SEARCH HIGH-TECH CRIME TRAINING SERVICES

April 2020

Best Practices for Securing a Zoom Meeting

By Lauren Wagner
High-Tech Crime Training Specialist
SEARCH

In light of the 2020 Coronavirus global health pandemic, agencies at all levels of government have closed businesses and mandated social distancing and other prophylactic measures to reduce community spread of COVID-19. In response, private industry and government agencies and educational institutions have shuttered their facilities and, in many cases, are adopting *work-from-home* and *distance-learning* schemes to maintain operations. This unprecedented shift to virtual work and learning environments has triggered a significant increase in the demand for video-teleconferencing (VTC) platforms to stay *connected* (figure 1). Organizations and individuals are turning to VTC applications to host business meetings, webinars, training workshops, online schooling, and even to celebrate birthdays virtually. Worldwide growth of VTC platforms increased 45% during the week of March 14–21, 2020, over the previous week, and is up 90% from the weekly average of Q4 in 2019.[1] The FBI released guidance on securing Zoom meetings on March 30, 2020; this document leverages and extends that guidance.

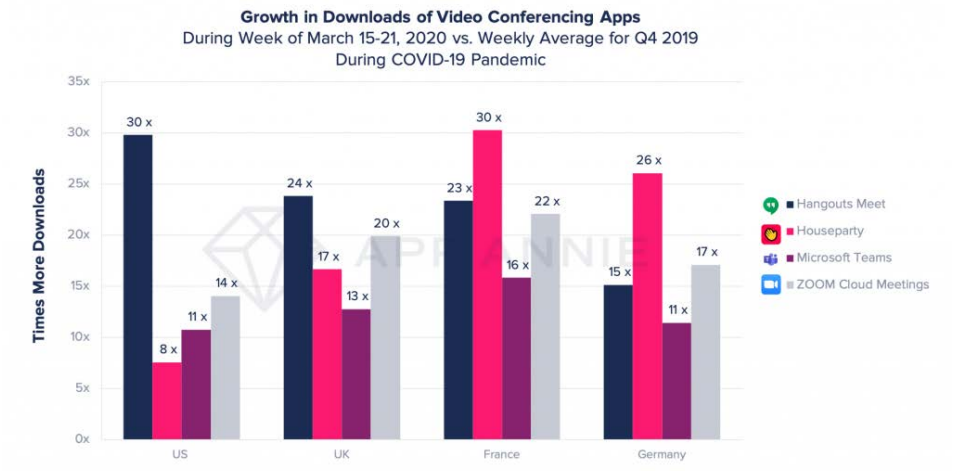

figure 1: Growth in downloads of video conferencing apps[2]

While several VTC platforms are available for personal use (e.g., Facebook Messenger, Google Hangouts, Houseparty, FaceTime), three that best fit the needs of educational institutions and businesses are:

1. Zoom Cloud Meetings
2. Microsoft Teams
3. Go-to-Meeting

[1] https://www.appannie.com/en/insights/market-data/video-conferencing-apps-surge-coronavirus/

[2] *Ibid.*

Given the substantial growth in the use of Zoom by business and government agencies, we focus on this application in this *Best Practices* brief. Future briefs will address other VTC applications.

Zoom. Zoom Cloud Meetings is an increasingly popular VTC option for business and educational institutions. Zoom was founded in 2011 by Eric Yuan in San Jose, California. By May 2013, Zoom had 1 million participants.[3]

Zoom offers a free basic meeting plan, which allows users to host up to 100 participants with unlimited one-on-one meetings and unlimited group meetings of up to 40 minutes.[4] Many educational facilities use the Zoom platform because for K–12 schools affected by the COVID-19 pandemic, Zoom is offering the basic meeting plan for free and removing the 40-minute time limit on group meetings.[5]

Zoom Cyberattacks Increase. With the increasing use of VTC, there is also a surge in people trying to exploit the VTC platforms. The FBI warning highlighted one particular vulnerability called "Zoom-bombing."[6] Zoom-bombing is a "gate-crashing" form of cyberattack in which an unauthorized person joins a Zoom meeting hosted by another person or organization with the intent of disrupting the meeting or obtaining or exposing privileged, private, or proprietary information. Users report their meetings have been interrupted by "strangers drawing offensive imagery onscreen, sharing pornographic images, doxxing[7] people in the chat, and taunting them with hate speech and threats."[8] School districts and businesses have actually begun banning the use of Zoom out of concern of online security threats.[9] Zoom meetings posted to public spaces are especially vulnerable.

Best Practices for Zoom Security. Zoom is a powerful tool to stay connected and the threat of Zoom-bombing can be mitigated by following several best practices to ensure privacy and security:

1. **Use a meeting password when setting up a Zoom meeting (figure 2).**

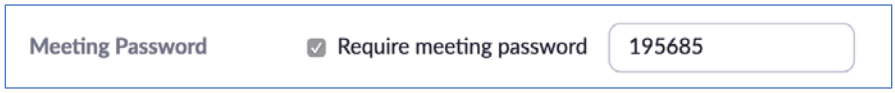

figure 2: Meeting Password set-up in a Zoom meeting

[3] https://en.wikipedia.org/wiki/Zoom_Video_Communications

[4] https://zoom.us/pricing

[5] https://zoom.us/education

[6] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

[7] "Doxxing" is the posting of personal information about another, e.g., address, phone number, email, etc.

[8] https://www.thecut.com/2020/04/what-is-zoombombing.html

[9] Valerie Strauss, "School districts, including New York City's, start banning Zoom because of online security issues" (*The Washington Post*, April 4, 2020, at: https://www.washingtonpost.com/education/2020/04/04/school-districts-including-new-york-citys-start-banning-zoom-because-online-security-issues/); Maggie Miller, "Thousands of Zoom meeting recordings exposed online: report" (*The Hill*, April 3, 2020, at: https://thehill.com/policy/cybersecurity/491106-thousands-of-zoom-meeting-recordings-exposed-online-report); Taylor Lorenz and Davey Alba, "'Zoombombing' Becomes a Dangerous Organized Effort" (*The New York Times*, April 3, 2020, at: https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html).

A meeting password that is directly provided to users and not posted publicly is by far the most important step to prevent Zoom-bombing. Meeting IDs[10] can be guessed using "war dialing" and if someone attacks a Zoom meeting with this method, the only prevention tool is a ***strong meeting password***.[11] If an unauthorized/uninvited person attempts to join your meeting, they will see this message (figure 3):

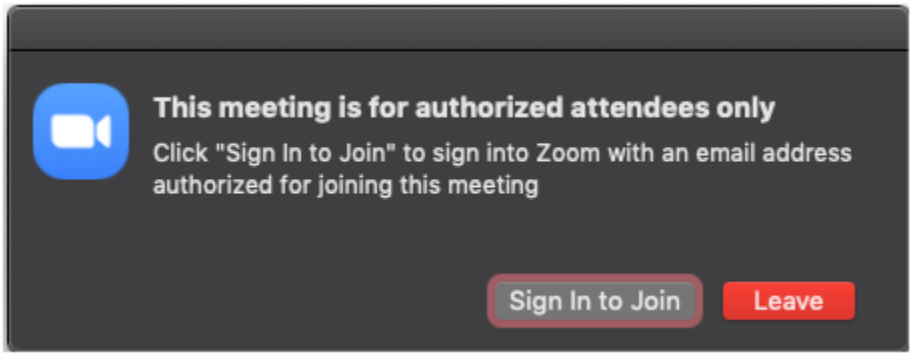

figure 3: Message for unauthorized/uninvited attendees

2. **Use a waiting room for attendees when setting up a Zoom meeting (figure 4).**

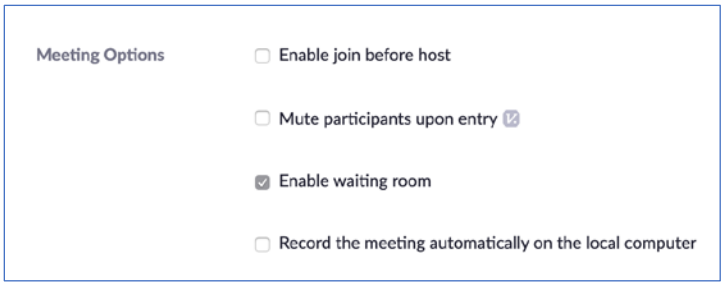

figure 4: Waiting room feature in the Meeting Options

A "waiting room" is an area where participants are cloistered in before the host joins. A meeting host can approve participants in a waiting room one-by-one or all at once. Waiting rooms can be configured for all participants or only guests (i.e., participants who are not on the Zoom account of the host or not currently signed into Zoom).[12]

3. **Provide the link directly to participants. Do not share a link to a Zoom meeting on a publicly available platform or social media platform.**

While steps 1–3 will prevent most Zoom-bombing scenarios, there are some additional steps users can take for even greater security:[13]

[10] For free Zoom accounts, Meeting IDs will always be a 9-digit number, while paid business accounts use a personalized, non-numerical ID.

[11] https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/

[12] Many more waiting room features are discussed at: https://support.zoom.us/hc/en-us/articles/115000332726-Waiting-Room

[13] https://zoom.us/security

4. Disable participants from being able to join before the host.
5. Make sure all hosts and participants are using the latest version of Zoom software (updated after January 2020 specifically).
6. Require encryption for third-party endpoints.
7. Use an automatically generated Meeting ID for non-reoccurring meetings. If a personal meeting ID is used, this can be reused by anyone who already has the numerical value.
8. Once a meeting has started, lock the meeting. This will prevent any other people from entering the meeting. This is done from the Participants list in the navigation sidebar. Click **More** and then **Lock Meeting**.
9. Once a meeting has started, assign one to two co-hosts. The co-hosts will be able to control the situation if anyone hijacks the controls of the original host.
10. If using Zoom for a webinar or training, change screen-sharing to "host only" and disable the remote-control function.
11. If using Zoom for sensitive material, make sure to disable participant recording.
12. If using for meetings beyond a select, specific group of participants, disable file transferring, annotations, disabling mute, and saving of chat.
13. If using Zoom to make a recording of the meeting, rename the recording. Zoom recordings have a standard naming convention that is easily guessed, therefore making them vulnerable to compromise.

With Zoom, as with any other digital communication methods, it is critical to practice good digital security practices:

- Use a strong password for your meetings – ***do not*** use easily guessed passwords such as *password* or *1111* or *12345*.
- Do not click on links for Zoom meetings when you are not expecting an invitation.
- Check the Zoom meeting URLs in any email you receive to make sure they are not a phishing attempt.[14]

People sometimes expect technology to provide all the security mechanisms. Remember: Even the best cybersecurity mechanisms can be bypassed with a little human exploitation. *Zoom does not employ full encryption over audio and video.* Similar to telephones, it is possible, though unlikely, that data may be subject to interception. Employing best practices security is critical, but also consider avoiding Zoom, or any VTC, for secret communications. A good maxim to follow is—*If you would not say it over a telephone, don't say it over Zoom.*

In addition to the best practices outlined in this brief, SEARCH has created a resource guide, "Zoom Configuration Resource Guide," which is available upon request from the SEARCH website at https://www.search.org/resources/e-crime-investigative-tools/.

[14] An easy way to check a URL is to hover over the URL in the email. Make sure the hyperlink is actually going to a Zoom meeting URL and not redirecting to a malicious website.