you can handle this.

Thanks.

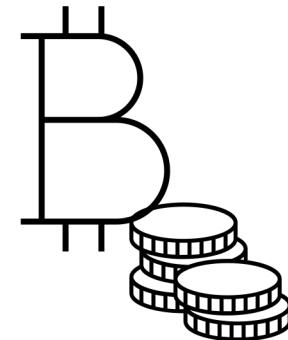
Best Regards.

Director

Ransomware

A type of malware used by bad actors that enable to actor threaten to:

- To publish the victim's data until a ransom is paid
- Perpetually block access until a ransom is paid



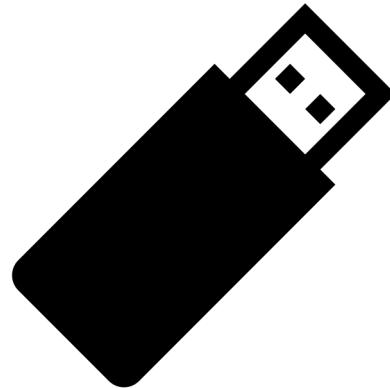
<https://us-cert.cisa.gov/ncas/tips/ST19-001>

Protecting Against Ransomware

Back up your computer

Store your backups separately.

- Best practice is to store your backups on a separate device that cannot be accessed from a network
- Once the backup is completed, make sure to disconnect the external hard drive, or separate device from the network or computer.



Does it really happen?

Google Sends At Least 50,000 Warnings To Users At Risk Of Government-Backed Phishing Attack

By Lea
10/15/

Washington State Agencies Battle Large Phishing Campaign

What you need to know about the massive hack of Washington unemployment data

Feb. 3, 2021 at 6:00 am | Updated Feb. 3, 2021 at 4:48 pm



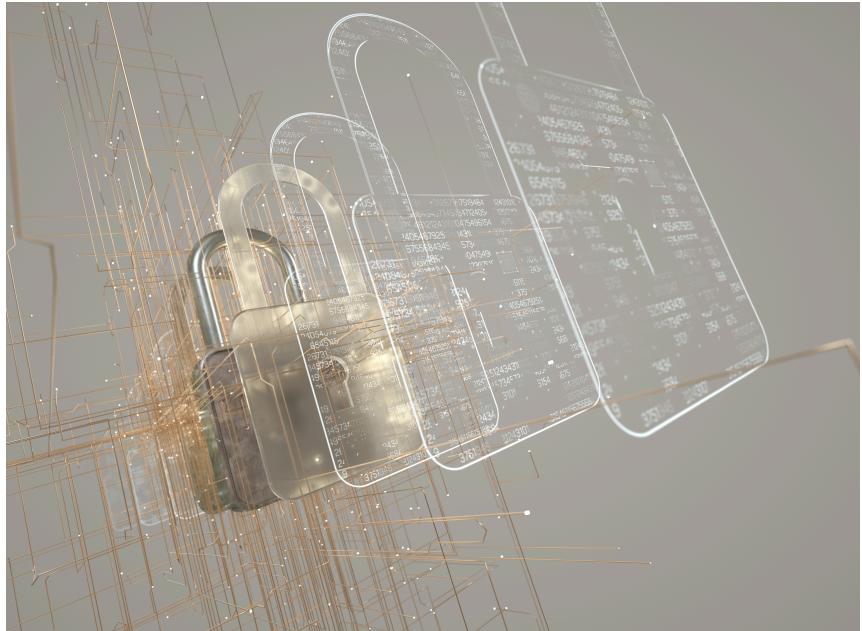
Who is responsible for Cybersecurity?

Short answer: Everyone

Defense in depth vs the user

Defense In depth:

- Physical controls
- Technical controls
- Administrative controls



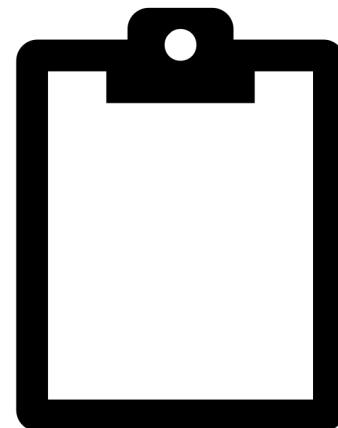
Where can we start?

Technical and Administrative Implementations:

- Asset Inventory
- Risk Assessments
- Planning (Security Plan, Incident Response Plan)
- Detection and Monitoring Capabilities.

User Awareness:

- Security Awareness Training
- Phishing Simulations
- Tabletop Exercises
- Bulletins or Alerts



Helpful resources

CISA

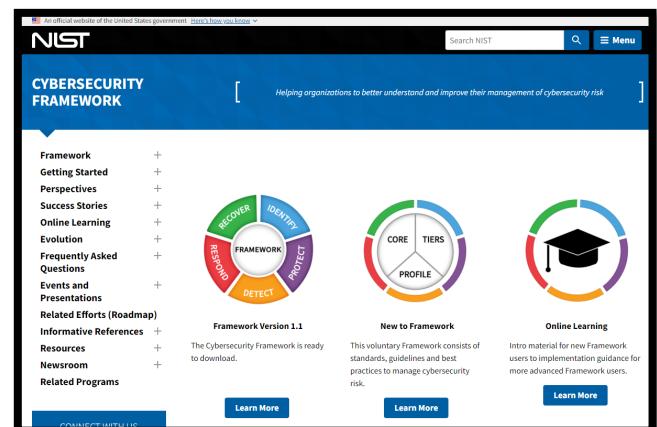
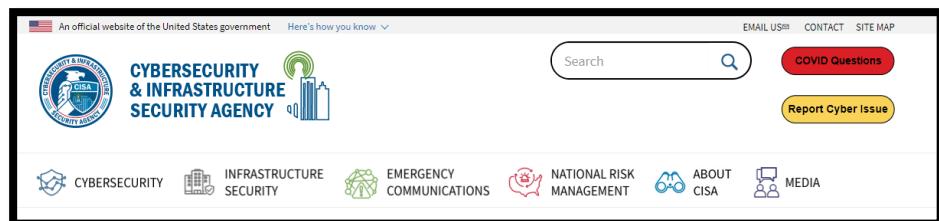
<https://us-cert.cisa.gov/ics>

NIST CSF

<https://www.nist.gov/cyberframework>

CIS Configuration Guidelines and Benchmarks

<https://www.cisecurity.org/cis-benchmarks/>



Never Alone

If you feel your organization is experiencing a cybersecurity emergency always feel free to reach out to the Office of Cybersecurity

<https://cybersecurity.wa.gov/>

**Call 360-407-8800
(option #2) to report
cybersecurity incidents.**



**Carve out time
for Hacktober!**

This Friday (Oct. 1) marks the first day of Cybersecurity Awareness Month (aka Hacktober) and kicks off a series of fun, interactive events aimed at improving everyone's understanding of online threats and how to protect information entrusted to the state. This year, WaTech's state Office of Cybersecurity is adding new, fun ways to test your cybersecurity knowledge including a virtual escape room, online quiz games and weekly presentations.

Q and A

Thank you!

Joshua.Eshenbaugh@watech.wa.gov

cirt@osc.wa.gov
