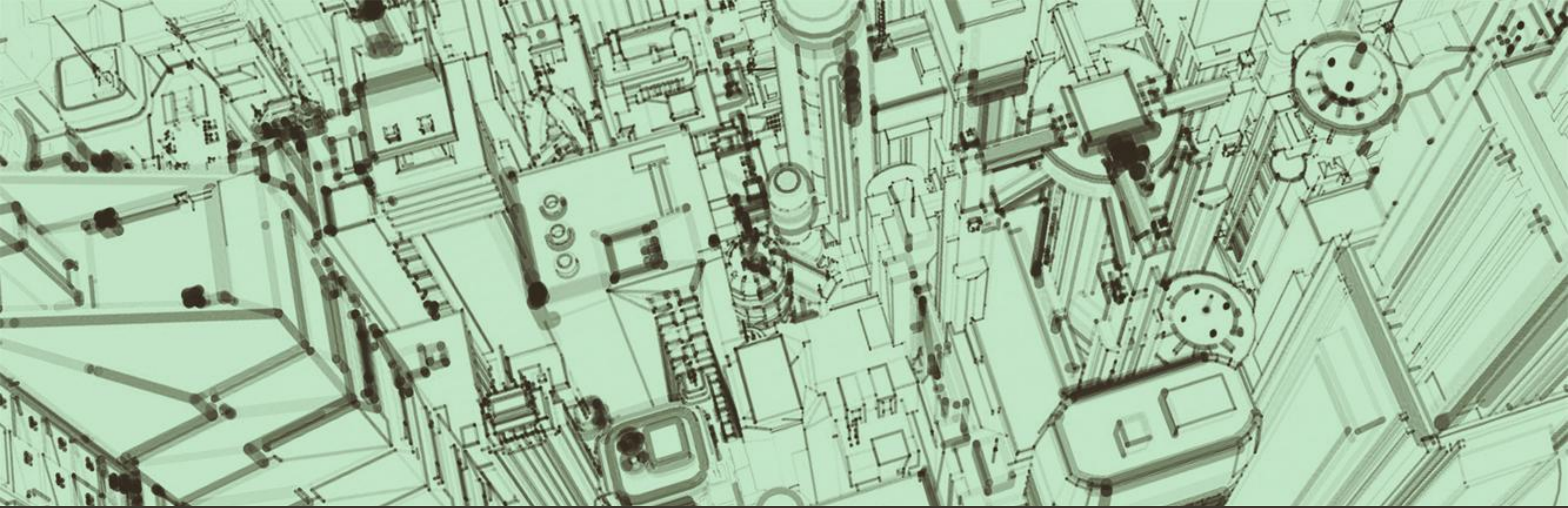
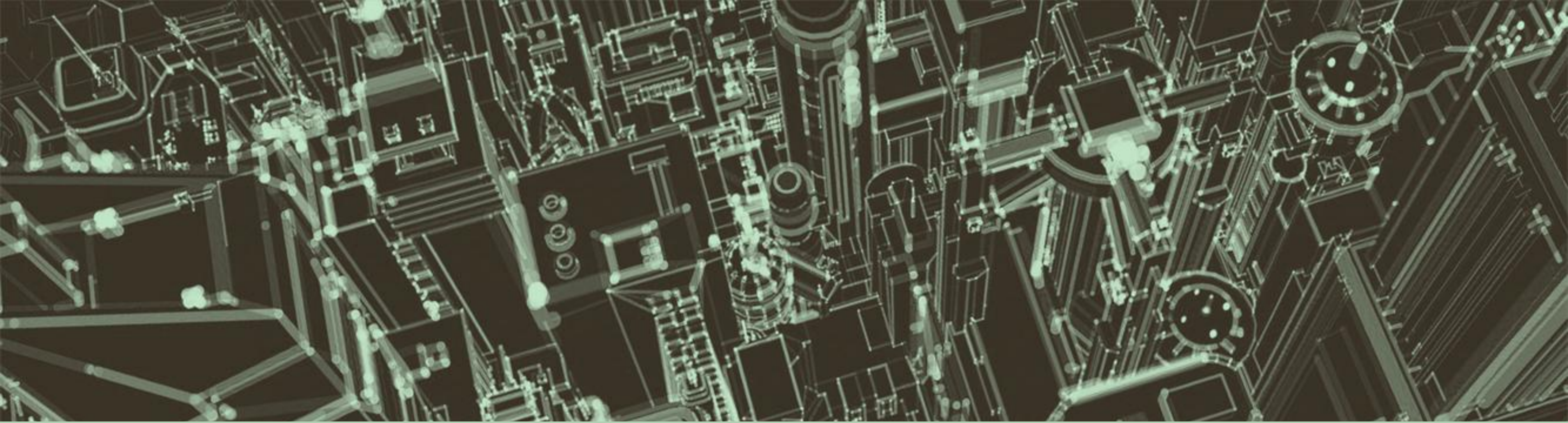
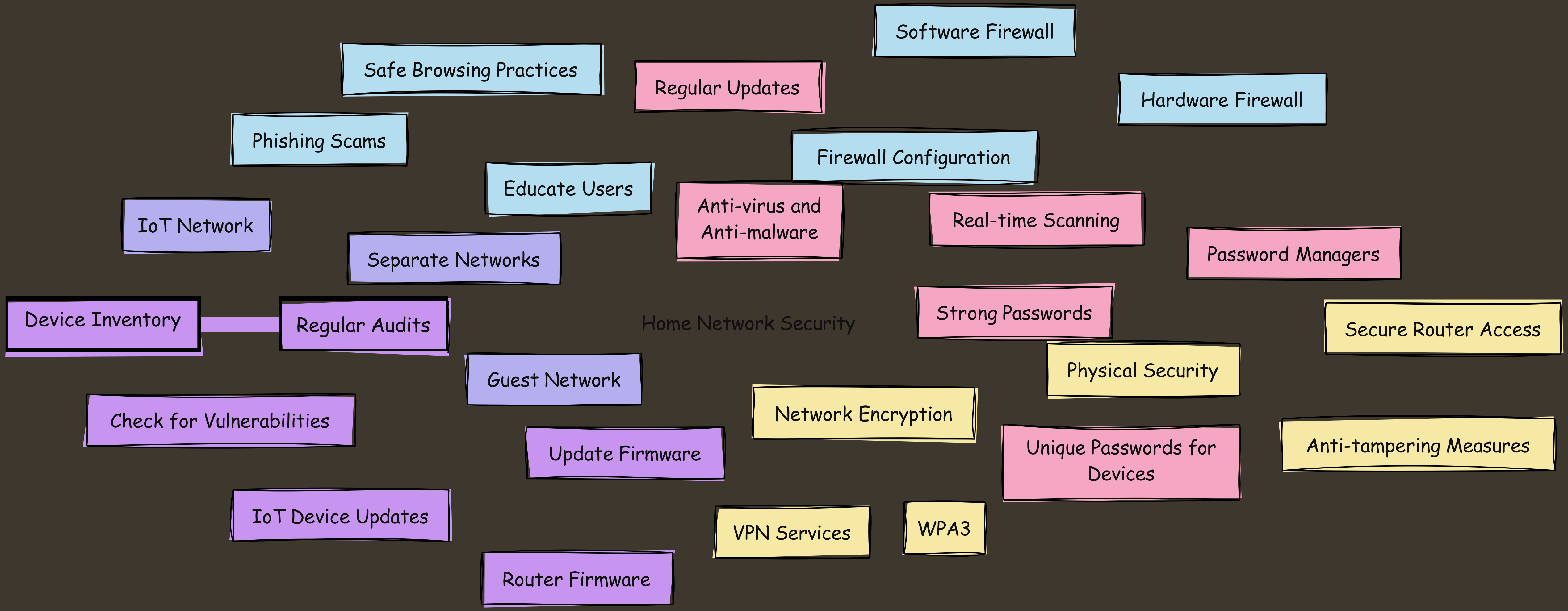


Securing Your Home Internet

Stephen Pinn



Privacy .vs. Security



Home Network Security

Software Firewall

Safe Browsing Practices

Regular Updates

Hardware Firewall

Phishing Scams

Firewall Configuration

Educate Users

Anti-virus and Anti-malware

Real-time Scanning

IoT Network

Password Managers

Separate Networks

Device Inventory

Regular Audits

Strong Passwords

Secure Router Access

Physical Security

Guest Network

Check for Vulnerabilities

Network Encryption

Update Firmware

Unique Passwords for Devices

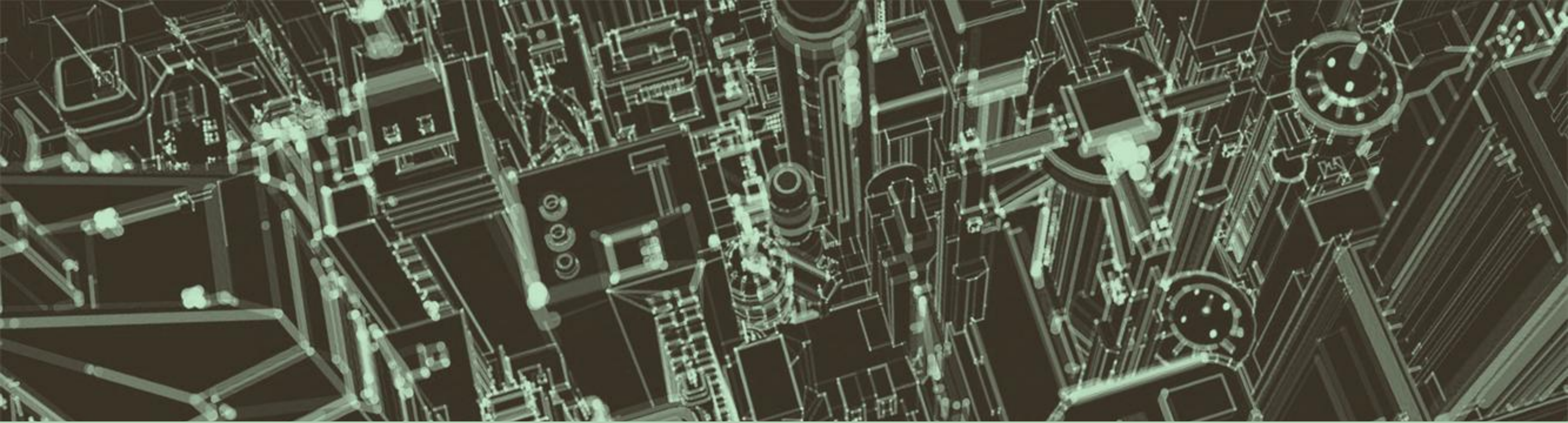
Anti-tampering Measures

IoT Device Updates

VPN Services

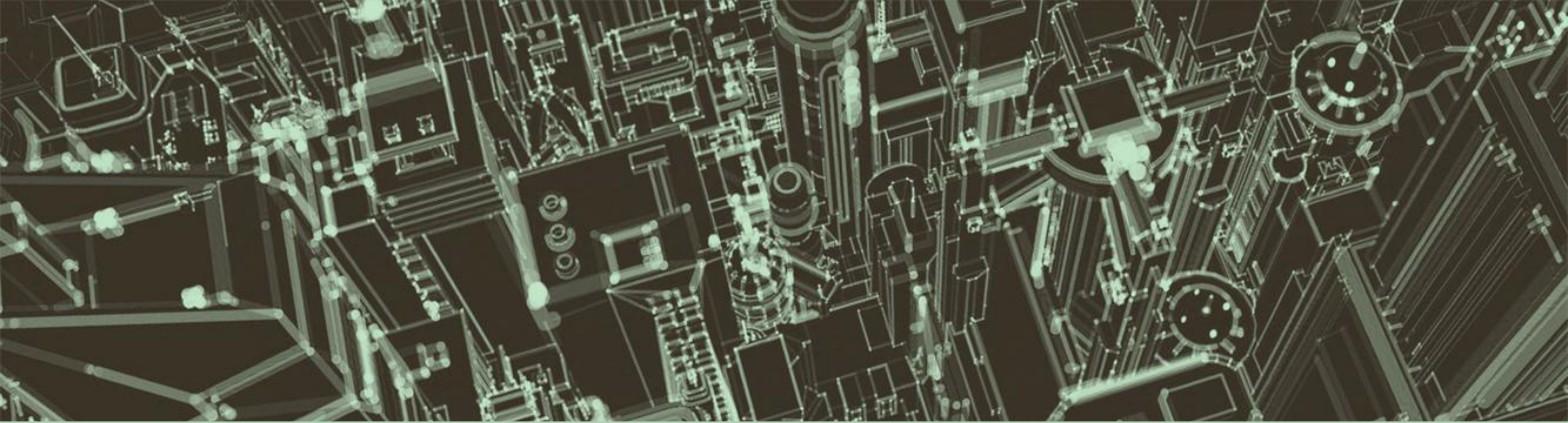
WPA3

Router Firmware



Our Objectives

- Keep Our Network Safe
- Not Become Network Administrators
- Try and Remember Everything



Fortress Home

~ Landscape of Threats

~ Building Your Defenses

~ Securing Your Router

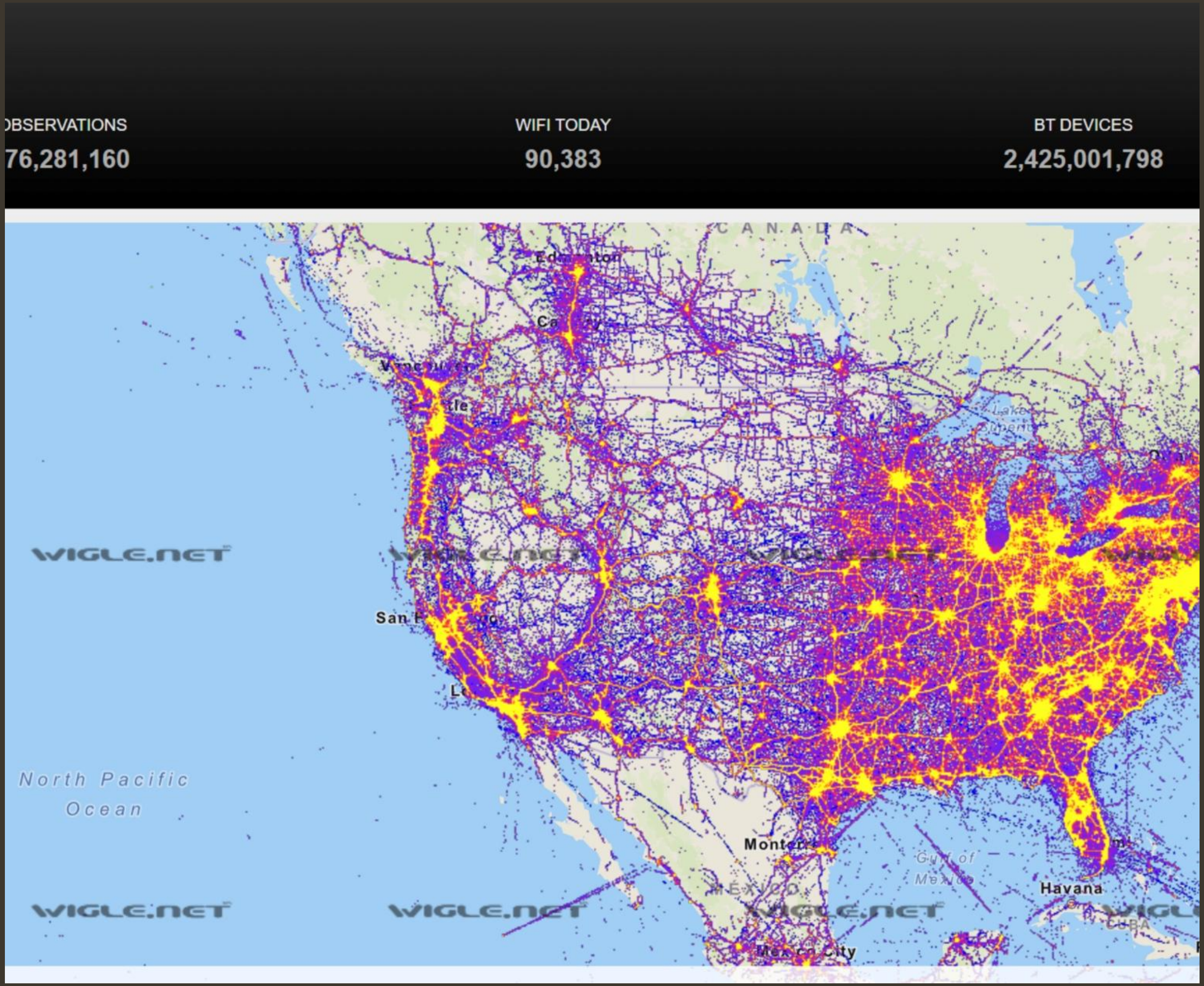
~ Guest (and IOT) Networks

~ Smart Device Security

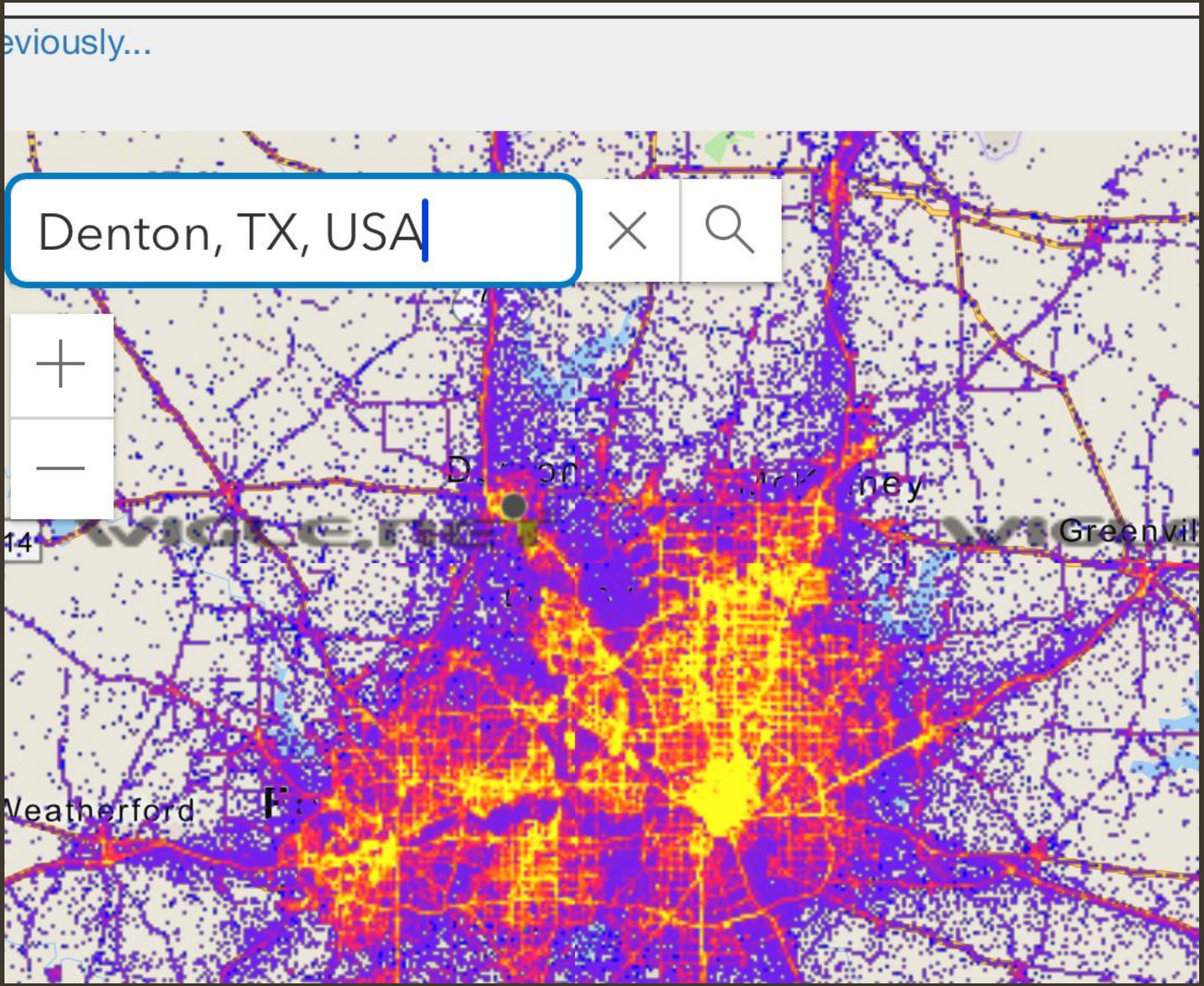
~ Phishing Awareness

~ Questions / Discussion

An Area Rich in Targets



BSERVATIONS	WIFI TODAY	BT DEVICES
76,281,160	90,383	2,425,001,798



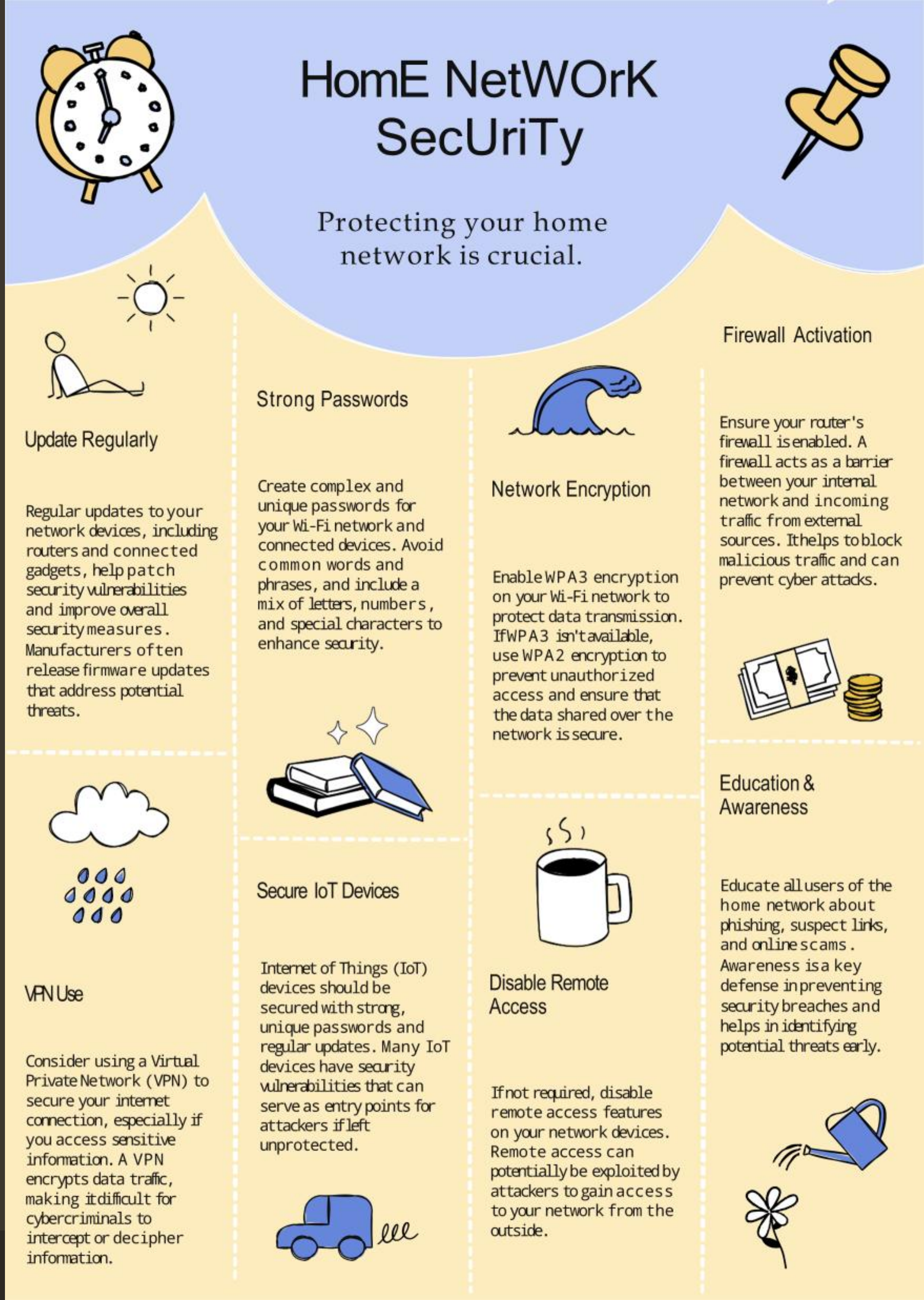
An Area Rich in Targets

Points and Types of Attacks

- Malware
- Phishing
- Man in the Middle
- Unsecured Networks
- DNS Poisoning

Securing Your Router

- Router Components
  - Modem (Gateway)
  - Access Point
  - Switch
  - Firewall
- All in One or Individual



HomE NetWOrK SecUriTy

Protecting your home network is crucial.

Update Regularly

Regular updates to your network devices, including routers and connected gadgets, help patch security vulnerabilities and improve overall security measures. Manufacturers often release firmware updates that address potential threats.

VPN Use

Consider using a Virtual Private Network (VPN) to secure your internet connection, especially if you access sensitive information. A VPN encrypts data traffic, making it difficult for cybercriminals to intercept or decipher information.

Strong Passwords

Create complex and unique passwords for your Wi-Fi network and connected devices. Avoid common words and phrases, and include a mix of letters, numbers, and special characters to enhance security.

Secure IoT Devices

Internet of Things (IoT) devices should be secured with strong, unique passwords and regular updates. Many IoT devices have security vulnerabilities that can serve as entry points for attackers if left unprotected.

Network Encryption

Enable WPA3 encryption on your Wi-Fi network to protect data transmission. If WPA3 isn't available, use WPA2 encryption to prevent unauthorized access and ensure that the data shared over the network is secure.

Disable Remote Access

If not required, disable remote access features on your network devices. Remote access can potentially be exploited by attackers to gain access to your network from the outside.

Firewall Activation

Ensure your router's firewall is enabled. A firewall acts as a barrier between your internal network and incoming traffic from external sources. It helps to block malicious traffic and can prevent cyber attacks.

Education & Awareness

Educate all users of the home network about phishing, suspect links, and online scams. Awareness is a key defense in preventing security breaches and helps in identifying potential threats early.

Secure Your Router

- Change Default Password and Username*
- Use WPA2 encryption as a Minimal (WPA3)
- Disable Remote Access
- Keep Router Firmware Updates
- Enable SPI, IDS and IPS if Available
- Disable WPS
- Monitor Connected Devices
- Limit DHCP Leases

Build Your Defenses – Strong Passwords

- Mix Upper and lower Cases
- Avoid Using Personal Information
- Unique Passwords for Each Account
- Consider a Password Manager
  - Must be portable
- Authentication / Dual Factor / Biometric

Guest Networks

- Provides Limited Access to Main Network
- Protects your Main Network SSID Info

Smart Devices

- Update Device Firmware Routinely
- Enable 2FA Where Available
- Setup a Separate VLAN if Possible
- Firewall Rules for Operation

Phishing Awareness

- Current Phishing Scams
- Treat Unsolicited Email and Messages with Caution
  - How to look at URLs
- Verify Website Authenticity Before Entering Sensitive Data
- Using and Understanding VPNs

Channels For Further/Deeper Information

- Dave’s Garage
- Network Chuck
- Techno Tim
- Crosstalk Solutions
- NMTV (Naomi Rockwell)
- ……