# 5 Ways to Protect Your Zoom Meetings From Hackers

inc.com/jason-aten/hackers-are-trying-to-get-into-your-zoom-meetings-here-are-5-ways-to-stop-them.html

Zoom quickly became the go-to tool for remote teams, teachers, and pretty much everyone who needs a little face-to-face time, even if only virtually. In fact, I wrote this week about how it's quickly become one of the most important apps--period.

Of course, as the vast majority of people start working from home, it shouldn't come as a surprise that the hackers have gone to work. Apparently, one of their favorite new tricks is to crash your Zoom party. In some cases, the party crashes aren't just there to snoop on your meeting or family reunion, they are taking over and sharing inappropriate material.

To protect your meeting, here are a few things you should do:

## 1. Disable Guest Screen Sharing

By restricting screen sharing to the host, you can prevent anyone else from being able to display what is on their desktop. It won't stop anyone from joining your meeting, but it will at least keep them from taking over the meeting and sharing inappropriate material.

## 2. Require the Host to Be Present

Zoom does provide the option for your meeting to start when the first person joins, even if it's not the host. This can be convenient if you're hosting a meeting but running a few minutes behind. Everyone else can get started in the meantime.

If you want to protect your meetings, however, it's best to turn this off. That way, you'll know that no one can start your meetings without you--including a hacker or "Zoombomber" (yes, that's apparently a real term). To do this, make sure the "Join before host" setting is off (it's off by default).

## 3. Keep Your Personal Meeting ID Private

Don't share your personal meeting ID (PMI) online. If you do, it's relatively easy for anyone to find it and join any meeting you're hosting. Instead, use a unique meeting ID for each separate meeting. When you schedule a meeting, you can have Zoom do this by default. Just make sure "Use Personal Meeting ID when scheduling a meeting" is toggled off.

By the way, this won't only keep away bad actors away, it also helps make sure that you don't accidentally end up with the attendees from your next meeting dropping in early.

## 4. Use a Password

If you do use your PMI, you can enable the feature in Zoom that protects those meetings with a password, and only share it with the people you want in your meeting. Just be careful not to share it online, otherwise it defeats the entire point.

## 5. Use the Waiting Room

Another option is to enable to waiting room feature, which places every guest in a virtual waiting room before the meeting starts. When you're ready, you'll then have to manually admit your guests.  This gives you control over who can attend and makes it easier to keep unwanted guests out.

The downside is that if you're meeting with a large number of participants, it can be cumbersome to have to manually admit everyone. In addition, if someone joins the meeting late, you'll need to be paying attention and let them in. Still, if it's important to you that only your invited guests attend your meeting or webinar, this is probably the most reliable way to control who gets in.

Published on: Mar 30, 2020