Adventist Risk Management, Inc.

By: Chris LeBrun - Manager, Marketing and Communication

Protect Your Zoom Meetings from Being Hijacked

April 06, 2020

Do you find yourself spending a lot more time these days on video conference calls? So do Internet hackers. With much of the world under some form of stay-at home order or lockdown due to the COVID-19 pandemic, employees are increasingly using Zoom and other video conferencing platforms for work, school, and even church. Hackers, called “Zoombombers,” have seized this opportunity and are causing havoc in virtual meetings, online classrooms, and video calls worldwide.

Some vulnerabilities exist for Windows machines if the hacker can post a link in the chat feature.[1] Of course, make sure your antivirus software is up to date. Also, never click a link sent from someone you don’t know. The biggest risk these attacks present comes from Zoombombers. They are looking to cause disruption in virtual meetings by yelling, usually profane or obscene things, and by taking over the screen to show inappropriate images.

How Hackers Gain Access

As far as hacking goes, gaining access to a Zoom meeting is relatively simple. Users are not required to sign in to attend a Zoom meeting. Simply enter a 9-digit Meeting ID on the website, and you can gain access to a meeting room. Hackers are using a computer script to randomly generate number combinations until they find one that is hosting a meeting. Then they take over the meeting.

So how do you prevent unwanted people from accessing your online meetings? Zoom offers a couple of options you may want to consider, both with pros and cons. The first is using a password to protect your sessions, and the second is enabling a “waiting room” for guests.

Password Protected Meetings

When scheduling a meeting, Zoom gives you the option to require a password for guests to enter the meeting. Unless you are using your Personal Meeting ID (PMI), this password is randomly generated and sent out with the invite. After entering the meeting ID, guests will also be required to enter the password before gaining access to your meeting.

This method will slow down would-be hackers, but it may not completely prevent them from gaining access to your meetings. The

randomly generated password from Zoom is a 6-digit numerical code, and the same program that generates the meeting ID could conceivably produce the correct password as well. A password can also be frustrating for teams that participate in multiple meetings a day, as they always have to enter the correct password to attend each session.

Using password-protected meetings is especially important when you will be sharing personally identifiable information (PII) about employees, clients, or members. This extra layer of security helps protect you from exposing your constituent's private information to unwanted guests.

Waiting Room Enabled Meetings

Another option is to enable the waiting room feature. This is found in the advanced options section when scheduling a meeting. When guests join your meeting, they will be placed in a virtual waiting room rather than immediately being added to the call. The host will be notified that people are in the waiting room and can choose to allow them to enter the meeting or not.

For teams who use a corporate Zoom account, an additional setting is buried deep in the online settings that allows internal users to bypass the waiting room for meetings scheduled by another corporate team member. This means only participants from outside your organization —those who pose the biggest threat of hijacking your meeting — would have to be approved by the host before entering the call.

Password protected meetings, and the virtual waiting room features can also be used together to add a duel-layer of security.

Additional Tips

Other steps you can use to prevent a hostile takeover of your meeting is to block participants from sharing their screen. This setting is changed in the online settings of your Zoom account and will apply to all meetings. You can grant permission for users to share their screens as needed from the Screen Share menu during the call. To increase security for schools, Zoom made an update to education accounts on March 26, 2020, which defaults to only allowing the host to share their screen.

To make your meetings run more smoothly have participants wait for the host to join before they are allowed to enter the meeting room. You can also mute participants upon entry and turn off the chimes that alert you to someone entering the meeting if that is distracting.

You should also be careful about how you distribute your Zoom meeting IDs. Publishing these on social media or on your website makes it that much easier for people to hack your meeting. If you want your church services open to the public, consider using Zoom's webinar feature (an additional cost) to broadcast the webinar on Facebook and/or YouTube.

Use email or other private communication methods to distribute meeting IDs for Sabbath School classes, small groups, prayer meeting, online school classes, and other meetings that require interaction from the group.

Backup Plan

Hackers will find new ways to get around security protections faster than companies can put new protocols in place. Develop a plan to quickly end a meeting if it becomes hacked. Part of this plan is communicating in advance to team members and external participants on how to reconnect quickly in another meeting room to continue the meeting.

Technology isn't always perfect, but we are blessed to have these modern conveniences to stay connected during this time of social distancing.

Reference

[1] https://www.pcworld.com/article/3535373/report-hackers-can-steal-windows-credentials-via-links-in-zoom-chat.html