## Table of Contents

How to Keep the Crashers Out of Your Zoom Event.......................................................... 1 – 6

How to Secure Your Zoom Meetings from Zoom-Bombing Attacks .............................. 6 – 14

FBI Warns of Ongoing Zoom-Bombing Attacks on Video Meetings ............................... 15 – 17

Confirmed: Zoom Security Flaw Exposes Webcam Hijack Risk, Change Settings Now .... 18 - 21
How to Keep the Crashers Out of Your Zoom Event

We love that so many people are finding Zoom to be an easy way to stay connected in this time of social distancing, school closures, and work-from-home routines. All these virtual happy hours, coffee breaks, afternoon hangs, dance practices, yoga sessions, and so many other events over Zoom — your creativity and resilience in these tough times are inspiring!

What’s more impressive is that many of us are learning to host these events on the fly! As more people use our platform and host their virtual events using Zoom, we wanted to offer up tips to ensure everyone joining an event does so with good intentions. Like most other public forums, it’s possible to have a person (who may or may not be invited) disrupt an event that’s meant to bring people together.

So, a couple of 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.

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.

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:

![Image of Zoom meeting with message: 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.](https://blog.zoom.us/wp-content/uploads/2020/03/Zoom_meeting_message.png)

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.
How to Keep the Crashers Out of Your Zoom Event

- **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.
Customize the waiting room UI

Meeting ID: 888-888-888

Hey! One sec. The meeting host will let you in soon...

The Waiting Room is really a great way to screen who’s trying to enter your event and keep unwanted guests out.

Keep Zooming responsibly

Zoom is a great way to stay connected right now, and we hope these tips will help you continue to host amazing events using our platform! If you’re not sure whether a public Zoom event is the way to go, share the meeting link only with your close friends, co-workers, and clients. You can even password-protect it for another layer of security.

And keep those pictures from your Zoom virtual events coming! Share them with us on LinkedIn, Facebook, and Twitter, and we’ll like, fave, or retweet a few!
How to Secure Your Zoom Meetings from Zoom-Bombing Attacks

Since countries have begun enforcing shelter-in-place and stay-at-home orders during the Coronavirus pandemic, the Zoom video conferencing software has become a popular way to keep in touch with friends and family, and even to join online fitness classes.

However, with Zoom's rise in popularity, a type of attack called 'Zoom-bombing' has also seen more and more activity.

Zoom-bombing is when someone gains unauthorized access to a Zoom meeting to harass the meeting participants in various ways to spread and hate and divisiveness, or to record pranks that will be later shown on social media.

Just yesterday, the FBI released an advisory warning Zoom users that they should properly secure their browsers from Zoom-bombing attacks.

"The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language," the alert published by the FBI warned.

This guide will walk you through securing your Zoom meetings so that virtual get-togethers, meetings, exercise classes, and even happy hours are not Zoom-bombed by unauthorized users.
Privacy considerations when using Zoom

Before we get into learning how to use Zoom, it is important to consider the privacy ramifications of participating in Zoom meetings.

One of the most important things to remember is that a Host can record a Zoom session, including the video and audio, to their computer. Therefore, be careful saying or physically 'revealing' anything that you would not want someone else to potentially see or know about.

Meeting participants will know when a meeting is being recorded as there will be a 'Recording...' indicator displayed in the top left of the meeting as shown below.

It is also important to remember that a user can download their chat logs before leaving a meeting. These logs will only contain messages that you could see, but not the private chat messages of other users.

Finally, it has been reported that there is no true end-to-end encryption (E2E) between Zoom users' endpoints.

What this means is that only the communication between a meeting participant and Zoom's servers is encrypted, while the related meeting data traversing over Zoom's network is not.

This theoretically means that a Zoom employee could monitor a meeting's traffic and snoop on it, but Zoom has told The Intercept that there are safeguards in place to prevent this type of activity.

"Zoom has layered safeguards in place to protect our users’ privacy, which includes preventing anyone, including Zoom employees, from directly accessing any data that users share during meetings, including — but not limited to — the video, audio and chat content of those meetings. Importantly, Zoom does not mine user data or sell user data of any kind to anyone."
Securing your Zoom meetings

Now that you know the potential privacy risks of using Zoom, before scheduling a meeting with friends or coworkers, you can familiarize yourself with the various ways you can secure Zoom meetings using the steps below.

Add a password to all meetings!

When creating a new Zoom meeting, Zoom will automatically enable the "Require meeting password" setting and assign a random 6 digit password.

You should not uncheck this option as doing so will allow anyone to gain access to your meeting without your permission.

Use waiting rooms

Zoom allows the host (the one who created the meeting) to enable a waiting room feature that prevents users from entering the meeting without first being admitted by the host.

This feature can be enabled during the meeting creation by opening the advanced settings, checking the 'Enable waiting room' setting, and then clicking on the 'Save' button.
Enable waiting room setting

When enabled, anyone who joins the meeting will be placed into a waiting room where they will be shown a message stating "Please wait, the meeting host will let you in soon."

The meeting host will then be alerted when anyone joins the meeting and can see those waiting by clicking on the 'Manage Participants' button on the meeting toolbar.

You can then hover your mouse over each waiting user and 'Admit' them if they belong in the meeting.

Admit a person into the meeting

Keep Zoom client updated

If you are prompted to update your Zoom client, please install the update.
The latest Zoom updates enable Meeting passwords by default and add protection from people scanning for meeting IDs.

With Zoom being so popular at this time, more threat actors will also focus on it to find vulnerabilities. By installing the latest updates as they are released, you will be protected from any discovered vulnerabilities.

**Do not share your meeting ID**

Each Zoom user is given a permanent 'Personal Meeting ID' (PMI) that is associated with their account.

If you give your PMI to someone else, they will always be able to check if there is a meeting in progress and potentially join it if a password is not configured.

Instead of sharing your PMI, create new meetings each time that you will share with participants as necessary.

**Disable participant screen sharing**

To prevent your meeting from being hijacked by others, you should prevent participants other than the Host from sharing their screen.

As a host, this can be done in a meeting by clicking on the up arrow next to 'Share Screen' in the Zoom toolbar and then clicking on 'Advanced Sharing Options' as shown below.

![Advanced Sharing Options](image)

When the Advanced Sharing Options screen opens, change the 'Who Can Share?' setting to 'Only Host'.

---

**Read more at:**
You can then close the settings screen by clicking on the X.

**Lock meetings when everyone has joined**

If everyone has joined your meeting and you are not inviting anyone else, you should Lock the meeting so that nobody else can join.

To do this, click on the 'Manage Participants' button on the Zoom toolbar and select 'More' at the bottom of the Participants pane. Then select the 'Lock Meeting' option as shown below.

Do not post pictures of your Zoom meetings
If you take a picture of your Zoom meeting than anyone who sees this picture will be able to see its associated meeting ID. This can then be used uninvited people to try and access the meeting.

For example, the UK Prime Minister Boris Johnson tweeted a picture today of the "first ever digital Cabinet" and included in the picture was the meet ID.

This could have been used by attackers to try and gain unauthorized access to the meeting by manually joining via the displayed ID.
Manually join a meeting by ID

Thankfully, the virtual cabinet meeting was password-protected but does illustrate why all meetings need to use a password or at least a waiting room.

Do not post public links to your meetings

When creating Zoom meetings, you should never publicly post a link to your meeting.

Doing so will cause search engines such as Google to index the links and make them accessible to anyone who searches for them.

As the default setting in Zoom is to embed passwords in the invite links, once a person has your Zoom link they can Zoom-bomb your meeting.

Be on the lookout for Zoom-themed malware

Since the Coronavirus outbreak, there has been a rapid increase in the number of threat actors creating malware, phishing scams, and other attacks related to the
This includes malware and adware installers being created that pretend to be Zoom client installers.

To be safe, only download the Zoom client directly from the legitimate Zoom.us site and not from anywhere else.
The US Federal Bureau of Investigation (FBI) warned today of hijackers who join Zoom video conferences used for online lessons and business meetings with the end goal of disrupting them or for pulling pranks that could be later shared on social media platforms.

"The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language," the warning published by FBI's Boston Division says.

**Zoom-bombing incidents**

According to FBI Boston's Kristen Setera, two Massachusetts schools within the division's area of responsibility (Maine, Massachusetts, New Hampshire, and Rhode Island) reported such incidents.

During late March 2020, a Massachusetts-based high school reported to the FBI that an unidentified individual(s) joined an online classroom taking place over the Zoom teleconferencing platform, yelling profanities and shouting the teacher’s home address.

In another incident reported by a Massachusetts-based school, an unidentified individual dialed into another Zoom classroom meeting displaying swastika tattoos on his webcam.
"As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called 'Zoom-bombing') are emerging nationwide," the FBI alert added.

Defend against video conference hijacking

Those who use Zoom's online video conference platform to host business meetings or online lectures are advised by the FBI to take a number of measures to prevent future hijacking attempts:

• **Do not make meetings or classrooms public**: In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.

• **Do not share Zoom conference links on public social media**: Provide the link directly to specific people.

• **Manage screen-sharing options**: In Zoom, change screen sharing to 'Host Only'.

• **Ensure users keep their Zoom clients up to date**: In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

• Lastly, ensure that your organization’s telework policy or guide addresses requirements for physical and information security.

FBI advises zoom-bombing victims to report such incidents via the FBI’s Internet Crime Complaint Center and any direct threats during a video conference hijacking incident at https://tips.fbi.gov/.

In January, a vulnerability was patched in Zoom's video conference software that could have made it possible for attackers to find and join unprotected Zoom meetings.

Last year, Zoom fixed another security vulnerability (1, 2) that enabled hackers to remotely execute code via a maliciously crafted launch URL on Macs where the app was uninstalled.

A different security issue (1, 2, 3) was patched last year to block remote attackers from forcing Windows, Linux, and macOS users to join video meetings with their cameras forcibly activated.
Zoom also used as bait for phishing and malware

Attackers are also attempting to capitalize on Zoom's increasing user base since the COVID-19 outbreak started by registering hundreds of new Zoom-themed domains that they later use for malicious purposes.

"Since the beginning of the year, more than 1700 new domains were registered and 25% of them were registered in the past week," as Check Point Research discovered. "Out of these registered domains, 4% have been found to contain suspicious characteristics."

The researchers also spotted malicious files using a zoom-us-zoom_############.exe naming scheme which launch InstallCore installers that will try to install potentially unwanted apps or malicious payloads depending on the attackers' end goal.

"When using a known brand name in a website, the intention of the malicious actors is usually to hide among other legitimate websites and lure users by impersonating the original website or a relating service and getting the user's credentials, personal information or payment details," Check Point told BleepingComputer.

"Malware infections would usually occur via phishing emails with malicious links or files. The actual malware used can change based on the attackers' capabilities and goals."
Confirmed: Zoom Security Flaw Exposes Webcam Hijack Risk, Change Settings Now

If you're one of the millions of Zoom video-conferencing users and have the app installed on a Mac, then you're being advised to check your settings to ensure you have the video camera disabled by default—the tickbox is "turn off my video when joining a meeting," and can be found in the video section of the settings.

This is because of a security flaw that has been disclosed today by researcher Jonathan Leitschuh under the zero-day approach. Users are also advised to ensure their apps are updated as patches are released by the company.

The flaw exploits an architectural vulnerability in Zoom, where a web server installed to improve user experience leaves systems open to malicious attack. Webcams can be activated—essentially by forcibly inviting users to ghost Zoom calls, denial of service attacks can be staged (since patched), and uninstalled apps can be reactivated, all without user permission.
Zoom explained this was done to improve patchy user experiences, telling ZDNet it was a workaround to changes in Safari 12—"a legitimate solution to poor user experience, enabling our users to have seamless, one-click-to-join meetings, which is our key product differentiator."

"First off," Leitschuh said in his disclosure, "having an installed app running a web server on my local machine with a totally undocumented API feels incredibly sketchy to me. Secondly, the fact that any website that I visit can interact with this webserver running on my machine is a huge red flag for me as a security researcher."

Leitschuh accused Zoom of "painting a huge target on its back" through the use of the local server, opening up millions of users to attack through a poorly-architected technical solution, which essentially bypasses user browser safeguards in the interests of user experience. Safeguards which are clearly there for good reason.

Leitschuh says that he approached Zoom back in March to disclose the "vulnerability that leverages the amazingly simple Zoom feature where you can just send anyone a meeting link (for example https://zoom.us/j/492468757) and when they open that link in their browser their Zoom client is magically opened on their local machine."
Leitschuh claims that Zoom delayed acting on the vulnerability and did not discuss what he had found until 18-days before the end of the 90-day non-disclosure "grace period." Then, on June 24 "after 90 days of waiting, the last day before the public disclosure deadline," Leitschuh says that Zoom simply deployed a "quick fix" he had suggested to the company three-months earlier.

A spokesperson from Zoom disputes this, telling me that "once the issue was brought to Zoom's Security team’s attention, we responded within ten minutes, gathering additional details, and proceeded to perform a risk assessment. Our determination was that both the DOS issue and meeting join with camera on concern were both low risk because, in the case of DOS, no user information was at risk, and in the case of meeting join, users have the ability to choose their camera settings. Our Security and Engineering teams engaged the researcher and were in frequent contact over the subsequent period."

Leitschuh also claims that "Zoom failed at quickly confirming that the reported vulnerability actually existed and they failed at having a fix to the issue delivered to customers in a timely manner. An organization of this profile and with such a large user base should have been more proactive in protecting their users from attack."

Tech-savvy users can hunt down and decompile the Zoom client application. For the rest of us, change that video setting and keep your app updated. There are no indications yet of major technical changes from Zoom to address this architectural weakness, so changing that video setting—and keeping it changed—seems like advice that will stick.

The spokesperson from Zoom told me that "we do not currently have an easy way to help a user delete both the Zoom client and also the Zoom local web server app on Mac that launches our client. The user needs to manually locate and delete those two apps for now. This was an honest oversight. As such, by this weekend we will introduce a new Uninstaller App for Mac to help the user easily delete both apps."

Zoom has also issued a full statement, confirming the issue and acknowledging that "if an attacker is able to trick a target user into clicking a web link to the attacker’s Zoom meeting ID URL, either in an email message or on an internet web server, the target user could unknowingly join the attacker’s Zoom meeting."

Zoom added that its July update "will apply and save the user’s video preference from their first Zoom meeting to all future Zoom meetings. Users and system
administrators can still configure their client video settings to turn OFF video when joining a meeting. This change will apply to all client platforms."

Zoom has also said that it "takes all security concerns related to our products very seriously and has a dedicated Security team in place. We acknowledge that our website currently doesn't provide clear information for reporting security concerns. As such, in the next several weeks, Zoom will go live with its public bug bounty program, supplementing our existing private program."

Leitschuh, though, remains skeptical and recommends the zero-day approach instead, which has clearly ensure that this exposure has hit the headlines this time around.

--

\textit{Updated later on July 9 with additional comments from Zoom's spokesperson.}