# CYB 320 SWOT Analysis Worksheet Personal Security and Home Technology

Perform a SWOT analysis on your personal security practices for the technology within your home; each quadrant must contain between five and seven items.

| Strengths | Weaknesses |
| --- | --- |
| 1. **High-End Desktop:** My main desktop's advanced features and capabilities make it a robust tool for managing security and other tasks efficiently, this is what I use for school and any work objectives. 2. **Diverse Technology Ecosystem:** The variety of devices (PCs, smart TVs, printers, gaming consoles) allows for flexible usage scenarios and entertainment options. 3. **Wi-Fi Connectivity:** Centralized internet access facilitates easy and consistent online activities for all devices and users in the home. 4. **Awareness of Security:** My awareness of the need for security in personal technology practices, which I try explaining every day to everyone in the home but no one gets it(much like managers at big companies). 5. **Multiple Users:** The diversity of users I try to share responsibility for security and maintaining device integrity. 6. **Physical Security:** good physical security practices are in place. 7. **Dedicated Devices for Users**: Having separate PCs for different family members can limit the spread of potential security issues between users. | 1. **Limited Security Knowledge Among Some Users:** Grandparents’ lack of security and computer knowledge could lead to vulnerabilities, which is an unfortunate event I deal with daily; they are 80 and set in their ways. 2. **Shared Wi-Fi Network**: All devices on one network can lead to vulnerabilities if one device is compromised, but being a home network there isn’t much of a choice. 3. **Lack of Specialized Security Software on All Devices:** Some devices do not have up-to-date antivirus or other security measures like my desktop does, because spite the concern others refuse to pay for such software with the attitude “it will never happen to me” like most the planet has. 4. **Inconsistent Security Practices:** Different users might have varying levels of diligence regarding security practices. 5. **Potential for Unsecured Smart Devices:** Smart TVs and gaming consoles might not be regularly updated or secured against vulnerabilities, and these products are just that because most of the time that is just how they are and will always be a risk. 6. **Physical Security Risks:** The high value of my desktop could make it a target for theft, but I’d fight someone first. 7. **Dependency on a Single Router/Modem:** A single point of failure for the entire network's security and functionality that I think about daily, but again it’s a home network without much choice in the matter. |
| Opportunities | Threats |
| 1. **Educating Users:** Providing security training for all users, especially grandparents, to reduce vulnerabilities. Is an everyday task, most of the time everyone gets annoyed by my concerns and refuse to believe how dangerous the internet really is. 2. **Network Segmentation:** Implementing a guest network or separate networks for different types of devices to enhance security. 3. **Upgrading Security Software:** Ensuring all devices have the latest security software installed and are regularly updated. 4. **Implementing Strong Password Policies:** Enhancing the security of all devices and accounts with strong, unique passwords and using a password manager. This is something I have started doing, saves lives. Which is why I added it here. 5. **Physical Security Enhancements:** Investing in better physical security measures for high-value items. 6. **Regular Security Audits:** Periodically reviewing and updating security practices and device settings. 7. **Adopting Two-Factor Authentication:** For all sensitive accounts and services accessed through home devices, and every account online this is now a must. | 1. **Phishing Attacks:** The risk of phishing attempts targeting less knowledgeable users, leading to potential security breaches. 2. **Malware and Ransomware:** The potential for malware or ransomware infections, especially on less-protected devices. 3. **Network Intrusions:** Risks associated with unauthorized access to my home network. 4. **Device Theft or Damage:** Physical risk to high-value items like the my main desktop. 5. **Outdated Device Software:** Vulnerabilities due to outdated firmware/software on smart TVs, gaming consoles, and printers. 6. **Social Engineering Attacks:** Targeted attempts to exploit user trust or lack of knowledge. 7. **Wi-Fi Eavesdropping:** Potential for eavesdropping on my Wi-Fi network, especially if it is not properly secured. |