# Video conferencing services: using them securely

**How to set up and use video conferencing services, such as Zoom and Skype, safely and securely**

The increased use of video conferencing technology in recent years mean many of us are now using video calls to stay in touch with family, friends and work colleagues. If you're new to video conferencing, this guidance will help you to use these services safely.

Even if you're familiar with video conferencing, we recommend you take a moment to check how you're using it.

> **Note**
> If you're using (or setting up) video conferencing services to use within your organisation (or using these services to work from home), please refer to our separate guidance for organisations.

---

## In this guidance:


- What is video conferencing?
- Downloading video conferencing software
- Setting up video conferencing services
- Hosting and joining calls


---

## What is video conferencing?

Video conferencing is a live audio and video conversation between 2 or more people in different locations, conducted using phone, tablet, laptop or desktop computer. Some video conferencing services also allow you to share files, pictures, or each other's screens.

Many devices have video conferencing functionality built in (such as Apple's FaceTime and Google's Duo), and many popular apps also provide this service (such as Instagram, WhatsApp and Facebook). There are also standalone video conferencing apps that you can download; popular titles include Zoom, Skype, Houseparty and Microsoft Teams.

Regardless of the type of service you use, this guidance is applicable to all video conferencing services. For more information about the security features of a specific service, please refer to the service providers' **official** support site.

---

## Downloading video conferencing software

If you're downloading standalone video conferencing software, make sure that you:

- **Only download the software from trusted sources**. This means using your phone or tablet's app store (such as Apple's App Store or Google Play), or downloading the software from the service provider's **official** website. Be wary of following advertised links at the top of search results pages (they will typically include the word 'Ad' at the beginning of the address or description of the website), and adverts for video conferencing software within websites. These may contain links to sites that are not always legitimate, and can be used to scam people. You should also treat any unsolicited links you receive that refer to video conferencing software with caution.
- **Check online to understand what app is right for you**. In most cases, the 'free' version of a video conferencing service will provide good enough functionality and security for personal use, provided you've set it up correctly. Premium versions of the same product may offer additional features and usability. You should consider paying for these versions if you

feel you'd benefit from extra features. With so many products available, you may want to carry out your own research beforehand - using tech websites or other trusted sources - to find out which one is right for you.

- **Check the privacy settings**. You should make sure that you understand what (if any) data the service will access during operation. You may have the option to opt out of sharing data.

---

## Setting up video conferencing services

Before making your first call, you should:

- **Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password**. If you need to install the video conferencing app, you'll have to create an account for it. Make sure that the password you use is different to all your other passwords, and difficult for someone to guess (we explain how to do this here). You should also set up 2-step verification (2SV) for the account (and for your device and other apps if available), as this provides an extra layer of protection and can stop criminals accessing your accounts (even if they know your password).
- **Test the service before making (or joining) your first call**. Most services have a 'test' function to ensure your microphone and camera work correctly, and that your internet connection is fast enough. You can also use the test function to learn how the service works. As a minimum, make sure you know how to mute your microphone and turn off the camera. This will give you more control over what you share with others.
- **Understand what features are available**. Many services allow you to record the call, share files, or show what is on somebody's screen. Find out how to tell if the call is being recorded, what exactly is recorded (audio, pictures, messages), and who can access the recordings. There may also be additional controls to manage who can join the call.

---

## Hosting and joining calls

It's important that you can control who can join your video conferencing call. For specific instructions, refer to the support website of the service you're using. However, the following general rules apply:

- **Do not make the calls public**. Connect directly to the people you want to call using your contacts/address book, or provide private links to the individual contacts. For some video conferencing services, you can set up the call so that a password is required in order to join. This adds another layer of protection. Do not post the link (or the password) publicly.
- **Know who is joining your call**. If you are organising the call for your family or friends consider using the lobby feature to ensure you know who has arrived. This is especially useful if individuals are joining the call via an unrecognised phone number. Make sure people are who they say they are before they join the call (the password function described above can help with this).
- **Consider your surroundings**. Take a moment to think about what your camera shows when you're on a call. Would you want to share that information with strangers? Consider blurring or changing your background - you'll find instructions on how to do this on the support website for your video conferencing service.

Finally, make sure that **all** your devices and applications (not just the video conferencing software) are kept up to date. Applying software updates is one of the most important things you can do to protect yourself online. Update all the apps (and your device's operating system) whenever you're prompted. It will add new features and immediately improve your security.

---

## Further advice for parents

Parents looking for more advice on keeping children safe chatting online will find plenty of information from our colleagues at the National Crime Agency at the following websites:

- Video chatting – a guide for protecting primary school age children *(external link)*
- Video chatting – a guide for protecting secondary school age children *(external link)*

**PUBLISHED**

21 April 2020

**REVIEWED**

21 April 2020

**VERSION**

1.0

**WRITTEN FOR**

Self employed & sole traders

You & your family