Deep Dive Information Security Questionnaire

Introduction: This questionnaire is designed to gather detailed information about specific aspects of your home network and security setup. The information you provide will help us develop a comprehensive security strategy tailored to your needs. Please answer the following questions to the best of your knowledge.

---

1. Smart Home Security

1. **IoT Devices**:

   o List all IoT devices (smart speakers, lights, thermostats, cameras, etc.) in your home, including brand and model:

   ---

   o Do you regularly update the firmware on these devices? If yes, how often?

   ---

   o Are these devices segmented on a separate network? If yes, please describe the segmentation:

   ---

   o Have you changed the default passwords on all IoT devices? Please provide details:

   ---

   o How do you manage IoT device access and control (e.g., mobile app, web interface)?

   ---

   o Do you use any voice assistants (e.g., Alexa, Google Home)? If so, how are they configured for privacy and security?

   ---

   o Are there any IoT devices that you've chosen not to connect to the internet for security reasons? If yes, please describe:

2. **Smart Home Hub**:

- o Do you use a smart home hub? If yes, please provide details (brand, model, firmware version):

- o How is the smart home hub secured (e.g., strong password, regular updates, two-factor authentication)?

- o Have you configured any custom security settings on the smart home hub? If yes, please describe:

---

2. Wi-Fi Security

1. **Network Configuration**:

- o How many Wi-Fi networks (SSIDs) do you have, and what are they used for (e.g., main network, guest network, IoT devices)?

- o What type of encryption is used on your Wi-Fi network (e.g., WPA3, WPA2)?

- o Do you use a Wi-Fi analyzer tool to check for unauthorized devices or interference? If yes, which tool?

- o Have you configured your Wi-Fi network to automatically disconnect inactive devices?

- o Do you use Wi-Fi 6 (802.11ax) or Wi-Fi 6E? If so, are you utilizing any of its enhanced security features?

- o Have you enabled WPA3 on your network if supported by your devices?

2. **Access Control**:

   o Do you use MAC address filtering, access control lists (ACLs), or other methods to restrict access? If yes, please describe:

   o How often do you change your Wi-Fi password?

   o Do you use any advanced Wi-Fi security features (e.g., hidden SSID, band steering, client isolation)?

3. **Guest Network**:

   o Do you provide a guest network for visitors? If yes, how is it configured and secured (e.g., separate VLAN, limited access)?

   o How do you manage and monitor access to the guest network?

3. Internet Security

1. **Router and Modem**:

   o What brand and model of router and modem are you using? Include firmware version if known:

   o Do you regularly update the firmware on your router and modem? If yes, how often?

   o Have you changed the default login credentials for your router and modem? If yes, please provide details:

- o Do you have remote management enabled on your router or modem? If yes, how is it secured?

---

2. **Firewall and DNS**:

- o Have you configured any custom firewall rules? If yes, please describe:

- o Are you using a secure DNS service (e.g., NextDNS, Cloudflare)? If yes, please provide details and any custom configurations:

---

3. **VPN Usage**:

- o Do you use a VPN service? If yes, please provide details (provider, devices used on, VPN protocol):

- o Is the VPN always on or used only on specific occasions? Describe the use cases:

---

4. **Browser and Email Security**:

- o What web browsers do you use, and do you have any security extensions installed (e.g., ad blockers, anti-tracking)?

- o How do you secure your email accounts (e.g., two-factor authentication, encrypted email services)?

---

5. **Network Monitoring**:

- o Do you use any network monitoring tools or intrusion detection systems? If yes, please describe:

- o Have you configured any parental controls or content filtering on your network? If yes, please describe:

---

4. Physical Security

1. **Device Security**:
   - o Are your important devices (e.g., computers, routers) physically secured (e.g., locked rooms, anti-theft devices)?

   - o How do you physically secure your networking equipment (e.g., in a locked cabinet, restricted access area)?

---

2. **Home Security Systems**:
   - o Do you have a home security system (e.g., cameras, alarms)? If yes, please provide details (brand, model, storage method):

   - o Are the security system devices connected to your network? If yes, how are they secured (e.g., VLAN, firewall rules)?

---

3. **Access Control**:
   - o Who has physical access to your network equipment and important devices?

   - o Do you have policies in place for managing physical access (e.g., visitor logs, restricted areas)?

---

4. **Environmental Controls**:
   - o Do you use any environmental controls to protect your devices (e.g., surge protectors, UPS, climate control)?

5. **Device Disposal**:

   o Do you have a plan for securely disposing of old devices that may contain sensitive data? If yes, please describe:

6. **Camera Configuration**:

   o Are your security cameras configured to avoid capturing private areas of neighboring properties? If yes, please describe:

5. Additional Security Measures

1. **Backup and Recovery**:

   o What is your backup solution (e.g., cloud backup, external drives)? Please describe the setup and software used:

   o How often are backups performed and tested? Describe your backup and recovery testing process:

2. **Security Awareness**:

   o Have you received any security awareness training? If yes, please describe the content and frequency:

   o Do you follow any specific security practices (e.g., phishing awareness, secure browsing)? Please provide examples:

3. **Incident Response**:

   o Do you have an incident response plan in place? If yes, please describe the plan and any roles/responsibilities:

- o Have you experienced any security incidents in the past year? If yes, please describe the incident, impact, and your response:

4. **Regular Security Audits**:

   - o Do you conduct regular security audits or assessments? If yes, please describe the frequency and scope of these audits:

   - o Have you used any third-party services for security assessments? If yes, please provide details:

5. **Password Management**:

   - o Do you use a password manager? If so, which one and how is it secured?

6. **Multi-Factor Authentication**:

   - o Have you enabled multi-factor authentication on all accounts that support it? If yes, please describe:

7. **File Encryption**:

   - o Do you use any encryption for sensitive files stored on your devices or in the cloud? If yes, please describe:

8. **Automatic Updates**:

   - o Have you enabled automatic updates on all devices and software where possible? If yes, please describe:

6. Mobile Device Security

1. **Mobile Devices**:

    o   How do you secure your mobile devices that connect to your home network? Please describe any measures in place:

    _____

    o   Do you use any mobile device management (MDM) solutions? If yes, please describe:

    _____

    _____

7. IoT Device Lifecycle Management

1. **End-of-Life Handling**:

    o   How do you handle the end-of-life for IoT devices, especially those that are no longer receiving security updates? Please describe:

    _____

    _____

8. Network Segmentation

1. **VLAN Implementation**:

    o   Have you considered implementing VLANs for different types of devices (e.g., work devices, personal devices, IoT)? If yes, please describe:

    _____

    _____

9. Smart TV and Streaming Device Security

1. **Device Security**:

    o   How do you secure your smart TVs and streaming devices? Please describe:

    _____

    o   Do you use any ad-blocking or privacy-enhancing features on these devices? If yes, please describe:

    _____

10. Home Office Security

1. **Work from Home**:

   o If you work from home, what additional security measures do you have in place for your work devices and data? Please describe:

---

11. Cloud Service Security

1. **Cloud Services**:

   o What cloud services do you use (e.g., Google Drive, Dropbox), and how do you secure access to these services? Please describe:

---

12. Third-party Access

1. **Access Management**:

   o Do you allow any third-party services or individuals (e.g., cleaners, pet sitters) access to your home network or smart home devices? If so, how do you manage this access? Please describe:

Closing: Thank you for providing this detailed information. Your responses will help us create a comprehensive security strategy tailored to your specific needs. We will review your answers and get back to you with our recommendations and next steps.