Cybersecurity Awareness

Protecting your devices and networks
Threats and Attacks on Networked Devices

- Threats
  - Vulnerabilities
  - Misconfigurations
  - Lack of Security

- Attacks
  - Man-in-the-middle
    - Eavesdropping
    - Replay/Redirection
  - Exploitation
Trusted vs. Untrusted Networks

**Trusted Network**
- Administered by a known person or entity
- Data is usually safe to travel transparently
- Examples:
  - ISP/Tier 1 Networks
  - Work Network
  - Home Network

**Untrusted Networks**
- Unknown by whom or if is administered
- If used, sensitive data must be encrypted
- Examples:
  - Public/Shared WiFi
  - Open WiFi – no password
Rouge Networks

• Malicious Wi-Fi Access installed on or near another network
• Designed to fool you into connecting
• May have a similar name/password as legitimate network
• May use common public name to fool your computer into connecting
• Often don’t require a password
Encrypted Data

Transport Encryption – Logon information to website

Tunnel Encryption – VPN Connection
Untrusted Public WiFi – No Password
Untrusted Public WiFi – With Password
Untrusted Public WiFi – With VPN
Virtual Private Networks (VPN)

- Creates Encrypted “Tunnel”
- Prevents Eavesdropping
- Prevents Redirection/Replay Attacks
- Helps with privacy
- Access secured resources remotely
### Public Wi-Fi Best Practices

- **Avoid if possible**
- Don’t join a network without a password
- Verify name and password with staff
- Don’t save the Wi-Fi network to your computer
- Use a VPN connection for any sensitive data
# What VPN to Use?

## VPN Services
- Fee to use
- Simple and easy setup
- May be included with other security offerings/features

## DIY VPN
- Setup free on your home network
- Difficult to setup and manage
- May be a feature of your home router/WiFi
- Access to home network remotely

## Work VPN
- Provided by work
- IT support
- Traffic monitoring/limitations for personal use
Protecting Your Home Network
Internet (servers of Quora, Google, Wikipedia, etc.)

Modem (located in your house and provided by your ISP)

Router (routes incoming and outgoing data; often both wired and wireless)

Wireless laptop

Wireless smartphone

Wired printer

Wired computer
Firewalls

A device of software that filters network traffic

Type
Source/Destination

Wi-Fi Router Firewalls
Built into most consumer Wi-Fi Routers
Pre-configured to filter all incoming-traffic

Personal Firewalls
Additional device with more features and functionality

Operating System Firewalls
Only protects one computer
Good extra layer of security
Home Wi-Fi Security

Passwords
- Change default router password
- Set a Wi-Fi Password
  - All data is transparent without one
  - Only share with trusted individuals

Wi-Fi Security Methods
- WEP
  - Old security standard
  - Easily cracked
- WPA/WPA2
  - Current standard
Protected Your Networked Devices

PCS
SMART PHONES
INTERNET OF THINGS (IOT)
Personal Computers

- OS Firewalls
  - Protect from incoming attacks
  - Protect unwanted outgoing communications
- Updates
  - Protect from vulnerabilities
  - Fix bugs
  - New Features
- Anti-virus
  - Keep up to date
- Only run trusted applications
- Set up a password and auto lock your computer
Smart Phones

• Updates
  • Protect from vulnerabilities
  • Fix bugs
  • New Features
• Anti-virus
  • Keep up to date
• Only run trusted applications
  • Only use the app store
• Setup up a password/PIN/etc
  • Auto lock your device
IoT Security

• Change default passwords (if possible)
• Turn off any features you don’t need
• Only use approved applications to control
• Update device when possible
• Review permissions of devices and limit when possible