Zoom

Stay safe while connecting virtually with others.

Three essential steps to keeping your Zoom secure and hackers out.

Zoom's ease of use made it easy for troublemakers to "bomb" open Zoom meetings, and Information-security professionals say Zoom's security has had a lot of holes. There's also been scrutiny of Zoom's privacy policies, and how they handle users' personal data, and its encryption policies, which have been more than a tad misleading. That created a backlash against Zoom. In April 2020, New York City public schools moved to ban Zoom meetings, and other school systems did the same, although New York lifted the Zoom ban the following month.

With these issues, it's smart to understand the security and privacy implications of using Zoom. The following tips help to ensure your highest level of privacy and control.

1. Use your browser, not their app.
Join Zoom meetings through your web browser rather than using the Zoom desktop software. The web browser version gets security enhancements faster and doesn't have the permissions an installed app has, limiting the amount of harm it can potentially cause.

2. Require a password to sign-in to meetings.
If you are hosting a Zoom meeting, require meeting participants to sign in with a password. This will make Zoom-bombing much less likely.

3. Set up two-factor authentication.
Be sure to secure your account using two-factor authentication. This security measure requires you to confirm your access using a separate trusted device or service.

! ***When you click a link to join a meeting, your browser will open a new tab and prompt you to use or install the Zoom desktop software, but you don't have to. Look for a link reading "join from your browser" and click that instead.***

When to Zoom and when to give the service a pass.

So, the ultimate question: When should you use Zoom and when should you avoid it? First, it depends on your own risk profile. If you really care about your privacy, and Zoom's policy doesn't sit well with you, you should probably look at an alternative that suits your use of video chatting. Privacy isn't a strong point of many of the video conferencing platforms, including Zoom.

But at the same time, Zoom is highly functional and most of the more secure and private alternatives can't match it. One of Zoom's benefits is the scheduling function for meetings, hence why so many businesses have jumped on it. If data privacy is extremely important to you, then you should probably consider a more secure method of communication. One option, if you care about your privacy and security, but accept there is a bit of a trade off when services are free, is to use Zoom for certain activities and not for others.

Do:

By all means, take that remote exercise class, have a chat with a group of friends or family, or even use it for online learning if the subject matter isn't sensitive. If you use the video conferencing app, you can take steps to secure it. For example, during that exercise class, turn off your camera and mic, and make sure you have a webcam cover.

Don't:

There are, of course, private activities that might make you more cautious about using Zoom. A therapy session, for example, and sensitive government or business meetings should be approached with more caution. If it's a one to one meeting, use a Signal type service, which is end-to-end encrypted but doesn't support group video chats.

PSA: Beware of fake Zoom apps.

The rise in popularity of Zoom has created a market of fake apps, which are actually dangerous malware. Recently, a Kaspersky security researcher found the number of malicious files incorporating the names of popular video conference services, including Zoom, had roughly tripled compared with the previous year.

If you must download the app, you should always go to Zoom's official website to access the correct version for your device. Zoom currently provides direct-download applications for both Mac and Windows, as well as app store links for iOS and Android devices.

Keep things civil.

Some essential tips to help keep your meeting running smoothly.

1. Update your Zoom app.
If using the Zoom app, keep it up to date.

2. Use unique IDs and passwords.
Use unique meeting IDs instead of giving out your assigned Personal Meeting ID (PMI). Additionally, require a password for each meeting.

3. Create a waiting room.
When you create a Zoom Waiting Room, participants can't get into the call until you, the host, lets them in. You can let people in all at once or one at a time, which means if you see names you don't recognize in the Waiting Room, you don't have to let them in. You can also send late participants to the waiting room.

4. Lock a meeting once it starts.
If you start a meeting and everyone you expect has joined, you can lock the meeting from new participants.

5. Own the screen.
Don't let anyone hijack the screen during a Zoom call. To prevent it, make sure your settings indicate that the only people allowed to share their screens are hosts.

6. Create an invite-only meeting.
For paid Zoom accounts, the only way to restrict who can join your Zoom call is to make it an invite-only meeting. That means the only people who can join the call are those you invite, and they must sign in using the same email address you used to invite them.

7. Disable cameras if needed.
Hosts can turn off any participant's camera. If someone is being rude or inappropriate on video, or their video has technical problems, the host can open the Participants panel and click on the video camera icon next to the person's name.

8. Disable file transfers.
In the chat area of a Zoom meeting, participants can share files, including images and animated GIFs—if you let them. If you'd rather not, then disable file transfer. It's on by default, so you have to actively disable it.

9. Manage who can chat.
Typically, other attendees can communicate via private messages. As a host, you can prevent unwanted communication between participants by disabling private chat.

10. Place attendees on hold.
Sometimes, an unruly participant manages to slip through the cracks. As the meeting host, you do have the power to place attendees on hold or remove them.

Advice for Large Meetings

Use these settings for controlling mics in large meetings.

Not all Zoom disruptors are bad actors. Sometimes participants make mistakes and don't realize that a yapping dog or crying child is causing a disturbance for everyone else. Here are two audio settings in Zoom you should review and familiarize yourself with.

Mute participants. As a host, you can mute and unmute an individual participant or everyone all at once.

Mute upon entry. You can also mute everyone automatically when they join a call. This can be done ahead of or during the call.

Zoom Alternatives

Check out these services that may offer more security than Zoom.

Zoom has been in the business for years, but it was only recently that it has exploded in popularity. The video conferencing service has become the go-to venue for personal communication, virtual parties, game events, online classes, travel plans, bible studies, reunions, and more. Given this major user influx, some are worried about how much the service can handle, and the security implications around its use.

Considering this, it's a good idea to keep some alternative services in mind, just in case.

- Cisco Webex
- Google Meet
- GoToMeeting
- Skype Meet Now
- Microsoft Teams
- BlueJeans
- Join.me
- TeamViewer
- Uberconference

Beware the Zapps

Integrated apps may be a privacy risk.

Zapps are third-party applications that integrate into Zoom's existing workflow so users can more easily access information and collaborate while on video calls. Services such as Dropbox, Salesforce, and Slack already have plans to provide such integration. Unfortunately, it's not yet known how access to your personal information is handled from within integrated apps and how much control Zoom users will have in restricting access. Until you learn more, you should be wary of using third-party apps from within Zoom.

Sources:
https://heimdalsecurity.com/blog/home-security-cameras-safety/
https://www.usnews.com/360-reviews/security-cameras/how-to-keep-your-security-cameras-safe
https://www.komando.com/privacy/keep-hackers-out-of-your-security-cameras/704338/
https://www.nytimes.com/wirecutter/reviews/best-security-cameras-for-your-home/
https://techxplore.com/news/2020-07-reveals-privacy-home-cameras.html