

- **Do** require a password for all meetings and webinars conducted in Zoom. This will help to minimize intruders from gaining access to your conferences.
- **Do** make sure to control screen sharing capabilities within Zoom. We recommend you never give up control of your personal screen to anyone you are in a meeting with.
- **Do** have all attendees register prior to meeting on Zoom in order to dissuade Zoombombers from entering your meetings.
- **Do** discuss potential security and privacy concerns with your participants or company prior to using Zoom.
- **Do** review updated security notes posted by Zoom.
- **Don't** use video call if it is not required. When possible, it is recommended to refrain from using video conferencing in Zoom. Instead, simply dial into meetings, which limits the information you are required to provide.
- **Don't** allow participants to share their screen during any of your meetings.
- **Don't** forget to lock your meeting once you have confirmed all known participants have entered your meeting domain. Doing so will prevent intruders from gaining access during your meeting.

The screenshot displays the Zoom web application interface. On the left, the 'PERSONAL' sidebar menu is visible, with 'Settings' highlighted in blue and outlined in red. The main content area shows the 'Meeting' tab selected, with various settings options. A red box highlights the toggle for 'Require that all meetings are secured with one security option' under the 'Security' section.

PERSONAL

Home **NEW**

Profile

Meetings

Webinars

Phone

Personal Contacts

Personal Devices

Whiteboards

Notes **NEW**

Recordings

Clips **NEW**

Scheduler

Settings

Data & Privacy **NEW**

Search Support 1.888.799.9666 Contact Sales Request a Demo

Schedule Join Host Web App **A**

The following steps are for the computer web-based application, followed by the Android and iPhone.

Once you are signed into your Zoom account, look to the left of your screen and below "Personal," select "Settings" (shown here highlighted in red to the left.) On the screen you will see three tabs; "Meeting," "Recording," "Audio Conferencing," "Collaboration Devices" and "Zoom Apps." In the "Meetings" tab scroll down until you see the section shown below. It is recommended you always authenticate users and require a password when scheduling any meeting.

General Meeting Recording Audio Conferencing Zoom Apps Whiteboard Notes **NEW** Clips **NEW**

General

Security

Schedule Meeting

In Meeting (Basic)

In Meeting (Advanced)

Email Notification

Other

General

Merge Meetings and Calendar tabs

View all Zoom Meetings and calendar events in one combined tab.

Show Zoom Meeting invitations

Show meetings I have been invited to by users from my account in my Zoom desktop app.

☐ show meetings only from my account

Security

Require that all meetings are secured with one security option

Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Meeting Passcode

All instant, and scheduled meetings that users can join via client, or room systems will be passcode-protected. The Personal Meeting ID (PMI) meetings are not included.

- ☒ Require a passcode for meetings which have already been scheduled



Passcode for already scheduled meetings

Personal Meeting ID (PMI) Passcode

All Personal Meeting ID (PMI) meetings that users can join via client, or room systems will be passcode-protected.

Passcode:

Enable Personal Meeting ID

A Personal Meeting ID (PMI) is a 9 to 11 digit number that is assigned to your account. You can visit [Personal Meeting Room](#) to change your personal meeting settings. [Learn more](#)

In response to criticisms of weak security and privacy, Zoom has modified passcode options. Zoom has pre-selected and locked user ability to toggle “Off” passcode options, thus making it more secure for users. We recommend you still verify these options are toggled “On,” as shown to the left. The last portion, “Only authenticated users can join meetings from Web client” allows users the option to toggle “On” or “Off.” We recommend you keep it toggled “On.”

To the left you will see a continuation of the password requirements and recommendations located in “Meeting.” We recommend you require meeting attendees to input the provided password and **not** to embed the password into the meeting link. We also recommend you use a “Pre-meeting Password” and not your “Personal Meeting ID.”

Require media encryption for 3rd party endpoints (SIP/H.323)

By default, Zoom requires encryption for all data transferred between the Zoom cloud, Zoom client, and Zoom Room. Turn on this setting to require media encryption for 3rd party endpoints (SIP/H.323) as well. 3rd party (SIP/H.323) endpoints that cannot negotiate media encryption compatible with Zoom's standards will be blocked from joining Zoom meetings.

Chat

Allow meeting and webinar participants to send chat messages

By default, allow participants to chat with

Everyone and anyone directly v

- ☐ Allow users to save chats from the meeting
- ☐ Only users in your account can chat

Send files via meeting chat

Hosts and participants can send files through the in-meeting chat.

Screen sharing

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

Disable desktop screen sharing for meetings you host

When this option is on, users can only share selected applications and files. This option may not be applicable to users using web clients.

Disable screen sharing when guests are in the meeting

Guests include users who are not signed in or not in the same account. Participants who dial-in via phone or join with SIP/H.323 devices will still be able to screen share.

Also, we recommend you use end-to-end encryption whenever possible when using any device that holds your personal information, Zoom is no different.

Note: Zoom’s encryption capabilities have been called into question on several occasions. Therefore, we recommend you watch what is documented on Zoom when in a meeting, as the meeting host’s encryption may not keep your information secure. While using chat features on Zoom, we recommend you not allow other attendees to save chats. In order to do this, scroll down until you see “Chat” (shown here to the left.) All configurations to the left are recommended for the “Chat” section.

Scrolling past “Chat” you will find “File transfer” next in your “Meeting” tab. Due to Zoom’s lack of acceptable encryption and recent security issues, we recommend you not send files of any kind on Zoom. Next, scroll down to “Screen sharing.” We recommend you not allow the ability to screen share when in a meeting on Zoom. If you must allow screen sharing, we recommend that users control who can share screens and who can take control of those screens.

As you continue to scroll down, we recommend you disable the sections “Whiteboard” and “Remote control” (highlighted here in red). It is never recommended that Users give up control of their own computer to any other individual, whether it is a personal computer or company computer.

Whiteboard

Allow participants to share whiteboard during a meeting ☒

Remote control

During screen sharing, the person who is sharing can allow others to control the shared content ☒

Allow removed participants to rejoin

Allow previously removed meeting participants and webinar panelists to rejoin ☐

Show invitee list in the Participants panel

Users invited to meetings on other platforms (e.g. Google, Outlook, or Exchange) will also be shown on this list ☒

Allow users to change their name when joining a meeting

By disabling this setting, users will always use their name on profile page to join a meeting ☐

Allow participants to rename themselves

Allow meeting participants and webinar panelists to rename themselves ☐

Allow host or co-host to rename participants in the waiting room

☐

There is a feature that allows participants to rejoin a meeting if they have been previously removed. It is important you turn this function to “off” in order to prevent users that might hack into your meetings, to continue to rejoin after you have identified and removed them. In order to do so simply scroll down past “Remote Control” and find “Allow removed participants to rejoin” and toggle it to “off.” It is also a good idea to not allow individuals to rename themselves in order to prevent any confusion from other participants.

Report to Zoom

Allow users to report meeting participants for inappropriate behavior to Zoom's Trust and Safety team for review. This setting can be found on the meeting information panel. ☒

Breakout room - Meetings

Allow host to split meeting participants into separate, smaller rooms ☐

Remote support

Allow meeting host to provide 1:1 remote support to another participant ☐

Far end camera control

Allow another user to take control of your camera during a meeting. Both users (the one requesting control and the one giving control) must have this option turned on. ☐

Auto-accept far end camera control

Allow users to add others to their Camera Control Group. When a member of the group requests camera control, they will automatically take control of the user's camera. Group members can be added or removed in Team Chat or Contacts. ☐

Identify guest participants in the meeting/webinar

Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests. ☒

Enable “Stop incoming video” feature

Allows meeting participants to turn off all incoming video feeds on their screen (does not affect other participants' screens). To access this feature, click the view button at the top-right corner of your screen. ☒

Other

Blur snapshot on iOS app switcher

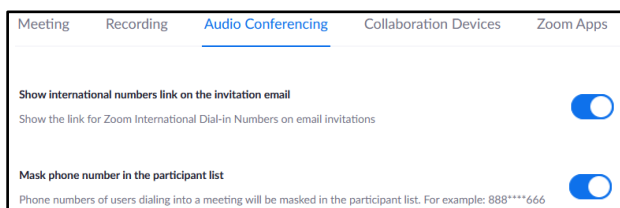
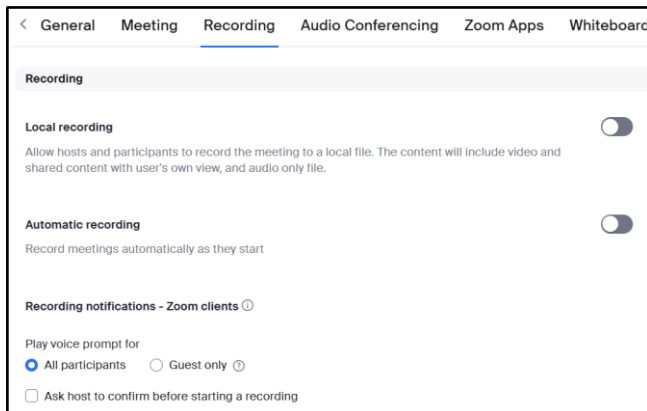
Enable this option to hide potentially sensitive information on the app switcher screen from Zoom. This screen will be shown only when multiple apps are open. ☒

Once you have set the above recommendations, continue to scroll down until you find the “In Meetings (Advanced)” section. Here you will find a series of settings that need to be updated/checked to ensure they meet your specific security requirements. However, we recommend meeting attendees **not** participate in any third-party activities while on Zoom. We also recommend users **not** allow other users to take control of their camera while using Zoom. When setting up a meeting or webinar, it is important to ensure you are able to see “guests” who might be participating for both you and your contacts. If you scroll down, still in “In Meetings (Advanced),” you can enable the “Identify guest participants in the meeting/webinar” (shown to the left).

If you scroll all the way to the bottom of this section, you will find yet another new section on Zoom. This final section will allow you to blur any photos that are being made from users on smart devices in order to control proprietary information or other individuals who might be in attendance. If you are using Zoom for business functions it is important that you enable this function to ensure your companies privacy.

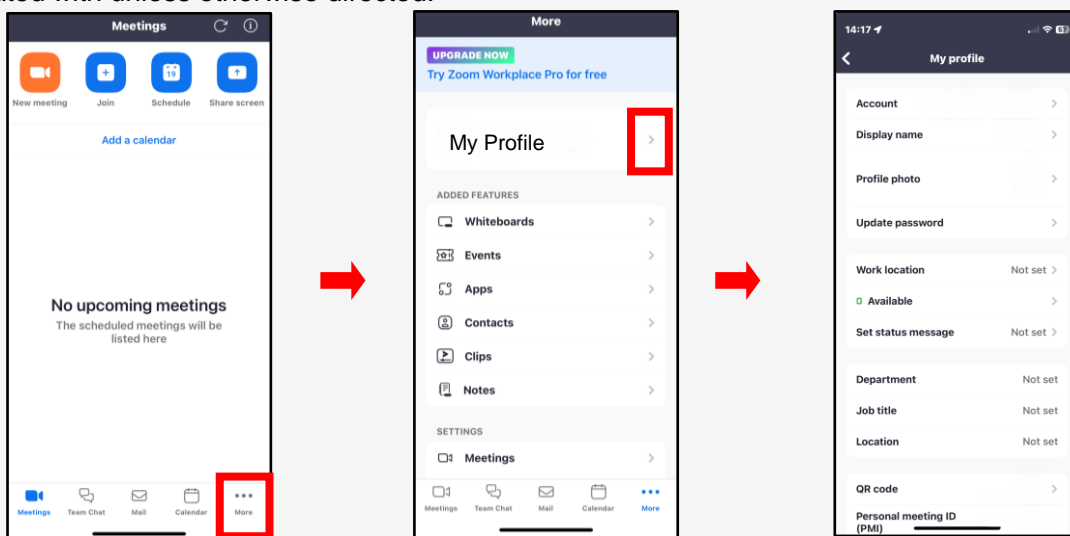
Now, scroll back to the very top of the screen and select “Recording” from the menu option (shown to the right, selected in blue).

Though there are not very many selections to go through, it is still very important to review all your settings here and enable or disable any features you see fit. It is recommended you disable most, and preferably all, features located in the “Recording” section. The only exception here would be the very last feature, which is more of a personal preference than a security issue. It is recommended you **not** allow anyone to record your meetings.



Head back up to the menu and select “Audio Conferencing” to review the final settings here. First, it is recommended that you mask meeting attendees’ phone numbers. In order to do this, simply toggle the “Mask phone number in the participant list” to enable (shown to the left in red).

When using Zoom on your smartphone there are a few security and privacy settings that should be considered for safe use. Though it is not recommended for use on your smart phone, should you choose, there are a few settings to consider here. On both the Android and iPhone, look to the lower right of your screen and select “More” (shown below to the left in red). Next, select your name/email from the top of the screen to take you to your profile page. NOTE: iPhone Users, before selecting your name/email you can look to the lower portion of your screen to “Enable” or (recommended) “Disable” any “Siri Shortcuts” related to this application. In your “My Profiles” section, review each individual section and ensure no personal information has been provided. It is recommended you use initials for your “Display Name,” write no “Personal Notes” about yourself and not fill in any other personal information about yourself or the company you are affiliated with unless otherwise directed.



Do you think your account may have been compromised or hacked? Have you noticed any of the following:

- Unexpected calls or messages made or received from your account.
- Any Direct Messages sent from your account you did not initiate.
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc).
- A notification from Zoom stating your account may be compromised.
- A notification from Zoom stating your account information (bio, name, etc.) has changed.
- Your password is no longer working, or you are being prompted to reset it. *If this occurs it is highly recommended you sign-in online and change your password immediately.

If you said "Yes" to any of the above, it is recommended you immediately do the following actions:

- Delete any unwanted messages that were posted while your account was compromised.
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password.
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess.
- Consider using login verification (if you haven't done so already,) instead of relying on just a password. Login verification introduces a second check to make sure you and only you can access your Zoom account. Note: Two Factor Authentication for Zoom ONLY works on the web-based app and only if you are an admin or if the admin has set it up for you.
- Be sure to check your email is secure. It may be worth changing the password to both your Zoom account and the email associated with your Zoom account.

If you need to report a violation of Zoom's Terms of Service follow this link:
<https://support.zoom.us/hc/en-us/articles/200613919-Report-Terms-Of-Use-Violation>.

If you would like to terminate your account, follow this link: <https://zoom.us/account>.

If you still need help or have questions, you can always contact Zoom using their Support site at: <https://support.zoom.us/hc/en-us/articles/201362003>.

Important Information Regarding Zoom: If your Zoom meeting gets "Zoombombed" there are a few things that can be done. First you can lock them out by going to the "Participants List" in the navigation bar and select "more." Next click "Lock Meeting" to prevent any additional intruders from entering your meeting, which will also allow you to remove individuals without them being able to regain access.

If you are less worried about the intruder and more worried about the disruption, follow the same path but to the "Participants List" and scroll down to select "Mute All Controls." This option is not recommended for privacy and security concerns.