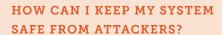**PLUG INTO SAFETY**

SMART HOME SECURITY SYSTEMS
BRING PEACE OF MIND

Smart home security systems can be wonderful additions to keep your loved ones and valuables safe. They also can be easy targets for attackers if they're not properly protected and updated regularly.

SMART HOME SECURITY RISKS

It's vital to ensure your smart home security systems are protected. If not, here are some of the main risks that come with unprotected smart home devices, according to NordVPN:

- **Data and identity theft:** Unprotected smart home accessories can store sensitive data that hackers can steal.

- **Device hijacking:** An attacker can take over control of a smart device, use your security cameras, or break your smart locks.

- **Man-in-the-middle attacks:** An attacker can intercept communication between two of your devices and can take control of them, and possibly install malware.

- **Distributed denial-of-service attacks:** An attacker can overload your device with multiple fake requests.

- **Permanent denial-of-service attacks:** An attacker can permanently damage your device to make it useless.

HOW CAN I KEEP MY SYSTEM SAFE FROM ATTACKERS?

You can take steps to ensure your safety with these systems by keeping your devices updated and using security measures like data encryption and two-factor authentication. You should also:

- **Secure your Wi-Fi router:** It should be password-protected with a strong level of encryption.

- **Be smart with your passwords:** Make them challenging to figure out, and don't reuse them.

- **Keep your devices up-to-date:** Regularly check and install firmware updates to improve security.

- **Try to find devices with enhanced security features:** Buy devices with these features and make sure you enable them.

These actions can help keep your private information safe while keeping your home secure.