

TVs, streaming & smart home | Medium | 2 min read

Smart home safety: updates, strong passwords and two-step sign-in

Smart TVs, speakers, plugs, cameras and doorbells are all connected to your home network. Like computers and phones, they need looking after to stay safe. A few simple habits make a big difference.

Keep everything updated

1. Turn on automatic updates in the device or its app, if it has the option.
2. Check the app now and then for update notices.
3. Update the apps on your phone that control the devices.
4. Replace devices when the maker stops providing updates, as they can become unsafe.

Use strong, different passwords

- Each account for a smart device, such as Ring, Amazon, Google or Apple, should have its own password.
- A good password is three or four random words together, with a few numbers or symbols.
- Never reuse your email password.
- Change any default password that came with a camera or device.

A password manager on your phone can remember them all for you.

Turn on two-step sign-in

Two-step sign-in, also called two-factor authentication or 2FA, asks for a code when you sign in on a new device. Even if someone gets your password, they cannot get in without the code.

1. Open the app or account page for the device maker.
2. Look for **Security**, **Account** or **Sign-in settings**.
3. Choose **Two-step verification**, **2FA** or similar.
4. Pick a text message or an authenticator app, and follow the steps.

Protect your Wi-Fi

- Use a strong Wi-Fi password.
- Do not share your main network with visitors. Many routers have a guest network.
- Keep the router updated too.

Be careful with cameras and microphones

- Check where cameras point, and avoid bedrooms and bathrooms.
- Turn off microphones or cameras when not needed.
- Review who has access to your account and remove anyone who should not.

When to get more help

Get in touch if you see sign-in alerts you did not expect, a device doing things you did not ask for, or you are unsure how to make a device safer. Change your password straight away if you think someone has your account.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.