Zoom and data protection: what's all the fuss about?

Popular video chat app Zoom is facing questions over various aspects of its data protection practices. The service has exploded in popularity in recent weeks, being used by workplaces, friends, schools and even the UK government.

At LOROS, we don't advocate the use of Zoom video conferencing; if people do have to use video conferencing methods for work reasons, we ask you to use Microsoft Teams.

However, inevitably in rare circumstances this may have been used where there was no alternative to conduct a meeting – or, you may like me, use Zoom from home to contact friends, family and others on a personal level, on your own PCs, laptops or your own mobile devices.

So I just thought it might be a good idea to let you know what all the fuss has been about recently in terms of privacy concerns. And to give advice that you can use at home. Please remember that it is NOT LOROS policy to use Zoom for work.

1. One concern stems from the fact that when a user downloads the iOS app and opens it on their phone, it communicates with Facebook, sending information such as the model of the user's device, where they are connecting from, what phone network they are on and a special unique code that can be used to identify the device.

2. A separate concern is the default settings of the service, meaning trolls can cause problems. Trolls, known as zoombombers, have used the screensharing feature to broadcast pornography and violent imagery. This is because each Zoom call has a randomly generated ID number between 9 and 11 digits long that's used by participants to gain access to a meeting. Researchers have found that these meeting IDs are easy to guess and even brute forceable, allowing anyone to get into meetings.

3. In addition, security experts have said the file transfer feature that is switched on by default could be used to spread malware.

4. Zoom also claimed that they were using end-to-end encryption for the meetings, and it has turned out that actually that was not true.

Zoom said that they "take the security of Zoom meetings seriously and we are deeply upset to hear about the incidents involving this type of attack. For those hosting large, public group meetings, **we strongly encourage hosts to review their settings and confirm that only the host can share their screen**."

How else have Zoom responded?
They have chosen to enable passwords on your meetings and turn on Waiting Rooms by default as additional security enhancements. We recommend that you ensure that at your meetings, only hosts can share their screen, and that you follow the guidance below in terms of passwords and 'waiting rooms'.

All meetings will have password enabled. If your attendees are **joining by clicking a meeting link with a password embedded, there will be no change to their joining experience.** For attendees who join meetings by manually entering a Meeting ID, they will need to enter a password to access the meeting. To locate your meeting password, log in to your account, visit your **Meetings** tab, select your upcoming meeting by name, and copy the new meeting invitation to share with your attendees. For step-by-step instructions, please watch this **2-minute video** or **read this FAQ**.

For instant meetings, the password will be displayed in the Zoom client and the password is also embedded in the meeting join URL by default.

Virtual Waiting Room Turned on by Default

Going forward, the **virtual waiting room feature** will be automatically turned on by default. The **Waiting Room** is just like it sounds: It's a virtual staging area that prevents people from joining a meeting until the host is ready.

How do I admit participants into my meeting?

It's simple. As the host, once you've joined, you'll begin to see the number of participants in your waiting room within the **Manage Participants** icon. Select **Manage Participants** to view the full list of participants, then you'll have the option to admit individually by selecting the blue **Admit** button or all at once with the **Admit All** option on the top right-hand side of your screen. For step-by-step instructions, please watch this **1-minute video**.

Check out these resources to learn **How to Manage Your Waiting Room** and **Secure Your Meetings with Virtual Waiting Rooms.**

For more information on how to leverage passwords and Waiting Rooms to secure your meetings, please visit our **Knowledge Center**, attend a **daily live demo**, or visit our **blog**.