Zoom Security – How to Minimize
Your Hosted Session from Being Zoombombed

By Roger Magnus, Roger Magnus Research, www.rogermagnusresearch.com

For a Zoom session, what do participants waiting in a room, not sharing their screens, and being locked down have in common? Actually, these variables all inter-relate when it comes to Zoom security and preventing Zoombombing (where an outsider hijacks a meeting and send derogatory comments (spoken or written), photos, or videos).

If you are intrigued, read on …

Below are some helpful steps Zoom hosts can take to minimize (though not completely eliminate as there is no guarantee) an incident and note that not only applying them but also proper **SEQUENCING** of them depending on the type of presentation can make a huge difference.

BIG PICTURE STEPS:

1.) **Be sure to download the latest version of the software** for maximum protection.

2.) **Do not share invites on a publicly accessible webpage or social media page.** It is acceptable to share invites over email though in most cases it is better to send a random ID and password and not the link by itself (Step 3 below). (Social media has numerous security risks.) However, hackers can still access email since the messages are not encrypted.

3.) ****Do NOT send the Join URL by itself unless the meeting is a very small (1-5 persons). If you send the meeting link only, once all participants are in the meeting, immediately Lock Down the meeting (OTHER STEPS - Step 4).**
Schedule a New Meeting – Meeting ID – Generate Automatically
Schedule a New Meeting - Meeting Password – Require Meeting Password (Note: can change password also)
Just like two-factor authentication on many websites, it is better to select **Automatically Generate an ID (NOT Personal ID that could be used repeatedly for new meetings) and a Meeting Password** and send a copy (Sending the link is optional; however sending it automatically activates the Zoom participant software if it is already installed.) to each participant via email. Any uninvited parties would need to know both variables to access the event (ID and Password).

OTHER STEPS:

1.) **Enable the Waiting Room. (And don't allow participants to join before the host.)**
Schedule a New Meeting – Meeting Options - Enable Waiting Room – Checked
Schedule a New Meeting – Meeting Options - Enable Join Before Host – Unchecked
If the meeting is not too big and the process is not too cumbersome, the host should approve everyone who enters the meeting. If that is not possible, then do Step 3 below ASAP. Whatever the size of the meeting, the host should start the meeting before any participants.

2.) **Turn Off Screen Share.**
Settings – In Meeting (Basic) – Screen Sharing – Who Can Share - Host Only
OR
Settings – In Meeting (Basic) - Disable Screenshare for Users - On
This step may be the most important of all since participants cannot share nefarious images or video. When beginning a meeting, only the host should be able to share a screen or the screen share can be turned off for everyone. In this way, a Zoom Bomber cannot share a negative file or image. If the host does not need to share a screen, then screen sharing can be completely disabled.

If the host needs to share a screen, then also disable Remote Control so a Zoom Bomber cannot take over the host's screen.
Settings – In Meeting (Basic) – Remote Control – Off

3.) **Disable File Transfer**.
Settings – In Meeting (Basic) – File Transfer– Off)
This will further prevent a Zoombomber from sharing negative content in a document.

4.) **Lock Down the meeting after all participants are present.**
In meeting – Security – Lock Down Meeting
A new feature under Security (meeting control panel) prevents anyone else from entering if all of the participants are there**.** If participants are running late, the host could set a time of limit of 5-10 minutes after the starting time.

Depending on the size/complexity of the meeting, the steps above can be followed in somewhat different sequences:

- **One other person (know everyone attending)**
  Suggested Steps:
  - Send the URL by itself and/orcustom ID and password over email.
  - Lock down the meeting as soon as all are present (Step 4).

- **Small meeting – 10 or fewer (know everyone attending)**
  Suggested Steps:
  - Send custom ID and password over email – don't send meeting URL by itself.
  - Enable Waiting Room and don't allow participants to join before the host (OTHER STEPS - Step 1); approve each participant.
  - Lock down the meeting as soon as all are present (OTHER STEPS - Step 4).

- **Small meeting – 10 or fewer or larger meeting (don't know everyone attending)**
  **It is better if you can require all attendees to register in advance so you know who is expected.
  Suggested Steps:
  - Send custom ID and password over email – don't send meeting URL by itself.
  - Enable Waiting Room and don't allow participants to join before the host (OTHER STEPS - Step 1); approve each participant.
  - Turn off screen share either for participants or everyone. If the Host needs to share a screen, then turn off Remote Control (OTHER STEPS - Step 2).
  - Optional: Turn off File Transfer (OTHER STEPS - Step 3).
  - Lock down the meeting a few minutes after it starts (OTHER STEPS - Step 4).

Remember hackers are very sophisticated, so any meeting can be Zoombombed. If it is, the meeting should be cancelled immediately and reported to Zoom and the appropriate police authorities. However, following the steps above should largely eliminate what has become a pervasive problem with this useful and versatile video conferencing software.

If you have any suggestions or feedback, please email me at roger@rogarmagnusresearch.com .

Sources Consulted:

"4 Security Settings to Change Now to Prevent Zoobbombing." Hodge, Rae. *c|net*. <https://www.cnet.com/how-to/4-zoom-security-settings-to-change-now-to-prevent-zoombombing/>

"10 Top Tips to Help You Zoom Safely." Wycislik-Wilson, Mark. *betanews*. <https://betanews.com/2020/04/21/zoom-safety-tips/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed+-+bn+-+BetaNews+Latest+News+Articles >

"How to Keep Uninivited Guests out of Your Zoom Event." *zoom blog*. <https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/>

"What is Zoombombing, and How You can Stop It?" Gunnel, Marshall. *How To Geek*.< https://www.howtogeek.com/667183/what-is-zoombombing-and-how-can-you-stop-it/>.