SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit

NHS England and NHS Improvement

Video Conferencing

With many people now having to work from home and wanting to keep in contact with family and friends, there has been an increase in the use of video conferencing software. If not done securely, video conferencing can come with cyber security risks.

We want you to be able to continue working and keeping in touch with family and friends as securely as possible to protect yourself, your family, and the NHS.

Choosing a service

There are two different scenarios for video calling, **work** and **personal**.

There are a few different considerations for both.

At Work

If you need to video call at work you should firstly consider the video conferencing tools available to you which have been approved by your IT team. These will have been vetted and approved for use when talking about work.

There are occasions when you may be invited to calls or webinars on conferencing tools which have not been approved by your IT team. You should never install software or programs which have not been approved.

In these cases, it is best to contact your IT service desk and talk to them about your requirements and why you need access to a particular software. They will be able to advise you whether it is safe to use, or what other options may be available to you.

At Home

Keeping in contact with friends and family is increasingly important, both to ensure that they are alright, and for our own wellbeing. You may consider using video conferencing software to do this.

If you don't currently have a platform you use, for example a social media platform, you may be considering downloading a new one. If this is the case there are a few things you may want to consider:

- Do your research and find a reputable provider who meets your requirements
- Check the basic security controls – does the software offer the security you require?
- Read the terms and conditions, and understand how they use and store your data
- Check the permissions the software needs, and only accept what you want it to have access to (microphone and camera)

Configuring video conferencing software

Once you have decided on the best platform for you to use, you need to ensure that it's configured as securely as possible. Alternatively, if you are attending a conference held by someone else, there are still some steps you can take to protect yourself:

- If you have to create an account, use a password which is strong, unique and not easily guessed
- If the option is available, enable two-factor authentication (2FA)
- Always apply updates to video conferencing software when available

If you are hosting a conference:

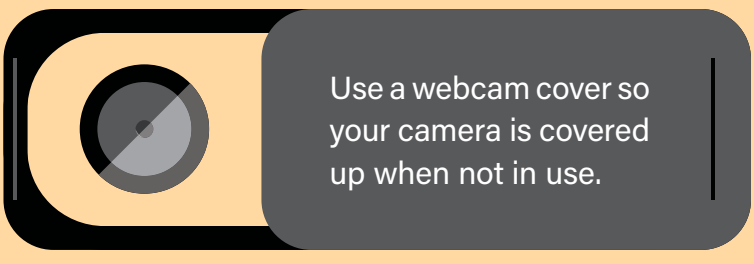
- If possible, put a password on the session
- Some platforms allow you to create a guest list, or create a 'waiting room' where you can only allow who you want in
- Do not advertise the link and password on public sites, instead, send e-mails of details directly to attendees
- Control who can present and share files during the conference call - only permit those who really need to
- If possible, mute attendees by default and only unmute them when they need to speak

Other Top Tips

If you receive an e-mail or notification inviting you to a video call that you aren't expecting, don't click on the link.

Verify whether the communication is genuine first by contacting the person or organisation.

STOP and THINK before replying or clicking on anything.



Consider your environment.

Remove any sensitive work documents or personal items you don't want others to see.

For more information on securely using video conferencing software, see the National Cyber Security Centre (NCSC)'s guidance at https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely