# 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 |
| --- | --- |
| All computers require a password to login and have password complexity.    I can respond fast to a security threat by not having to wait for approval.    All computers in my home have the latest security updates.    The SSID is not a default password by Internet Service Provider, instead it is a custom one with password complexity.    The router is in an area where if anyone tried to access it without approval they would be spotted. | Computer Browser remembers passwords and will autofill.    There is no software installed to monitor the network traffic.    I am the only member at home with decent knowledge of technology.    The SSID for the router is not hidden.    There are no browser restrictions stopping people from going to a malicious site. |
| Opportunities | Threats |
| Requiring password complexity for logging into computers could be enhanced by changing the password once a month, making it even harder for attackers to crack.    Teaching the rest of my family how to manage technology safely will minimize the attack surface for attackers.    All computers in my home should be automatically updated and checked to see if they are for a hardened security posture.    The SSID could be hidden to increase the security of the network as this will help by not letting attackers brute force attack as easily because they would first have to find out network.    The router should be kept in a cabinet and locked to make access harder for an attacker, as it is already in a spot that is impossible to get to without being spotted. | If an attacker were to penetrate the computer they could easily get into all accounts, because of the autofill for passwords linked to all our accounts.    If an attack were to happen such as a DDoS (Distributed Denial of Service) attack, we would not know because there is no software installed to monitor the network.    If I am not at the house when an attack happens there will be no response to stop it.    The SSID not being hidden extends the accessibility of an attack by making it easier for attackers to find the network and plan an attack.    No browser restrictions from malicious sites means if there is malware, trojan horse, or spyware installed no one will know and damage can be done. Again, the attack surface is larger due to this threat. |