CSNP
CYBERSECURITY NON-PROFIT

Smart Home Security Guide

Protecting your family in the connected home

CHAPTER 1

Understanding Smart Home Risks

Smart devices bring incredible convenience to family life, but they also create new security vulnerabilities. Each connected device is a potential entry point for hackers, and many come with default settings that prioritize ease of use over security.

The good news? With a few simple steps, you can dramatically improve your family's digital safety while still enjoying all the benefits of your smart home.

Common Vulnerabilities

- Weak default passwords
- Unencrypted data transmission
- Outdated firmware

What's at Risk

- Personal conversations
- Video footage of your home
- Daily routines and schedules

CHAPTER 2

Securing Smart Speakers

Smart speakers like Alexa and Google Home are always listening for their wake word, which means they're processing audio in your home 24/7. While major brands have strong security, proper configuration is essential.

01

Review voice recordings regularly

Both Amazon and Google allow you to review and delete voice recordings through their apps.

02

Disable purchasing by voice

Prevent accidental or unauthorized purchases by requiring a PIN or disabling this feature entirely.

03

Mute when discussing sensitive topics

Use the physical mute button during private family conversations or financial discussions.

04

Enable multi-factor authentication

Add an extra layer of security to your Amazon or Google account to prevent unauthorized access.

CHAPTER 3

Smart Cameras & Doorbell Security

Video doorbells and security cameras provide peace of mind, but they also capture intimate details of your family's life. Securing these devices is critical to preventing unauthorized access to your home's video feeds.

- **Use unique, strong passwords**

  Never use the default password. Create a password with at least 12 characters combining letters, numbers, and symbols.

- **Enable two-factor authentication**

  This prevents hackers from accessing your cameras even if they obtain your password.

- **Keep firmware updated**

  Enable automatic updates or check monthly for security patches from the manufacturer.

- **Review sharing permissions**

  Regularly audit who has access to your camera feeds and revoke unnecessary permissions.

CHAPTER 4

Smart TV Privacy Settings

Automatic Content Recognition

ACR tracks everything you watch to serve targeted ads. Disable this feature in your TV's privacy settings to prevent data collection.

Microphone & Camera

Many smart TVs have built-in microphones and cameras. Disable them when not in use or cover the camera with removable tape.

Limit Data Sharing

Navigate to privacy settings and opt out of sharing viewing data with third parties and advertisers whenever possible.

CHAPTER 5

Smart Toys & Baby Monitors

Internet-connected toys and baby monitors require extra vigilance since they're used in the most private spaces of your home—your children's rooms.

Research before buying

Check reviews and look for toys with strong security features and positive privacy track records.

Register products

Registration ensures you receive security updates and recall notices directly from manufacturers.

Monitor baby monitor access

Change default passwords immediately, use encrypted connections, and regularly check who has access.

CHAPTER 6

Network Segmentation Strategy

One of the most effective security measures is creating separate networks for different types of devices. This isolation prevents a compromised smart device from accessing your computers, phones, or sensitive data.

1

Main Network

Computers, phones, tablets with sensitive information

2

Guest Network

Smart home devices, IoT gadgets, entertainment systems

3

Kids Network

Children's devices with parental controls and time limits

Most modern routers support creating multiple networks. Check your router's admin panel or contact your internet provider for setup assistance.

CHAPTER 7

Essential Privacy Settings Checklist

Change All Default Passwords

Replace factory passwords with unique, strong passwords for every device. Use a password manager to keep track.

Enable Two-Factor Authentication

Add this extra security layer to every account that supports it, especially video cameras and smart locks.

Turn On Automatic Updates

Keep all devices current with the latest security patches by enabling automatic firmware updates.

Review Privacy Settings

Disable unnecessary data collection, opt out of marketing programs, and limit third-party sharing.

Audit Device Access

Regularly review which family members and apps have access to each device and remove old permissions.

Secure Your Router

Use WPA3 encryption, change the default admin password, and disable remote management features.

Your Family Security Checklist

Use this comprehensive checklist to secure your smart home. Tackle one section at a time—even small improvements make a big difference in protecting your family's privacy.

Initial Setup

- Change all default passwords
- Enable two-factor authentication
- Create separate networks
- Register all devices
- Review privacy policies

Quarterly Reviews

- Update all passwords
- Review sharing permissions
- Check privacy settings
- Remove unused devices
- Test security cameras

Monthly Tasks

- Check for firmware updates
- Review camera footage access
- Audit connected devices
- Delete old voice recordings

Annual Actions

- Full security audit
- Replace outdated devices
- Update router firmware
- Review insurance coverage

Remember: Perfect security doesn't exist, but consistent effort creates strong protection for your family.

Cybersecurity Non-Profit (CSNP)

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Business & Non-Profit Security

Family Cybersecurity

Kids Safety

Senior Digital Safety

Women's Security

Parents & Educators

> **Everything we offer is completely free.**

Visit csnp.org

Access Free Resources