

ZOOM SMART CARD

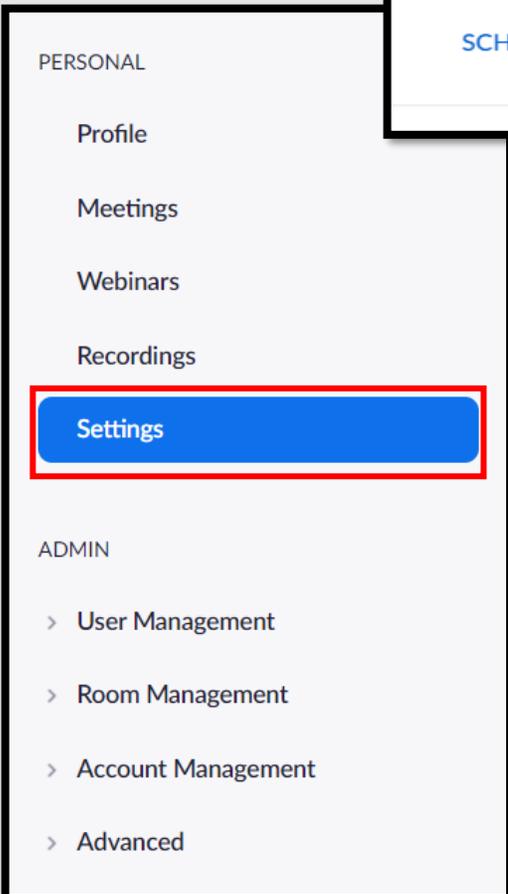
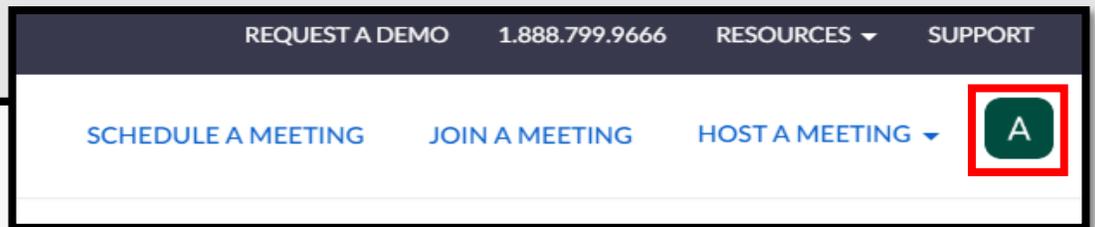


Do's and Don'ts

- 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. It is recommended you never give up control of your person 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 not 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.
- Do not allow participants to share their screen during any of your meetings.
- Do not 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.
- Do not engage a Zoombomber. It is recommended you lock your meeting to prevent intruders.

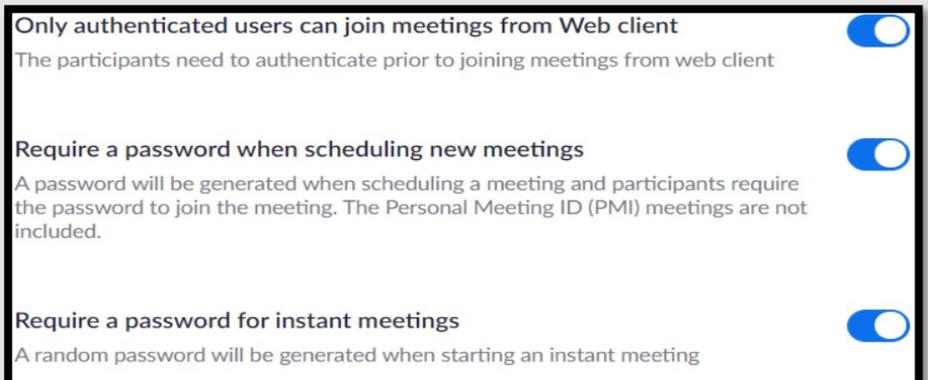
Zoom is a U.S. based remote conferencing service utilized by businesses, schools and individuals all over the world. It provides a remote conferencing service that combines video conferencing, online meetings, as well as a messaging feature. Zoom has recently come under major scrutiny for its inadequate privacy and security protocols, most notably its lack of encryption and accidental routing of calls through China. While it is not recommended for use overall, the next several pages below show recommended ways to manage the security and privacy settings for Zoom.

When utilizing video conferencing it is important to remember to check and secure your network connections. #updateandbesafe.



The following steps are for the computer web based application, followed by the Android and iPhone (should the process be different).

Once you are signed into your Zoom account, look to the right of your screen and select your profile icon (highlighted atop this text, in red). From your "Profile" page select "Settings" to the left of your screen (shown here highlighted in red to the left). On the screen you will see three tabs; "Meeting," "Recording," and "Telephone." In the "Meetings" tab scroll down until you see the section shown below. It is recommended that you always authenticate Users and require a password when scheduling any meeting.



ZOOM SMART CARD



It is important to think about what people can see and hear when using Zoom. Encourage the use of virtual backgrounds so Users' personal environments are not shown.

Require a password for Personal Meeting ID (PMI)

Embed password in meeting link for one-click join

Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.

To the left you will see a continuation of the password requirements and recommendations located in "Meeting." It is always recommended you require Users to input the provided password and not to embed the password into the meeting link. It is also recommended you always use a pre-meeting password and not your Personal Meeting ID.

Require Encryption for 3rd Party Endpoints (H323/SIP)

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

Chat

Allow meeting participants to send a message visible to all participants

Prevent participants from saving chat

Private chat

Allow meeting participants to send a private 1:1 message to another participant.

Auto saving chats

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

When possible it is highly recommended you utilize end-to-end encryption 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, it is recommended individuals watch what is documented on Zoom when in a meeting or simply on their profile, as their encryption may not keep User information secure.

While using chat features on Zoom, it is recommended you not allow individuals to save chats. In order to do this scroll down in the "Meeting" tab until you see "Chat" (shown here to the left). All configurations shown to the left are recommended for the "Chat" section.

File transfer

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

Only allow specified file types

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, it is highly recommended that Users not send files of any kind on Zoom.

Screen sharing

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

Disable desktop/screen share for users

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

Next, scroll down to "Screen sharing". When possible, it is recommended you not allow the ability to screen share when in a meeting on Zoom. If you must allow screen sharing, it is highly recommended Users control who can share screens and who can take control of those screens.

ZOOM SMART CARD



As you continue to scroll down, it is recommended 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 com-

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

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

Closed captioning
Allow host to type closed captions or assign a participant/third party device to add closed captions

Save Captions
Allow participants to save fully closed captions or transcripts

Far end camera control
Allow another user to take control of your camera during a meeting

Virtual background
Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.

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.

Once you have set the above recommendations, continue to scroll through “Meeting” 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, it is recommended Users not participate in any third party activities while on Zoom. It is further recommended Users never allow any other individual to take control of their camera while using Zoom. Even if you know the individual to whom you are considering giving access, it is still highly recommended that you not allow them control. When setting up a meeting or webinar, it is important to ensure you are able to see “guests” that 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).

Now, scroll back to the very top of the screen and select “Recording” from the menu option (shown to the left, 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, if not all, features located in the “Recording” section. The only exception here would be the very last feature, which is more of a personal preference, but not a security issue. It is highly recommended you not allow anyone to record or format Zoom to automatically record any of your meetings.

Meeting **Recording** Telephone

Recording

Local recording
Allow hosts and participants to record the meeting to a local file

Automatic recording
Record meetings automatically as they start

Recording disclaimer
Show a customizable disclaimer to participants before a recording starts

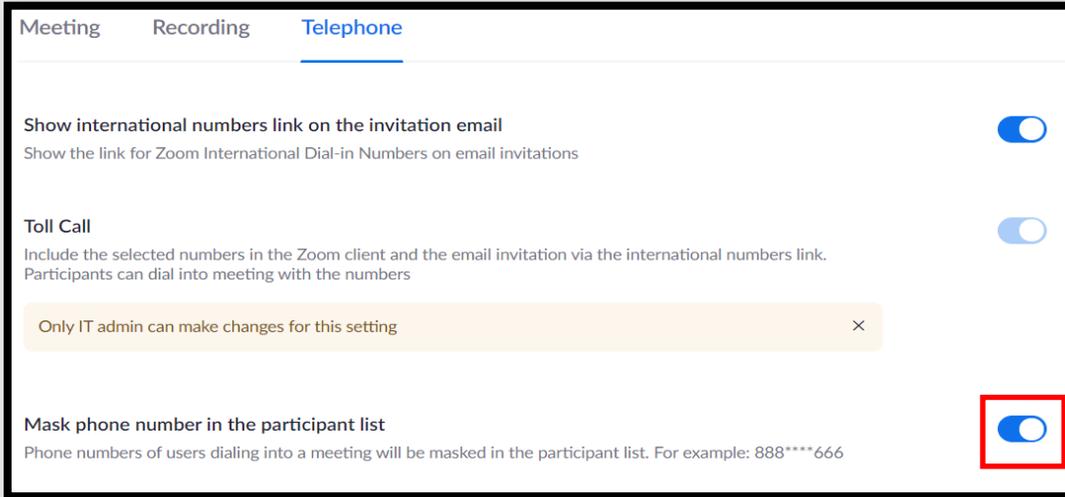
Multiple audio notifications of recorded meeting
Play notification messages to participants who join the meeting audio. These messages play each time the recording starts or restarts, informing participants that the meeting is being recorded. If participants join the audio from telephone, even if this option is disabled, users will hear one notification message per meeting.

When possible use a Co-Host or an Alternate Host to help monitor activity during your meeting.

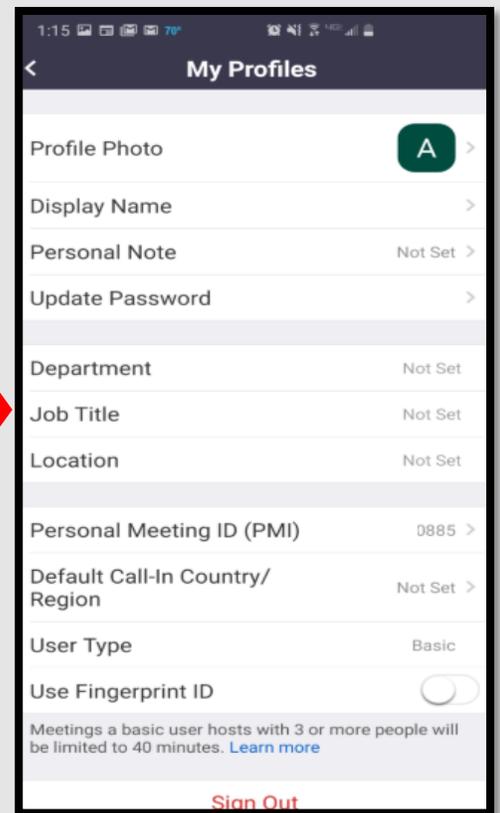
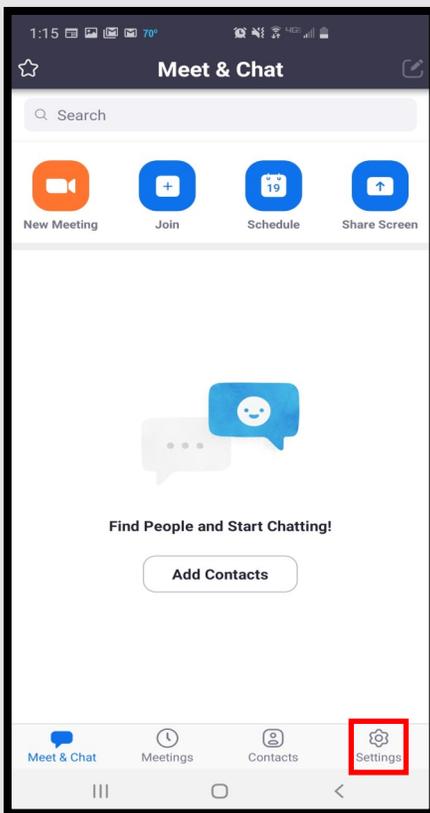
ZOOM SMART CARD



Holding participants in a "waiting room" and approving the connection of each individual gives the host control over who is in the meeting.



Finally, head back up to the menu and select "Telephone" to review the final settings here. It is recommended you do allow phone numbers by participating Users to be masked to preserve each members personal information. In order to do this, simply toggle the "Mask phone number in the participant list" to enable (shown here to the left highlighted 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 chose, there are a few settings to consider here. On both the Android and iPhone, look to the lower right of your screen and select "Settings" (shown above 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.

ZOOM SMART CARD



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 that you did not initiate
- ◆ Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- ◆ A notification from Zoom stating that your account may be compromised
- ◆ A notification from Zoom stating that 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 that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is recommended that you immediately do 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 that 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 that 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 Zooms Terms of Services 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 cannot log in to your email account, **Twitter** has provided links to each email accounts "having trouble signing in" page for your convenience. Please see the **Twitter** smart card for this information.

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.

PASSWORD LENGTH	POSSIBLE COMBINATIONS	TIME TO CRACK S = SECONDS M = MINUTES H = HOURS Y = YEARS
4	45697	< 1 S
5	11881376	< 1 S
6	308915776	< 1 S
7	8031810176	~ 4 S
8	208827064576	~ 1.5 M
9	5429503678976	~ 45 M
10	1411677095653376	~ 19 H
11	3670344486987780	~ 1 Y
* 12	95428956661682200	~ 1.5 Y
13	248115287320374E4	~ 39.3 Y
14	645099747032972E5	~ 1,022.8 Y
15	167725934228573E7	~ 26,592.8 Y
16	436087428994289E8	~ 691,412.1 Y
17	113382731538515E10	~ 17,976,714 Y
18	2947951020001390E10	~ 467,394,568 Y