WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

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

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Objectives

What does the cyberthreat landscape look like?

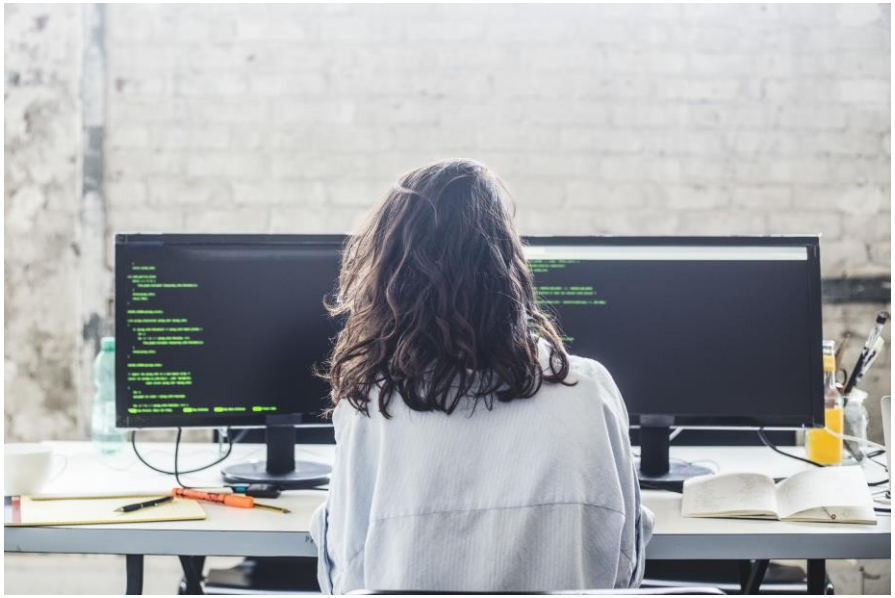
Who is responsible for protecting it?

How do we get started?

What resources are available?

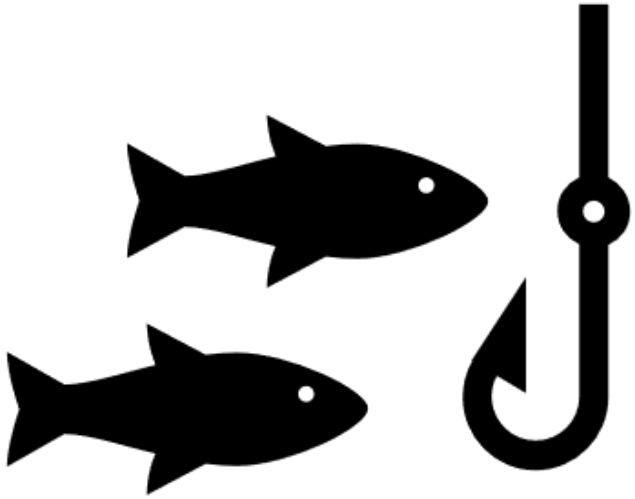
Cyberthreats

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



WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

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

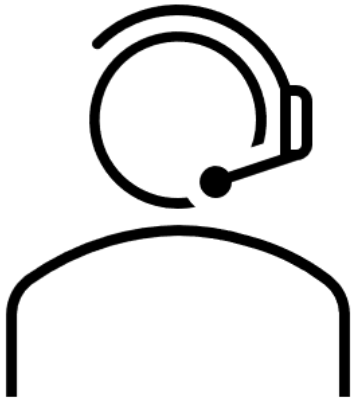
Phishing


username@organizationname.tld CDC Message
Do you recognize the sender's email address? Is it from outside your organization?
[organizationname.tld] Secured Mail [redacted]
To username@organizationname.tld
Reply
Reply All
Forward
Wed 12/16/2020 5:16 AM
If there are problems with how this message is displayed, click here to view it in a web browser.
CDC
Pfizer
Would you expect to recieve a direct communication from the CDC?
Does the email try to convey a sense of urgency?
You've received a secure message
Signature for Vaccine-2690
Yes / No
Never click on a link or attachment without first verifying the email's authenticity.
Are there grammar and punctuation errors?
Authorize Pfizer vaccine distribution use for your reference. Complete the form to ensure vaccine count for your area.
Pfizer

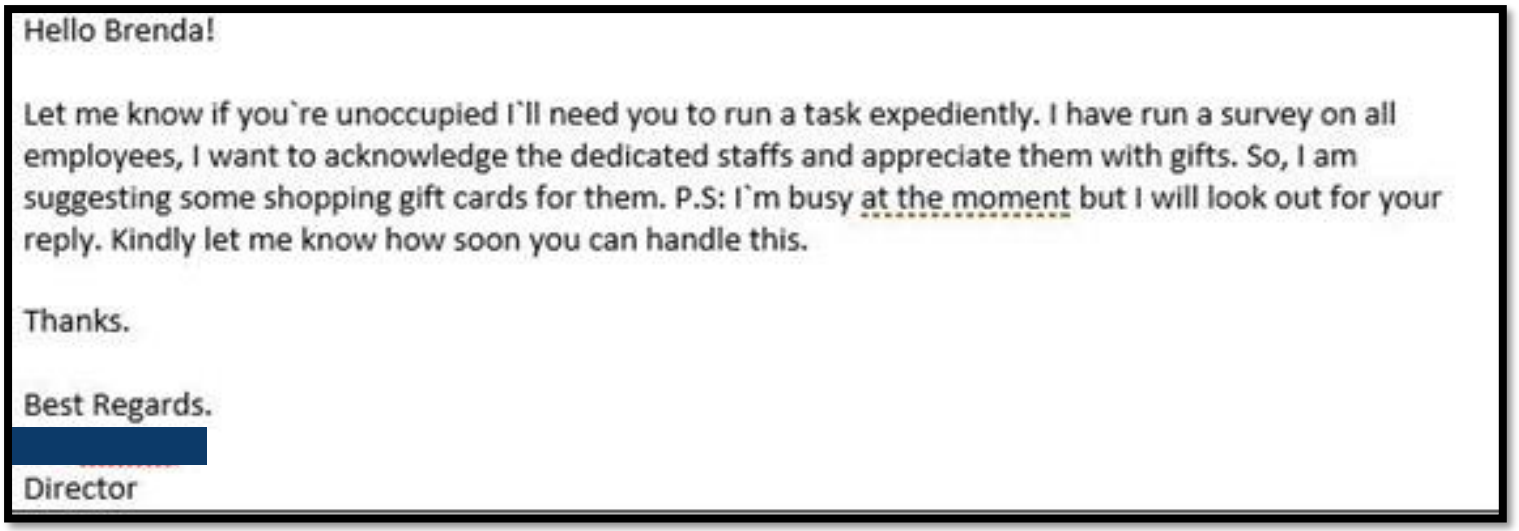
Spoofing

- 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.

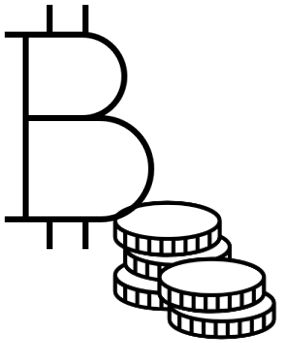
[redacted]

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

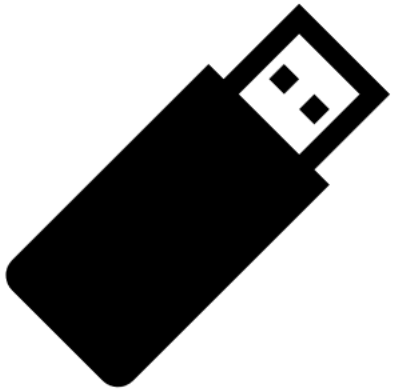
Protecting Against Ransomware

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.



WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Does it really happen?

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

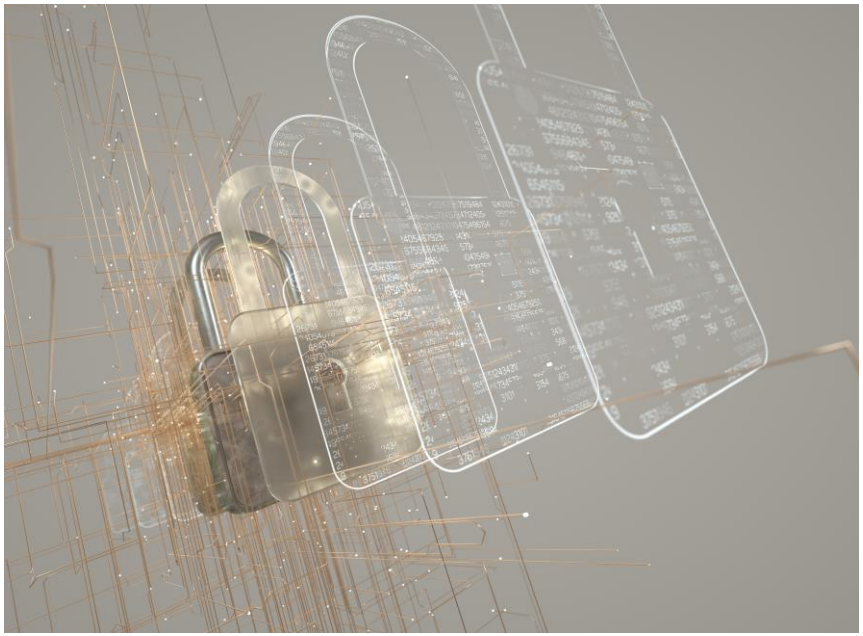
Who is responsible for Cybersecurity?

Short answer: Everyone

Defense in depth vs the user

Defense In depth:

- Physical controls
- Technical controls
- Administrative controls



WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

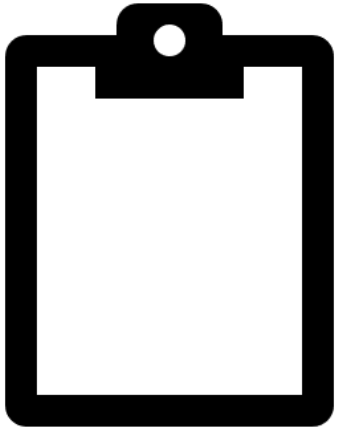
Where can we start?

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



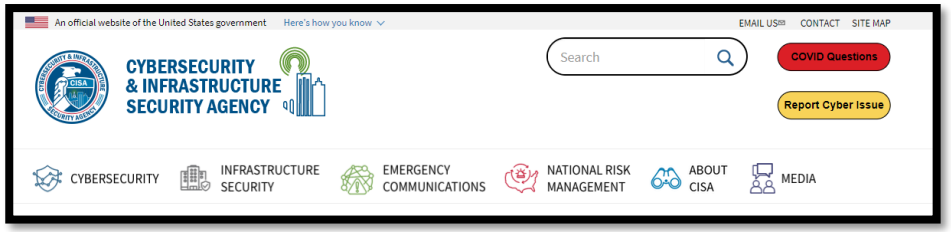
Helpful resources

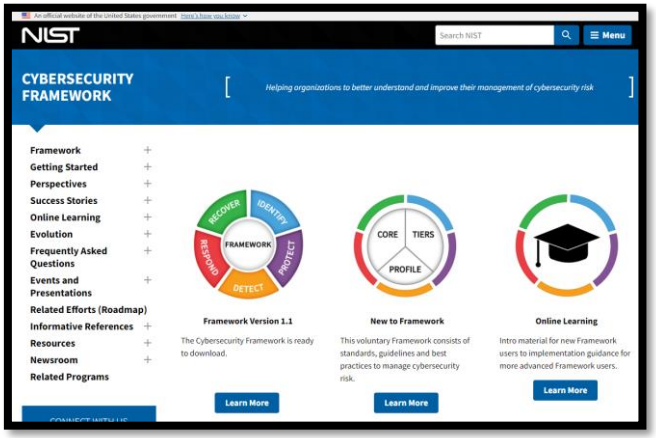
CISA
https://us-cert.cisa.gov/ics

NIST CSF
https://www.nist.gov/cyberframework

CIS Configuration Guidelines and Benchmarks
https://www.cisecurity.org/cis-benchmarks/

American Water Waters association
https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance





WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

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/

Washington state agencies should call 360-407-8800 (option #2) to report cybersecurity incidents.

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Q and A

Thank you!

Joshua.Eshenbaugh@ocs.wa.gov