

North East Regional Special Operations Unit Notification



NERSOU | *Protecting communities
from organised crime*
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT

Video conferencing services



The COVID-19 lockdown means many of us are now using video calls to stay in touch with family, friends and work colleagues.

Here's how to set up and use video conferencing services, safely and securely...



Downloading video conferencing software...

- 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.
- Check online to understand what app is right for you
- Check the privacy settings. Make sure that you understand what data the service will access during operation. You may have the option to opt out of sharing data.



Setting up video conferencing services...

- Make sure your video conferencing account is protected with a strong password. You should also set up two factor authentication (2FA) for the account
- Test the service before making (or joining) your first call. As a minimum, make sure you know how to mute your microphone and turn off the camera.
- Understand what features are available. Find out how to tell if the call is being recorded, what exactly is recorded (audio, pictures, messages), and who can access the recordings.



Hosting and joining calls...

- 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.
- Know who is joining your call. If you are organising the call for your family or friends consider using the lobby feature
- Consider your surroundings. Think about what your camera shows when you're on a call
- Make sure that all your devices and applications (not just the video conferencing software) are kept up to date.

For more info on video conferencing visit:

<https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely>

If you have been a victim of fraud or cyber crime, report it to Action Fraud

Action Fraud
Report Fraud & Internet Crime
0300 123 2040