What is zoom bombing and how do I stay safe on Zoom?

Zoom-bombing Zooms have become a popular hobby for malicious attackers on the Internet, so it's essential to equip yourself with a few ways to combat them. There are a lot of options that you can activate to stop Zoom-bombing

What is zoom-bombing and how can I stay safe from this attack? Perhaps this is a question that many people ask, especially for those who are using Zoom to organize online meetings or open online classes. The following article will give you the detailed answers.

For those who are using Zoom to work from home, malicious attackers flock to the breaches of the program to cause havoc. One such attack is called Zoom-bombing. Despite its humorous name, it can cause serious disruption and insult to everyone in a meeting.

In this article, TipsMake will give you information about what Zoom-bombing is, why you don't want to experience it, and how to protect yourself against this attack.

1. What is zoom-bombing?

Zoom-bombing or "bombing Zoom" is the act of breaking into an unsecured Zoom meeting room. This can happen if the meeting room owner has not set up security measures to prevent Zoom-bombing. As such, it has similarities with photo bombing, except that throwing a Zoom bomb could do a lot more harm.

Zoom-bombing simply means that a stranger enters the meeting room, the classroom to harass, harass, scream, or even spread objectionable content such as pictures or videos. There have also been cases of students taking advantage of Zoom-bombing to disrupt online classes on Zoom.

2. Why is it so easy for others to bombard the Zoom meeting?

Usually, Zoom-bombing happens when someone posts a link to a Zoom meeting room publicly with no additional security.

Zoom-bombing happened due to 2 mistakes. The first is to host the meeting without additional protections and secondly someone to expose the meeting ID publicly to the public table. That could be sharing a link on social media, a member intentionally leaking an ID to someone else, or the ID being revealed by an uncontrollable accident.

When these two mistakes happen, the stranger can find the link, click on it and blatantly enter the meeting. This opens up opportunities for Zoom-bombers to share a link and coordinate a more important raid.

3. How to stay safe from the Zoom-bombing attack?

Last March, British Prime Minister Vladimir Johnson tweeted an image of his Zoom conference to announce the first teleconference meeting. However, by doing so, he also revealed the meeting room ID.

Fortunately, Boris has put a password and 2-factor authentication in the room so that no one else can join. But think about it, if the conference room didn't have these protections, anyone could sneak into an important government meeting and record what happened, what would the consequences be?

It's easy to set up a meeting to prevent Zoom-bombing. You just need to make sure a few settings are turned on before running a new session or using an existing room.

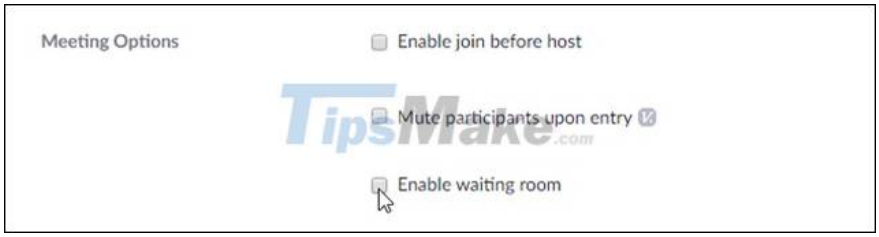
Method 1. Set a password for the Zoom meeting

First, make sure your meeting has a secure password. When you are organizing or setting up a new meeting, search for the Require meeting password and check the option. To set a password, please refer to how to set a password for a class in ZOOM here,

Method 2. Open the waiting room for the Zoom meeting

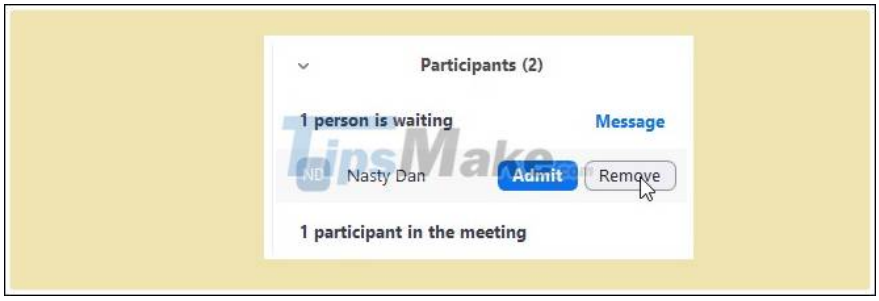
A password will prevent random people from breaking your meeting, but it is not 100% secure for the meeting's security. As mentioned above, someone you invite to join may unintentionally share the link and password. To prevent this attack, open a waiting room for your meeting. This option is not enabled by default, so make sure you enable it when you create or edit your meeting room.

When you change the room settings, check the Enable waiting room checkbox to enable this feature.

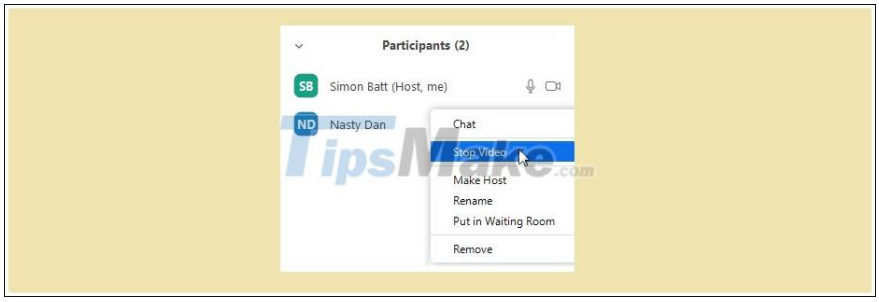


Now, when someone joins the meeting, they are put in a virtual queue, unable to contribute to the meeting. You can view the queue by clicking Manage participants at the end of the active meeting.

You can let them in if you invite them, or decline if they seem suspicious.



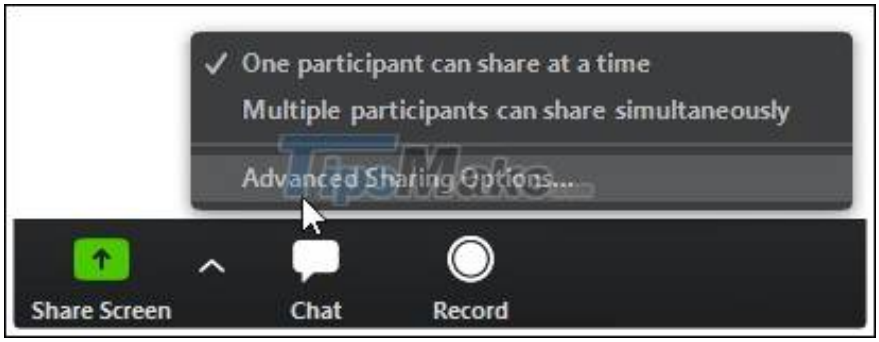
Unfortunately, at the time of writing, there is no way to prevent someone from turning on their webcam. However, if they are displaying inappropriate content through it, you can click More next to their name on the list of users, then turn off their camera.



Method 3. Prevent others from sharing the screen in Zoom

Part of the Zoom bomb attacks involve displaying offensive images. This is achieved by screen sharing, where attackers stream what's on their screen instead of their webcam.

To prevent this, click the up arrow next to Share Screen while participating in a meeting and click on Advanced sharing options.

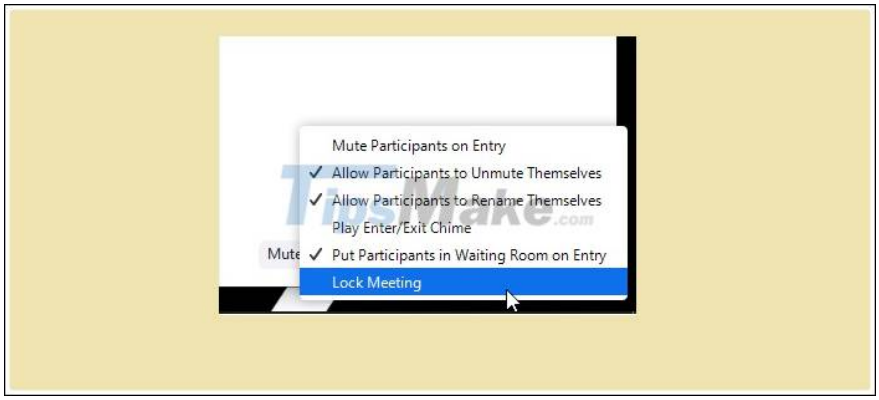


Then, under Who can share, choose Only host.

This will prevent the participant from sharing the content on their screen, while still giving you the freedom to do so as the meeting's host.

Method 4. Lock the Zoom meeting

Finally, after everyone has joined the meeting, you can lock the room. To do that, make sure the list of participants is complete. Click Manage participants again and under the list of participants click More> Lock Meeting.



When a meeting is locked, it will deny anyone trying to connect. In addition, you should update the latest version of Zoom for better support.

Good luck.

You finished reading the article "**What is zoom bombing and how do I stay safe on Zoom?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.