

Name _____

Fortify Your Fortress: Securing Your Home Wi-Fi Network

Open-Ended Response Answer Key

1. To create a strong Wi-Fi password, I would follow these steps:
 - Use a combination of uppercase and lowercase letters, numbers, and symbols.
 - Avoid using common phrases, dictionary words, or easily guessable information like names or birthdays.
 - Make the password at least 12 characters long.
 - Use a mix of unrelated characters to increase complexity.
 - Ensure the password is unique and not used for other accounts.
2. Not updating your router's firmware regularly can pose security risks as it may contain vulnerabilities that cybercriminals can exploit to gain unauthorized access to your network. These vulnerabilities can be used to launch attacks or compromise the security of connected devices. Keeping the firmware up to date is crucial to patch these vulnerabilities, enhance network security, and ensure that the router benefits from the latest security features and improvements.
3. Disabling remote management features on your router is important for security. Remote management allows access to your router's settings from outside your network, which can be exploited by attackers. By disabling this feature, you prevent potential entry points for cyber threats and reduce the risk of unauthorized access or tampering with your router's configuration.
4. Enabling a guest network on your router offers security advantages by segregating guest devices from your main network. Guests have limited access, reducing the risk of unauthorized access to your devices and data. However, it also adds complexity to network management, as you may need to set up additional passwords and access controls for the guest network. Careful configuration and monitoring are necessary to maintain security while providing guest access to the internet.

