

Can You Trust Zoom?

By Neil Herber

The good/bad news

Zoom has received a lot of good and bad press.

I have tried to follow up on all the "negatives".

Much of the concern about Zoom relates to issues they have already addressed.

Be sure to ALWAYS update to the latest version of the Zoom client.

"Zoom sends info to 3rd parties without permission."

Zoom used to include a component that reported user data to Facebook, possibly only for people who were logging in via Facebook.

That component was removed from the client in mid-April 2020.

.

"Zoom steals info about me."

You do NOT need a Zoom account and you do NOT need to sign in to Zoom to attend a meeting as a guest.

Only the meeting host needs to sign in.

Zoom gets no info about you as a guest other than the name you show on the screen.

"Spammers and worse can crash Zoom meetings."

People were able to crash Zoom meetings (Zoom bombing) because the hosts were posting meeting IDs and passwords publicly.

The most high-profile example was Boris Johnson posting a cabinet meeting ID on social media.

Some hosts were not requiring password access.

Zoom now creates default passwords for ALL meetings to protect inexperienced hosts.

.

"Spammers upload malware files to guests."

By default, Zoom now prevents anyone other than the host uploading files.

.

"Hackers can play my private Zoom meeting recordings."

Zoom allows you to record meetings and save them to the cloud.

The naming scheme for the saved video files was easy to hack and bad actors were doing searches for meeting recordings stored on insecure sites.

Zoom now randomizes the saved video names and also suggests NOT storing them on "open access" sites if you want them to be private.

"No one knows where the Zoom servers are located."

Zoom did not initially disclose what servers were being used to route a conference.

Many companies/governments were concerned that they could be routed through "unfriendly nations".

Zoom now allows hosts to specify which servers to use for routing the conference.

"Zoom encryption can be easily compromised."

Zoom initially wrote their own encryption software
(very bad idea) to encrypt meeting traffic.

They have now enabled well-known and tested
encryption schemes.

See <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf>

"I still don't trust them."

Note that it is still possible for information to leak.

For example, if you share your screen for a demo and it happens to include any visible info like email addresses that you didn't want to share.

Many of the "problems" people had/have with Zoom are related to the host settings. There are a LOT of them.

If you need help checking your Zoom host settings, just ask.

Zoom On!

