Zoom Best Practices

Prepared by

C | COMPUFIT LLC

Technology Leadership • Cloud Solutions • Managed Services • Cybersecurity

compufit.com

Zoom Acknowledgment

Compufit recognizes that there’s a lot of fear surrounding the use of Zoom right now. In recent weeks, numerous articles have come out detailing the security and privacy issues that Zoom has encountered. Even the FBI released a statement regarding “Zoom Bombing”. Zoom has since made a statement regarding the issues, their resolution and their path forward. Compufit is taking part in Zoom’s CEO weekly meetings to obtain the latest updates on their security and privacy concerns, in order to keep our clients updated.

Zoom Acknowledgment Cont.

With any new and emerging technology, there’s bound to a lot of bumps in the road. Especially when your numbers surge to over 200 million daily meeting participants! What was intended to be a company assisting us in connecting to others during their time in isolation, has shined the light on hackers taking advantage of an emerging platform.

Zoom Acknowledgment Cont.

Currently, the issues that have surfaced have now either been fixed or clarification has been given by Zoom. Always remember, new updates and security patches will be released and need to be implemented. Hackers love figuring out how to exploit technology. *Think Microsoft “Patch Tuesday” or the constant app updates on your phone. T*o assist with the use of Zoom, we’ve compiled a list of best practices for our clients.

Zoom Best Practices

Hosting Public Meetings/Events

- If you shared your meeting links on social media or other public forums, understand that anyone who can see your social media account can join the meeting by default. Be extremely careful with this!
- Avoid using your "Personal Meeting ID" for public events. Your personal meeting ID does not change, so if it's shared to the public, anyone can jump on all calls going forward. Under "Meeting ID", use "Generate Automatically" and not "Personal Meeting ID".

Managing Screen Sharing

- Never give control of your screen in a public meeting. By default, we would encourage you to turn this feature off in your settings. Log into Zoom, go to settings, then "In Meeting (Basic)" to make this change.
- If you know you're the only person who should be sharing their screen, ensure your settings are configured to "Host Only". This can also be found in "In Meeting (Basic) settings.

Manage Your Participants

- Allow only signed-in users to join your meetings. If someone tried to join your event and isn't logged into Zoom with the email they were invited through, they will be forced to log in first.
- Set up your own two-factor authentication! You can send the invite in one email or post it online. When someone accepts the invite, you can send them a second email with the passcode or private message them on social media.

Zoom Best Practices

Manage Your Participants (Cont.)

- Remove unwanted or disruptive participants. From the participants menu, you can mouse over a participant's name. Several options will appear. Click "Remove" and they're gone!
- Turn off file transfer. In-meeting file transfer allows people to share files through the in-meetings chat. This could cause users to get bombarded with unsolicited pics, GIFs, memes, and other content.

Waiting Room

- The Waiting Room feature allows you to stage all participants until you're ready to allow them to join the meeting. If you don't know who they are, you don't have to allow them to join!

Encryption

- There's been a lot of articles talking about encryption standards in Zoom. If you need to have your meeting fully encrypted due to the discussion of sensitive content, make sure all participants are using the Zoom app on their phone or computer.

Zoom Best Practices

Multifactor Authentication

- The administrator for your company's Zoom account should ensure that multifactor authentication is set up for all accounts created for business use. Please note that MFA is not available in the free version of Zoom. The free version is not recommended for business use.

Meeting Lock

- When the meeting has started and all participants have entered, click the Security button at the bottom of the screen and select "Lock Meeting". Anyone else trying to enter the meeting will be denied. This ensures no one new can "bomb" the meeting.

Sign-In Methods

- For business purposes, it's recommended to always log in with your work account. The company administrator should disable "Allow users to sign in with Google/Facebook" by default. If you don't work at Google or Facebook, you shouldn't use that account for business purposes. Reserve that for happy hour with your friends!

Questions

If you have any questions, we're here to help. Please contact us below:

Jeff Wilson – C|CISO, CISSP
Chief Information Security Officer
jwilson@Compufit.com