

Video Conferencing Tips for Organizers

As organizations and individuals rush to work from home (WFH), video conferencing has become a key part of staying connected and working together. However, as this technology is rapidly developing and relatively new for so many, people need guidance on how to use these technologies safely and securely. Here are key tips for securely hosting a video conference.



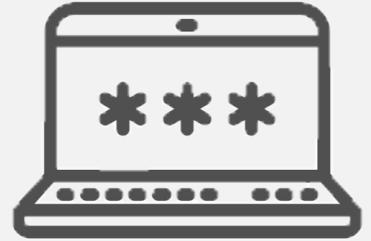
Update software

Make sure you are always using the latest version of the software. New security features and bug fixes are constantly being released. The more recent and updated your software, the more secure you will be. Ensure you are always using the latest version by enabling automatic updating. In addition always quit your program when you are done with it and restart it the next time you want to use it as some teleconferencing software updates every time you restart it.



Require a password for entry

One of the most effective ways to protect the privacy and security of your conference is to require a password for people to join. The password can often be included in the conference invite, making it easy for people to securely join.



Review attendees

Review the people attending your event. If there is someone whom you do not know or cannot identify, have that person confirm their identity. If you have any concerns, remove them from the conference.

Lock the conference

Many solutions offer the option to lock the conference once it has begun so no one else can join unless you manually allow them.



Eliminate disruptions

Remove disruptive or rude participants immediately.

Configure audio/video settings

Set your event's default settings to mute participants' microphones and disable video upon entry. You want everyone muted from the start, then enable audio individually when you want.



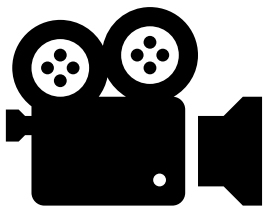


Double-check before you screen share

Exit all other applications and remove any sensitive materials from your computer's desktop. This helps ensure you don't get any distracting pop-ups on your screen or accidentally share any sensitive or embarrassing information while sharing your screen. Consider only sharing the app screen and not your entire desktop.

Clean up your background

If you want to enable your webcam, be aware of what is behind you. Ensure you do not have any sensitive or personal information or family members walking behind you during the call. Some video conferencing software lets you set up your own virtual background or blur your background, so people cannot see what is behind you.



Inform if recording

If you will be recording the event, make sure everyone knows on the call before you start recording.

Disable screenshots

Do not take nor share screenshots of the conference call, you could accidentally share very sensitive information that should not be public. Also, as organizer you may be able to disable screenshots for anyone attending your conference.

