CYBER AWARE

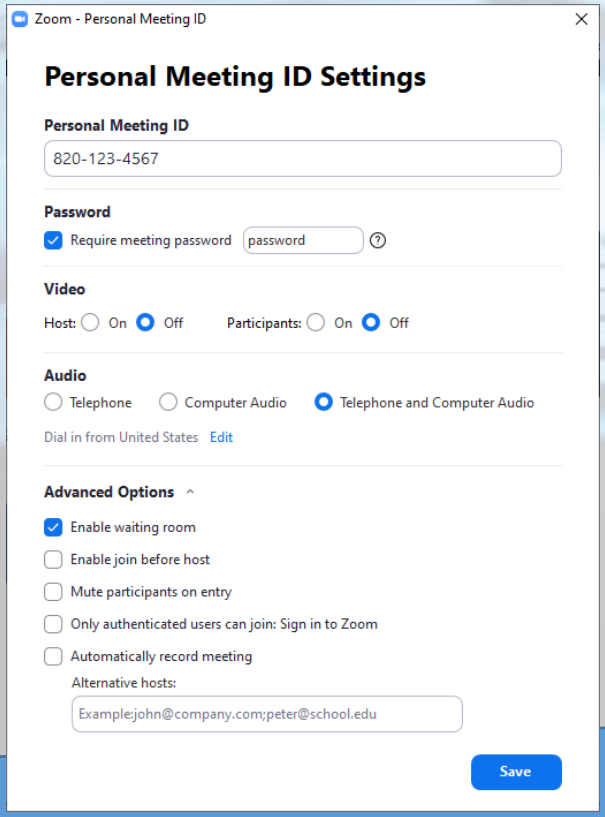
The ‘Zoom Bomb’ phenomenon

Surrey & Sussex CCU Newsletter – May 2020

Since the start of the Covid 19 lockdown, people have needed to find alternative ways to communicate with friends and family. Many are using Zoom – a popular video conferencing application that has seen a meteoric rise in popularity since the pandemic began. Unfamiliar users can leave themselves vulnerable to ‘Zoom Bombing’ where uninvited users gain access to the meeting for nefarious purposes. This guidance has been prepared following a particularly unpleasant incident that took place in Sussex.

How do you use Zoom?

The Zoom app is available on a multitude of devices, enabling communication between a range of devices. Subscribers can use a paid-for licenced version or a free version which has some restrictions. Upon registration, users are allocated a Personal Meeting ID (or PMI) which they can use to host meetings. It is not necessary to register with Zoom to participate in a meeting – all you need is the meeting ID which is made available by the host and the Zoom software. If inadequate settings are applied to the meeting, it may be vulnerable to Zoom Bombing. As a result, the host must take some basic precautions.



What precautions should I take?

Before starting the meeting, hosts should ensure the following settings are applied: -

Make the meeting private.

This can be done in 2 ways – (1) by requiring a password to access the meeting and (2) by using the ‘Waiting Room’ to control the admission of participants. In the latest version of the Zoom software, the default setting for the ‘Waiting Room’ feature is set to ‘enabled’ and passwords are also issued by default.

Manage your participants.

Remember – links to meetings (invitations) should only be sent to those individuals you wish to participate.

Consider other options like video and audio use and set your requirements accordingly.

contd…

Useful Links

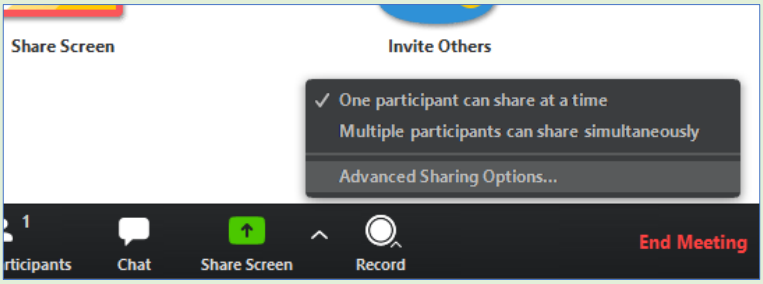
SEROCU: www.serocu.police.uk/organisations

NCSC: www.ncsc.gov.uk

CYBER AWARE

When you have created the meeting, it is important to review additional security options. These are particularly important if you are hosting a public or open meeting.

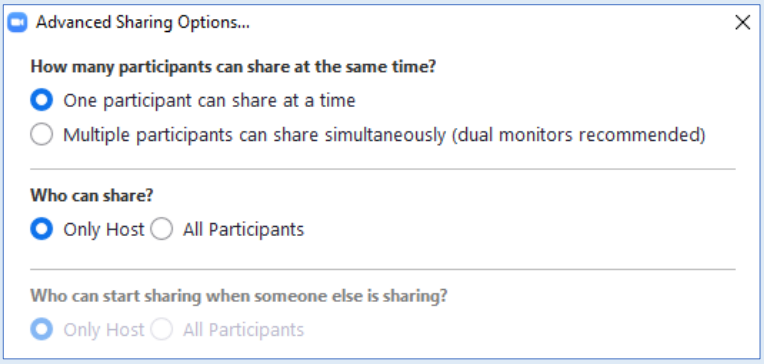
To prevent 'Zoom Bombing' you will need to set some options for **participants** and **screen sharing**. Moving your mouse over the meeting window will show the options bar at the bottom of the window. From here you can access the 'Share Screen' menu. Click 'Advanced Sharing Options…'



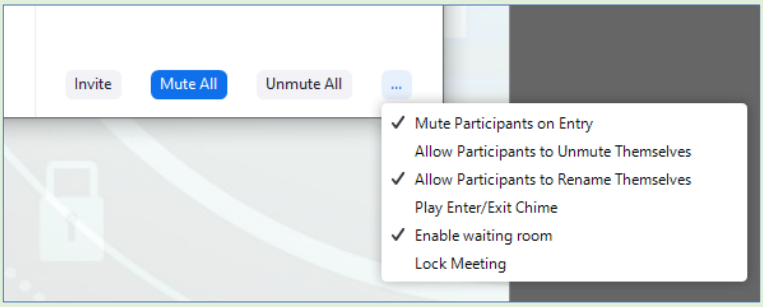
In the 'Advanced Sharing Options…'window, under the section 'Who can share?' select the option 'Only Host' and close the window.

This will ensure that no other participants can share any part of their screen with the meeting.

Use the 'Share Screen' icon on the main Zoom window to select what you wish to share in the meeting.



Now, select 'Manage Participants'. A new window will appear to the right of the main 'Zoom' application where you can see details of participants. To change settings, click the button with three dots in the bottom right corner of the screen. To prevent unwanted audio interruptions, select 'Mute Participants on Entry' and deselect 'Allow Participants to Unmute Themselves'.



Remember, you can also record meetings in Zoom. This may assist law-enforcement in the event of criminal activity taking place during your meeting – but please ensure participants are aware of any recording being created. Please also familiarise yourself with the other Zoom options.

Visit the Zoom website for more information: https://zoom.us/docs/en-us/covid19.html

Useful Links

SEROCU: www.serocu.police.uk/organisations

NCSC: www.ncsc.gov.uk