Zoom security considerations for camera clubs

There has been a lot of negative press around Zoom security issues. A lot of this is "old news" as well as the usual sensationalising by the media. There have been a number of reported incidents of "Zoom bombing" or hijacking of Zoom meetings for mischievous or even sinister purposes and some governments and enterprises have already banned the use of Zoom. It is therefore understandable that some clubs and members will have concerns over the security in Zoom.

Zoom has been quick to respond to criticism and security concerns and had, in fact, addressed many of the issues even before they had been reported publicly. They have made and are continuing to make significant improvements to the security features in the Zoom clients and infrastructure. We should also consider that the security requirements for camera clubs or federations are hardly the same as a national government or the UN!

Zoom now has a wide range of features that can be applied to secure your Zoom meeting

- Zoom encrypts all network traffic to secure against eavesdropping. An upgrade of the encryption algorithms to state-of-the-art is being rolled out with the latest upgrade. Although Zoom does not currently support end-to-end encryption in the strict sense this is true of most other video conferencing platforms in their normal setting. In any event the protection offered is more than sufficient for our usage.
- The Zoom account can be set up to limit which data centres are used for a Zoom session. So you can now exclude routing through China for instance (the vast majority of our sessions are routed through Europe anyway)
- The Zoom meeting host now has a security tab that groups a number of useful features together
- A waiting room can be set up for a meeting so that would-be attendees can be vetted by the host before admission. The waiting room is now enabled by default
- The host can remove an attendee and prevent them from re-entering or simply put them "on hold"
- The host can lock a meeting after it has started to prevent anyone else from joining
- Passwords can be set for the meeting so that it is only possible to join if you have the meeting link or the meeting ID and password. The meeting password is now the default setting
- Sharing can be controlled by the host to prevent others from sharing or to allow only specific individuals to share. Participants can make annotations while someone else is sharing. This feature can also be disabled
- The host can mute all or selected participants
- The host can disable chat
- Zoom has enforced upgrades of the client applications to ensure that the latest security features are implemented on users' devices

There have been concerns that Zoom collects and resells user data. It is fair to say that their privacy policy was previously poorly worded and led some to report that Zoom were playing fast and loose with your personal data. The current privacy policy is quite clear and comprehensive and can be found at https://zoom.us/privacy.

You do not need a Zoom account to join a Zoom meeting. Only the host needs to have one. So, even assuming that Zoom was harvesting personal data you are not supplying information such as your email address, phone number or even real name to Zoom. There have been reports that Zoom on

IoS collects information from your Facebook profile if you use Facebook to log in. This was fixed several updates ago. There have been no further such issues that we are aware of.

Different types of meetings have different security requirements. Basingstoke Camera Club has, to date, run 12 successful online meetings of different types:

1 committee meeting
3 remotely judged competitions
1 external speaker presentation
1 AV presentation
2 photo clinics
3 photography training sessions
1 virtual aperitif party

We generally make the sessions as open as possible. We have started to use passwords but we give the link to members and this includes the embedded encrypted password, allowing them to join with a single click. We never disclose meeting IDs in the public domain. We do not use the personal meeting ID – a unique ID is generated for each meeting. We are experimenting with selling tickets to online events using Eventbrite and the guest only receives the link once they have paid. We encourage guests to use their real names as handles when joining to avoid being removed from a session because they are not recognised by the host.

We use the waiting room to hold early arriving participants in presentations and competitions while we brief the speaker/ judge but generally disable it and admit all once we are ready. So far we haven't found the need to lock any meetings to allow entry for late arrivals and have not had problems so far.

We usually allow anyone to share but only the host being able to start sharing while someone else is sharing. This is sufficient to prevent someone else hijacking the session. For photo clinics (where a group share each other's images for critique) it is beneficial that anyone can share and annotate and, again, we have not experienced any problems so far.

Chat can be useful to ask questions silently during a presentation but we have started to disable it for competitions as it is distracting. We have not disabled chat for security reasons.

For competitions it is advisable that the person running the competition software is not also the host. The latter needs to be free to monitor guest activity – muting individuals, checking late joiners, possibly removing unidentified guests, etc

In summary, Zoom security has received intense scrutiny and the company has been impressively active in addressing issues and improving security capabilities. It seems likely that as a result of all this attention Zoom will soon be one of the most secure video conferencing platforms available. Zoom already offers a wide range of security related features are at the disposal of the meeting host. A pragmatic approach is needed on the part of the host to maintain security in a meeting, but Zoom security is more than adequate for camera clubs and federations.

Stewart Lacey
President Basingstoke Camera Club
May 2020