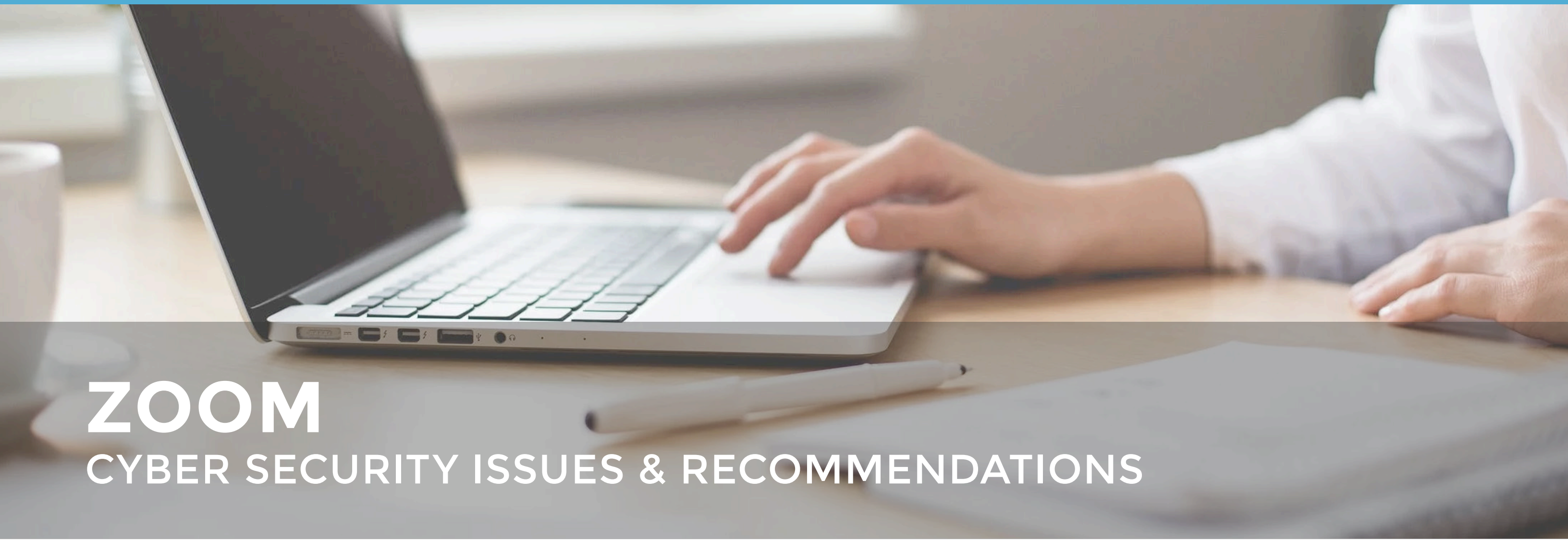


ZOOM

CYBER SECURITY ISSUES & RECOMMENDATIONS

Zoom is a cloud-based enterprise communication platform with over 74,000 customers and 13 million active users. It offers chat, audio, video conferencing, and options to host webinars and virtual meetings online.

While continuing to practice social distancing, several agencies and businesses are using technology to hold important meetings. Children are vulnerable to this hack as many students have switched to online classes due to the novel coronavirus. Daily meeting participants on the platform surged from 10 million in December to 200 million in March. With that popularity came Zoom's privacy risks extending rapidly to massive numbers of people. From built-in attention-tracking features to recent upticks in "Zoombombing" (in which uninvited attendees break into and disrupt meetings with hate-filled or pornographic content), Zoom's security practices have been drawing more attention as well as at least three lawsuits.

Concerns

While the pandemic and resulting shelter-in-place mandates have thrust Zoom into the daily lives of people and businesses, many privacy and cybersecurity concerns have been raised, including allegations of:

- Zoom sending data from users of its iOS app to Facebook for advertising persons, even if the user does not have a Facebook account
- The Windows version of Zoom being vulnerable to attackers who could send malicious links to users’ chat interfaces and gain access to their network credentials
- Zoom not requiring a user’s consent before allowing the host of the meeting to record the session
- The presence of a security flaw that would enable hackers to take over a user’s Mac, including tapping into the microphone and webcamand
- Despite frequently asserting it used “end-to-end encryption for video meetings” which would ensure neither external attackers nor Zoom itself could access the contents of a video meeting, Zoom using only transport encryption for video meetings, meaning Zoom has access to unencrypted audio and video from meetings.

ZOOM CYBER SECURITY ISSUES

Zoom under fire for cybersecurity issues

The popular videoconferencing platform Zoom is struggling to manage the dramatic influx in users and privacy issues as the COVID-19 pandemic drives more people to work remotely, according to The Wall Street Journal.

"Things you just would like to have in a chat and video application — strong encryption, strong privacy controls, strong security — just seem to be completely missing," said Patrick Wardle, a security researcher who previously worked at the National Security Agency.

Zoom says the promised end-to-end encryption will be available in a few months.

"The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language," the bureau's Boston office said this week. As concerns have arisen, Zoom has worked to address them. It published a guide last month on how users can protect meetings. It also changed settings for accounts used by schools and universities to make their meetings more private by default.

https://zoom.us/security

The website Motherboard found that Zoom was sharing data with Facebook, even data on people who are not Facebook users.

Zoom says that was a mistake and that it stopped sharing that data in March, but it's now facing a class action lawsuit.

Zoom CEO Eric Yuan said in a blog post Wednesday that "We recognize that we have fallen short of the community's – and our own – privacy and security expectations," he wrote. "For that, I am deeply sorry, and I want to share what we are doing about it."

Zoom may be easy to use, but people should be wary of its track record. "This product was designed to prioritize things other than privacy and security,"

Zoom: Every security issue uncovered in the video chat app

Here's a timeline of Zoom's rapid rise and the security problems that have come to light.

ZOOM CYBER SECURITY ISSUES

New Zoom Bug Lets Hackers Compromise Windows Credentials

Security researchers claimed that online video meeting platform Zoom is vulnerable to remote attacks.

According to cybersecurity expert Mitch@_g0dmode, Zoom's video conferencing software for Windows is vulnerable to "UNC path injection" flaw that could let hackers steal Windows passwords and execute arbitrary commands on their devices,

The researcher stated that these kinds of attacks are possible because Zoom for Windows software supports remote UNC paths that convert insecure URIs into hyperlinks when received via chat messages.

How Does the Bug Work?

The existence of the vulnerability is also confirmed by security researchers Matthew Hickey and Mohamed Baset, who stated that attackers exploit the process where Windows inevitably exposes a user's login username and NTLM password hashes to a remote SMB server while downloading a file hosted on it. In order to steal passwords, the attacker needs to send a crafted URL (i.e., \\x.x.x.x\abc_file) to a victim via a chat interface. Once the user clicks the URL, it eventually allows the attacker-controlled SMB share to capture the verification data from Windows, without the user knowledge.

Zoom Fixes the Bug

Soon after the vulnerability was identified, the company fixed the issue by releasing a patch. The CEO of Zoom, Eric Yuan, addressed the security issues and stated that a patch has been released to fix the UNC vulnerability. The fix will be pushed out automatically to all the users.

FBI Slams Zoom

Recently, the FBI slammed Zoom for not maintaining proper privacy and security measures for its users. The authorities also warned that the video meeting app is prone to hacking, as it has certain unpatched bugs.

Cybercriminals Target Zoom Domains to Distribute Malware

With majority of the employees working remotely, online communication platforms like Zoom saw a sudden increase in their popularity. According to a report from Check Point, hackers are taking advantage of the rise in

ZOOM CYBER SECURITY ISSUES

Zoom usage by registering fake and malicious Zoom domains. The report stated that around 1,700 new Zoom domains have been registered since the pandemic, with 25% of the domains registered in the past seven days alone.

How to avoid 'Zoombombers' from hacking your virtual conference

"Zoombombing occurs when hackers hijack internet video conferences, like those offered by the fast-growing platform Zoom."

To increase privacy and guard against Zoombombing:

- Create separate passwords for each virtual meeting
- Establish a Zoom waiting room for meeting participants
- Lock down the meeting once everyone invited to attend has joined
- Do not publicly post meeting links on social media or any other public platform

Zoom also offers privacy settings to provide hosts an additional level of protection.

To enable the extra security features, hosts should click on the settings menu, scroll down to “screen sharing,” find “who can share?” Then click on “host only.”

Finally, the user should save the changes. After saving the new preferences, subsequent meetings should enact these enhanced privacy features by default.

The Zoom Timeline

March 26

Motherboard investigation: Zoom iOS app sending user data to Facebook

An investigation by Motherboard revealed that Zoom's iOS app was sending user analytics data to Facebook, even for Zoom users who did not have a Facebook account, via the app's interaction with Facebook's Graph API.

March 27

Zoom removes Facebook data collection feature

ZOOM CYBER SECURITY ISSUES

Responding to concerns raised by the Motherboard investigation, Zoom removed the Facebook data collection feature from its iOS app and apologized in a statement.

"The data collected by the Facebook SDK did not include any personal user information, but rather included data about users' devices such as the mobile OS type and version, the device time zone, device OS, device model and carrier, screen size, processor cores, and disk space," Zoom told Motherboard.

March 30
The Intercept investigation: Zoom doesn't use end-to-end encryption as promised

An investigation by The Intercept found that Zoom call data was being sent back to the company without the end-to-end encryption promised in its marketing materials.

"Currently, it is not possible to enable E2E encryption for Zoom video meetings," a Zoom spokesperson told The Intercept.

Classroom Zoombombings reported

Reporting cases of classroom Zoombombings, including an incident where hackers broke into a class meeting and displayed a swastika on students' screens, led the FBI to issue a public warning about Zoom's security vulnerabilities. The organization advised educators to protect video calls with passwords and to lock down meeting security with currently available privacy features in the software.

Letter from New York Attorney General sent

The office of New York Attorney General Letitia James sent Zoom a letter outlining privacy vulnerability concerns, and asking what steps, if any, the company had put in place to keep its users safe, given the increased traffic on its network.

First class action lawsuit filed

A class-action lawsuit was filed against the company, alleging that Zoom violated California's new data protection law by not obtaining proper consent from users about the transfer of their Zoom data to Facebook.

ZOOM CYBER SECURITY ISSUES

More bugs discovered

After the discovery of a Windows-related Zoom bug that opened people up to password theft, two more bugs were discovered by a former NSA hacker, one of which could allow malicious actors to assume control of a Zoom user's microphone or webcam. Another of the vulnerabilities allowed Zoom to gain root access on MacOS desktops, a risky level of access at best.

April 1

SpaceX bans Zoom

Elon Musk's SpaceX rocket company prohibited employees from using Zoom, citing "significant privacy and security concerns," as reported by Reuters.

More security flaws discovered

Reporting from Motherboard again revealed another damaging security flaw in Zoom, finding the application was leaking users' email addresses and photos to strangers via a feature loosely designed to operate as a company directory.

Apologies from Yuan

Yuan issued a public apology in a blog post, and vowed to improve security. That included enabling waiting rooms and password protection for all calls. Yuan also said the company would freeze features updates to address security issues in the next 90 days.

April 2

Automated tool can find Zoom meetings

Security researchers revealed an automated tool was able to find around 100 Zoom meeting IDs in an hour, gathering information for nearly 2,400 Zoom meetings in a single day of scans, as reported by security expert Brian Krebs.

The discoverable meetings were those left unprotected by passwords, but the tool was able to successfully generate meeting IDs up to 14% of the time, according to reporting from The Verge.

ZOOM CYBER SECURITY ISSUES

More plans for Zoombombing

Motherboard, meanwhile, discovered that 8chan forum users had planned to hijack the Zoom calls of a Jewish school in Philadelphia in an anti-Semitic Zoombombing campaign.

Data-mining feature discovered

The New York Times reported that a data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users.

April 3

Zoom video call records left viewable on the web

An investigation by The Washington Post found thousands of recordings of Zoom video calls were left unprotected and viewable on the open web. A large number of the unprotected calls included discussion of personally identifiable information, such as private therapy sessions, telehealth training calls, small-business meetings that discussed private company financial statements, and elementary school classes with student information exposed, the newspaper found.

Attackers planning 'Zoomraids'

Reporting from both CNET and The New York Times revealed social media platforms, including Twitter and Instagram, were being used by anonymous attackers as spaces to organize "Zoomraids" -- the term for coordinated mass Zoombombings where intruders harass and abuse private meeting attendees. Abuse reported during Zoomraids has included the use of racist, anti-Semitic and pornographic imagery, as well as verbal harassment.

Zoom apologizes, again

Zoom conceded that its custom encryption is substandard after a Citizen Lab report found the company had been rolling its own encryption scheme, using a less secure AES-128 key instead of the AES-256 encryption it previously claimed to be using. In a direct response, Yuan said publicly, "We recognize that we can do better with our encryption design."

ZOOM CYBER SECURITY ISSUES

Second class action lawsuit filed

Tycko and Zavareei LLP filed a class action lawsuit against Zoom -- the second suit against the company -- for sharing users' personal information with Facebook.

Congress requests information

Democratic Rep. Jerry McNerney of California and 18 of his Democratic colleagues from the House Committee on Energy and Commerce sent a letter to Yuan raising concerns and questions regarding the company's privacy practices. The letter requested a response from Zoom by April 10.

April 4

Another Zoom apology

"I really messed up as CEO, and we need to win their trust back. This kind of thing shouldn't have happened," Zoom CEO Eric Yuan told the Wall Street Journal in a lengthy interview.

Surveying the damage to the company's reputation, Yuan described how Zoom pushed for expansion in an effort to accommodate workforce changes during the early stages of the COVID-19 outbreak in China.

April 5

Calls mistakenly routed through Chinese whitelisted servers

In a statement, Zoom admitted that some video calls were "mistakenly" routed through two Chinese whitelisted servers when they should not have been. Certain meetings were "allowed to connect to systems in China, where they should not have been able to connect," it said.

April 6

Some school districts ban Zoom

School districts began banning teachers from using Zoom to teach remotely in the midst of the coronavirus outbreak, citing security and privacy issues surrounding the videoconferencing app. New York's Department of Education urged schools to switch to Microsoft Teams "as soon as possible," Chalkbeat reported.

ZOOM CYBER SECURITY ISSUES

Zoom accounts found on the dark web

Cybersecurity firm Sixgill revealed that it discovered an actor in a popular dark web forum had posted a link to a collection of 352 compromised Zoom accounts. Sixgill told Yahoo Finance that these links included email addresses, passwords, meeting IDs, host keys and names, and the type of Zoom account. Most were personal, but not all.

"One belonged to a major US health care provider, seven more to various educational institutions, and one to a small business," Sixgill told Yahoo Finance.

Zoom seeks to grow its lobbying presence in Washington

Zoom's response to security concerns pivoted to Washington, DC. The company told Politico it was looking to grow its lobbying presence in Washington, and had hired Bruce Mehlman, a former assistant secretary of commerce for technology policy under President George W. Bush.

Urging an FTC investigation

In an open letter, the Electronic Privacy Information Center urged the Federal Trade Commission to investigate Zoom and issue privacy guidelines for videoconferencing platforms.

Sen. Richard Blumenthal, a Connecticut Democrat more recently known for spearheading legislation that critics say could cripple modern encryption standards, called on the FTC to investigate Zoom over what he described as "a pattern of security failures and privacy infringements."

Senator Blumenthal calls for an FTC investigation into Zoom over recent privacy and security issues pic.twitter.com/xuayLVMja2
--Joseph Cox (@josephfcox) April 7, 2020

Third class action lawsuit filed

A third class action lawsuit was filed against Zoom in California, citing the three most significant security issues raised by researchers: Facebook data-sharing, the company's admittedly incomplete end-to-end encryption, and the vulnerability which allows malicious actors to access users' webcams.

ZOOM CYBER SECURITY ISSUES

April 8

Fourth lawsuit

In a lawsuit filed Tuesday in federal court, Zoom shareholder Michael Drieu accused the company of having "inadequate data privacy and security measures" and falsely asserting that the service was end-to-end encrypted. Drieu also said that media reports and public admissions by the company on security problems have caused Zoom's stock price to plummet.

Google bans Zoom

In an email to employees, which cited security vulnerabilities, Google banned the use of Zoom on company-owned employee devices and warned that the software will stop working on those devices this week. Zoom is a competitor to Google's Hangout Meet app.

In an email to BuzzFeed, a Google spokesperson said employees using Zoom while working remotely would need to look elsewhere and that Zoom "does not meet our security standards for apps used by our employees."

Bug bounty hunters emerge

Hackers around the world have begun turning to bug bounty hunting, searching for potential vulnerabilities in Zoom's technology to be sold to the highest bidder. A Motherboard report detailed a rise in the bounty payout for weaknesses known as zero-day exploits, with one source estimating that hackers are selling the exploits for $5,000 to $30,000.

New security advisor and council

Zoom brought former Facebook and Yahoo Chief Security Officer Alex Stamos on board after he defended the company on Twitter. As reported by CNET sister site ZDNet, Stamos said he joined the company as a security advisor after a phone call last week with Zoom founder and CEO Eric Yuan, and that he'll be working with Zoom's engineering team.

In a statement, Zoom announced the formation of a chief information and security officer council and advisory board. The board's goal will be to conduct a full security review of the company's technology and will include, Yuan said, "a subset of CISOs who will act as advisors to me personally."

ZOOM CYBER SECURITY ISSUES

Classroom security

In an email, a Zoom spokesperson told CNET that the company is continuing to push for wider user education on existing security features and explained its move to secure classroom uses of the product.

"We recently changed the default settings for education users enrolled in our K-12 program to enable virtual waiting rooms and ensure teachers are the only ones who can share content in class," the spokesperson said.

"Effective April 5, we are enabling passwords and virtual waiting rooms by default for our Free Basic and Single Pro users. We are also continuing to proactively educate users on how they can protect their meetings from unwanted intruders, including through our offering of trainings, tutorials and webinars to help users understand their own account features and how to best use the platform."

Read more: Zoombombing: What it is and how you can prevent it in Zoom video chat

Usability versus security

In an interview with NPR, Yuan said the balance between security and user-friendliness had shifted for him.

"When it comes to a conflict between usability and privacy and security, privacy and security [are] more important -- even at the cost of multiple clicks," he said. "We're going to transform our business to a privacy-and-security-first mentality."

IDs hidden

The company released a software update aimed at improving security, which removes the meeting ID from the title bar when meetings are taking place. As reported by Bleeping Computer, the move is meant to slow attackers who circulate screenshots of meeting IDs on the open internet.

Weekly webinars

Yuan held the first of Zoom's promised weekly webinars, available on the company's YouTube channel, emphasizing the surge of users working from home due to the COVID-19 pandemic "far surpassed anything we expected."

ZOOM CYBER SECURITY ISSUES

Yuan said that prior to the surge, daily peak use of the product amounted to around 10 million users but that it now amounts to more than 200 million. Yuan also detailed the company's mistakes during the surge: Zoom's user-facing security features aren't friendly enough for the average user, and enterprise-focused tools like its attention-tracking feature don't make sense for privacy-minded average consumers.

Yuan also denied selling any customer data, and he recommended that users engage the software's security features as often as possible. He also said the company is working on ensuring Zoom's webinar tool has waiting room improvements, which allow meeting hosts to approve users before they can enter a meeting, but he didn't have a timeline for completion. Another security feature in the works over the next 45 days is an encryption-standard improvement, and a renewed focus on protecting health-related data, he said.

AI Zoombomb

Zoombombing took a surreal turn when a Samsung engineer Zoombombed a colleague with an AI-generated version of Elon Musk.

How to Keep Uninvited Guests Out of Your Zoom Event

A few reminders on using Zoom to host public events:

- When you share your meeting link on social media or other public forums, that makes your event … extremely public. ANYONE with the link can join your meeting.
- Avoid using your Personal Meeting ID (PMI) to host public events. Your PMI is basically one continuous meeting and you don’t want randos crashing your personal virtual space after the party’s over. Learn about meeting IDs and how to generate a random meeting ID (at the 0:27 mark) in this video tutorial.
- Familiarize yourself with Zoom’s settings and features so you understand how to protect your virtual space when you need to. For example, the Waiting Room is an unbelievably helpful feature for hosts to control who comes and goes. (More on that below.)

Read on for a list of Zoom features that can help you safely share your Zoom virtual cocktail hour or dance break without unwanted interruptions. Ok, Zoomer? Let’s do it!

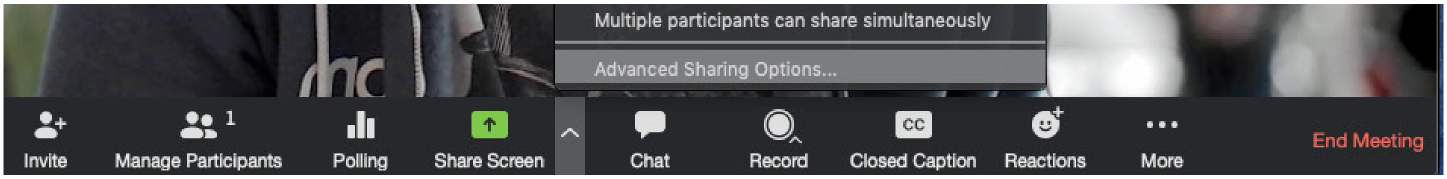
Manage screen sharing

The first rule of Zoom Club: Don’t give up control of your screen.

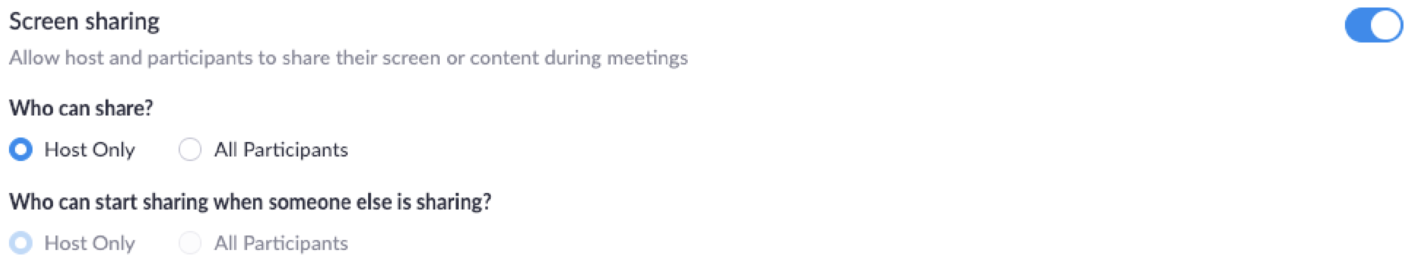
ZOOM CYBER SECURITY ISSUES

You do not want random people in your public event taking control of the screen and sharing unwanted content with the group. You can restrict this — before the meeting and during the meeting in the host control bar — so that you're the only one who can screen-share.

To prevent participants from screen sharing during a call, using the host controls at the bottom, click the arrow next to Share Screen and then Advanced Sharing Options.



Under "Who can share?" choose "Only Host" and close the window. You can also lock the Screen Share by default for all your meetings in your web settings.



Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

● Host Only ○ All Participants

Who can start sharing when someone else is sharing?

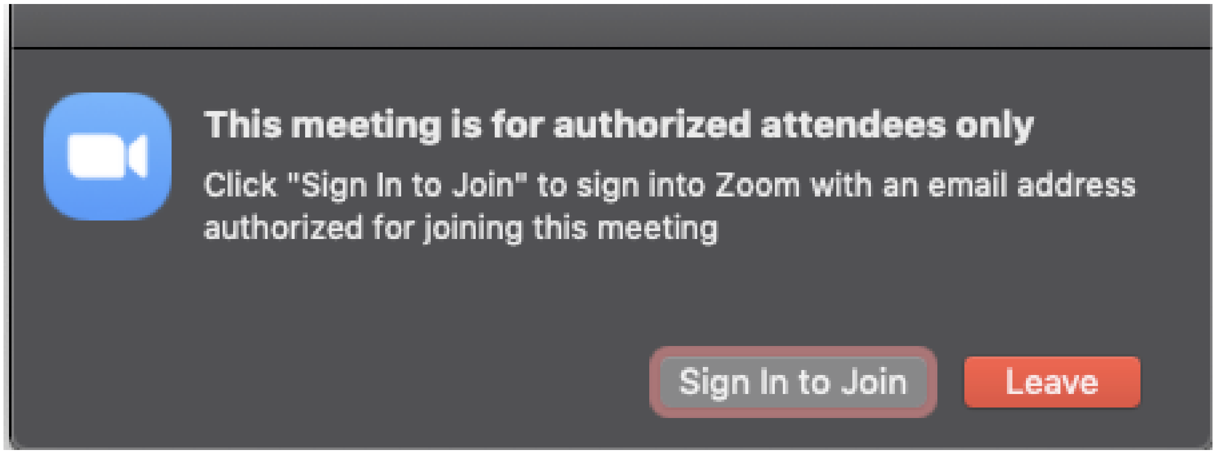
● Host Only ○ All Participants

Manage your participants

Some of the other great features to help secure your Zoom event and host with confidence:

- Allow only signed-in users to join: If someone tries to join your event and isn't logged into Zoom with the email they were invited through, they will receive this message:

ZOOM CYBER SECURITY ISSUES



This meeting is for authorized attendees only

Click "Sign In to Join" to sign into Zoom with an email address authorized for joining this meeting

This is useful if you want to control your guest list and invite only those you want at your event — other students at your school or colleagues, for example.

- Lock the meeting: It's always smart to lock your front door, even when you're inside the house. When you lock a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.

- Set up your own two-factor authentication: You don't have to share the actual meeting link! Generate a random Meeting ID when scheduling your event and require a password to join. Then you can share that Meeting ID on Twitter but only send the password to join via DM.

- Remove unwanted or disruptive participants: From that Participants menu, you can mouse over a participant's name, and several options will appear, including Remove. Click that to kick someone out of the meeting.

- Allow removed participants to rejoin: When you do remove someone, they can't rejoin the meeting. But you can toggle your settings to allow removed participants to rejoin, in case you boot the wrong person.

- Put 'em on hold: You can put everyone else on hold, and the attendees' video and audio connections will be disabled momentarily. Click on someone's video thumbnail and select Start Attendee On Hold to activate this feature. Click Take Off Hold in the Participants list when you're ready to have them back.

ZOOM CYBER SECURITY ISSUES

- Disable video: Hosts can turn someone's video off. This will allow hosts to block unwanted, distracting, or inappropriate gestures on video or for that time your friend's inside pocket is the star of the show.

- Mute participants: Hosts can mute/unmute individual participants or all of them at once. Hosts can block unwanted, distracting, or inappropriate noise from other participants. You can also enable Mute Upon Entry in your settings to keep the clamor at bay in large meetings.

- Turn off file transfer: In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.

- Turn off annotation: You and your attendees can doodle and mark up content together using annotations during screen share. You can disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.

- Disable private chat: Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants' ability to chat amongst one another while your event is going on and cut back on distractions. This is really to prevent anyone from getting unwanted messages during the meeting.

Try the Waiting Room

One of the best ways to use Zoom for public events is to enable the Waiting Room feature. Just like it sounds, the Waiting Room is a virtual staging area that stops your guests from joining until you're ready for them. It's almost like the velvet rope outside a nightclub, with you as the bouncer carefully monitoring who gets let in.

Meeting hosts can customize Waiting Room settings for additional control, and you can even personalize the message people see when they hit the Waiting Room so they know they're in the right spot. This message is really a great spot to post any rules/guidelines for your event, like who it's intended for.