

5 Ways to Protect Zoom Meetings From Hackers

Other organizations have reportedly had incidents of Zoom meetings (larger group meetings, not one on one meetings) being hacked. While we believe the way Oaklawn is choosing to utilize Zoom is protected from hacking attempts, we wanted to put out some safety measures you can use, just in case.

Firstly, it is important to note, **Zoom Meetings are Encrypted** so once the meeting has begun, the meeting content is protected. The email we send with the meeting link is not encrypted (unless it is only sent to internal Oaklawn emails) which is where a hacker might gain access to your meeting. If you have a Zoom meeting hacked, notify your supervisor and the Telemed Tech Team right away. The below tips can help prevent others from hacking your meeting as well as manage disruptions from participants.

1. 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.

The image shows a screenshot of the Zoom 'Schedule Meeting' dialog box. The 'Meeting ID' section is circled in red, indicating the setting to 'Generate Automatically' is selected, while 'Personal Meeting ID 528-314-7799' is unselected. Other settings include: Topic: Kelly Williams' Zoom Meeting; Start: Thu April 2, 2020 at 11:00 AM; Duration: 1 hour and 0 minutes; Time Zone: Eastern Time (US and Canada); Password: Require meeting password (unchecked); Video: Host On, Participants On; Audio: Telephone and Computer Audio (selected); Calendar: Outlook (selected); Advanced Options: Enable join before host (checked), Mute participants on entry (unchecked).

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

2. Use a Password

If you do use your PMI (personal meeting ID) or even generate it automatically, 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, and if you do share it via email, **be sure your email message is encrypted**, otherwise it defeats the entire point.

Schedule meeting ×

Schedule Meeting

Topic
Kelly Williams' Zoom Meeting

Start: Thu April 2, 2020 11:00 AM

Duration: 1 hour 0 minute

Recurring meeting Time Zone: Eastern Time (US and Canada)

Meeting ID
 Generate Automatically Personal Meeting ID 528-314-7799

Password
 Require meeting password 028386

Video
Host: On Off Participants: On Off

Audio
 Telephone Computer Audio Telephone and Computer Audio
Dial in from United States [Edit](#)

Calendar
 Outlook Other Calendars

Advanced Options ▾

[Schedule](#) [Cancel](#)

3. Use The Waiting Room

Another option is to enable the waiting room feature, which places every guest into a virtual 'waiting room.' When you start a meeting, 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.

Schedule Meeting

Topic: Kelly Williams' Zoom Meeting

Start: Thu April 2, 2020 11:00 AM

Duration: 1 hour 0 minute

Recurring meeting Time Zone: Eastern Time (US and Canada)

Meeting ID

Generate Automatically Personal Meeting ID 528-314-7799

Password

Require meeting password

Video

Host: On Off Participants: On Off

Audio

Telephone Computer Audio Telephone and Computer Audio

Dial in from United States [Edit](#)

Calendar

Outlook Other Calendars

Advanced Options

Enable waiting room

Enable join before host

Mute participants on entry

[Schedule](#) [Cancel](#)

The downside is that if you're meeting with a larger 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.

4. Require the Host to Be Present (this is a global setting)

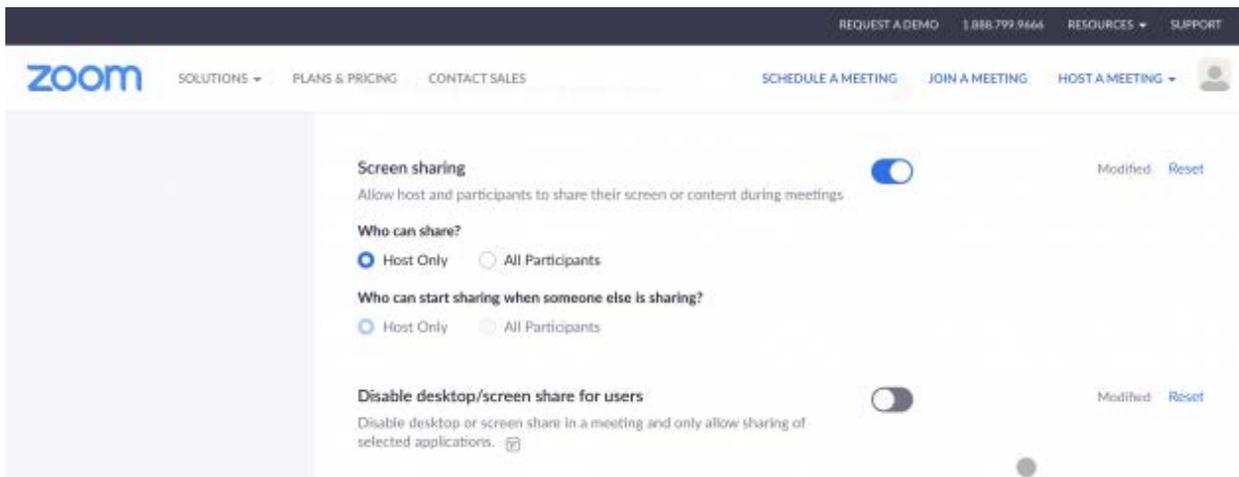
Zoom does provide the option for your meeting to start when the first person joins, even if it's not the host. This can be convenient if you're hosting a meeting but running a few minutes behind. Everyone else can get started in the meantime.

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 a real term). To do this, make sure the "Join before host" setting is off (it's off by default). **This setting is handled by an Administrator and applies to the entire organization.**



5. Disable Guest Screen Sharing (this is a global setting)

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. **This setting is handled by an Administrator and applies to the entire organization.**



The screenshot shows the Zoom Admin Center interface. At the top, there is a dark navigation bar with links for 'REQUEST A DEMO', '1.888.799.9444', 'RESOURCES', and 'SUPPORT'. Below this is a white header with the Zoom logo and navigation links: 'SOLUTIONS', 'PLANS & PRICING', 'CONTACT SALES', 'SCHEDULE A MEETING', 'JOIN A MEETING', and 'HOST A MEETING'. The main content area is a settings card for 'Screen sharing'. It features a toggle switch that is currently turned on. Below the toggle, there are two radio button options: 'Host Only' (selected) and 'All Participants'. A second set of radio buttons is labeled 'Who can start sharing when someone else is sharing?' with 'Host Only' selected. At the bottom of the card, there is a section for 'Disable desktop/screen share for users' with a toggle switch that is currently turned off. The card also includes 'Modified' and 'Reset' links.

REQUEST A DEMO 1.888.799.9444 RESOURCES SUPPORT

zoom SOLUTIONS PLANS & PRICING CONTACT SALES SCHEDULE A MEETING JOIN A MEETING HOST A MEETING

Screen sharing Modified [Reset](#)

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

Disable desktop/screen share for users Modified [Reset](#)

Disable desktop or screen share in a meeting and only allow sharing of selected applications.