HOW TO SECURE YOUR ZOOM MEETINGS

The security vulnerabilities of popular videoconferencing platform Zoom have come to light in the transition into full-force remote work, leaving many organizations to ban its use for meetings. However, Zoom remains the preferred platform choice for several industries, including the legal industry, due to its exclusive features that more secure options like Microsoft Teams don't offer.

Luckily, there are several steps that your organization can take if you're obliged to use Zoom. Taking these precautions should give you some peace of mind in knowing that you're using the platform in the most secure way possible.

There are several steps that can be taken to increase the security of any meeting using Zoom (LawPro, 2020). Keep in mind that many of these steps are only applicable to paying Zoom customers. They include...

1. Make sure you use a password to lock your meeting, and do not embed it into the automated Zoom email invitation. Instead, send it in a separate email or message to your invitees.
2. Disable the "join before host" option in your Zoom waiting room, which will allow you to let invitees in and avoid having any individuals not scheduled to be in the meeting enter.
3. Use the "lock the meeting" function once all invitees have entered the meeting. This will prevent others, including Zoom bombers, from joining.
4. Disable the file sharing function available directly on Zoom. Instead, you should only be sharing files through other, more secure file hosting platforms like OneDrive and Dropbox.
5. While some Zoom add-ons may seem tempting such as chats, screen sharing, and whiteboards, don't use them for the sharing of professional or sensitive data. For most professional meetings, this will mean not using add-ons at all.
6. Use a personal meeting ID that is randomly selected by the platform rather than using a custom ID chosen yourself.
7. Use a data center region which the host can select to enhance security so that you don't end up with the system assigning one to your session that is in a less secure region or one that cannot be trusted for its security.
8. If prompted to select a data centre region, select one yourself rather than allowing the system to assign you one. The system may automatically assign you a less secure region.

9. If you choose to record your meeting with permission of all attendees, ensure that you are recording it to a secure server of your choosing and not saving it to Zoom, and consider enabling the recording disclaimer. See how to do that here.

While none of these steps guarantee that your Zoom experience will be entirely secure, they should give you some peace of mind that you've taken the available precautions to protect yourself and your network.

Have Questions?

Contact us at info@gradea.ca, or call us at 613-721-3331.