Video conferencing
Using services securely

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, the tips below will help you to use it safely. Even if you're familiar with video conferencing, you should take a moment to review how you're using it.

@NCSC @cyberhq ncsc.gov.uk National Cyber Security Centre

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.

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 and Microsoft Teams.

For more information about the security features of a specific video conferencing service, please refer to the service provider's official support site. The service provider's website can also help if you have any problems whilst using the service.

Downloading a video conferencing software

- If using standalone video conferencing software, only download it from trusted sources (such as Apple's App Store or Google Play), or from the service provider's official website.
- Use tech websites and other trusted sources to research what app is right for you. The 'free' version of a video conferencing service will provide good enough security for personal use, provided you've set it up correctly.
- 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 a video conferencing services

- Make sure that the password for your video conferencing account (or for the device or app you are using for video conferencing) is different to all your other passwords, and difficult for someone to guess. If available, set up 2-step verification (2SV) for the account (and for your device and other apps, if available).
- Test the service before making (or joining) your first call. Check that your microphone and camera work and that your internet connection is fast enough. Learn how to mute your microphone and how to turn off the camera.
- Many services allow you to record the meeting, share files, or show what is on somebody's screen. Find out how to tell if the call is being recorded

Hosting and joining calls

- Do not make calls public. Connect directly to the people you want to call using your contacts/address book, or provide private links to the individual contacts. If possible set up the call so that a password is required to join.
- Consider using the lobby feature to ensure you know who has arrived. Make sure people are who they say they are before they join the call, the password function described above can help with this.
- 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.

Keep all devices and applications up to date

- 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.

National Cyber Security Centre
a part of GCHQ