Zoom Best Practices

Quick Guide to Securing Your Zoom Practices

These recommendations and best practices for securing your Zoom meetings can be set in your individual Zoom account under "Meetings and Settings." You can also set some of these on an induvial meeting bases when you are scheduling a meeting.

1 Consider a Paid Version

You get what you pay for with software and cyber security. Make sure that Zoom provides you with a more secure experience by investing in the paid version.

2 Set a Password

Setting a password is a straightforward way of securing Zoom meetings and will filter out any bad actors that are using a scanner to try and enter random Zoom meetings to disrupt them.

3 Keep Zoom Updated

There is a window of opportunity between when Zoom finds, creates an update, and patches a vulnerability and when your employees install those patches. It's a Zoom best practice for securing your Zoom meetings to shorten that window and install those updates as soon as they are available. **Update, update, update!**

4 Internal Meetings: Authenticate Users

When you are scheduling internal staff meetings you can apply a setting that allows only users with a specific domain to enter. (i.e. users@iconicit.com).

5 External Meetings: Waiting Room

Enabling a waiting room as the host of a Zoom meeting allows you to grant access individually to users who are trying to access your meeting room. This means you can control who has access to the meeting, and weed out users you do not recognize.

6 Disable Participants from Screensharing

If you are hosting a meeting where you are the only one who needs to share a screen, disable other participants from screen sharing. Many zoom-bombers are using screen sharing to hijack a meeting and share explicit or hateful content.

7 Familiarize Yourself with the New Security Icon

One of Zoom's updates is a new in-meeting icon that allows you to lock down a meeting after a breach. The "In Meeting" icon is a way of securing your Zoom meetings by disabling chat and spontaneous screen sharing as well as controlling individuals' permissions and access.

8 Disable Join Before Host

While the "In Meeting" security icon is a great tool for the hosts starting the meeting, it's not helpful if bad actors can join the meeting before the host and cause disruption.

9 Zoom Meeting Best Practices: No Public Meetings

Instead of making your meetings public or publishing the link on social media or other public forums, create a sign up. This allows you to choose who you send your meeting invitations to. You still must actively vet those that sign up for this to be most effective, but it adds one layer of complexity that bad actors will most likely avoid. Bad actors always look for the easy way out (or in), and they will bypass you in search of lower hanging fruit.

Finally consider other elements to your security. Securing your Zoom meetings is a great start, but it's only the beginning.

Check out: Cybersecurity Do's and Don'ts Do It Yourself Times to Protect Your Network in the Remote Ages

10