NJSBA: HERE FOR YOU

- INFORMATION
- RESOURCES
- UPDATES

CLICK HERE

Best Practices to Stay Cyber Safe on Zoom

Zoom has become a ubiquitous part of conducting business during the COVID-19 public health crisis as nearly every thing we do now happens online, whether its meeting with family and friends, consulting with clients, or participating in a business meeting or court hearing.

Like any online platform authorities recommend exercising due diligence and caution in your cybersecurity efforts. Not every Zoom account is created equally—some, like the one the New Jersey State Bar Association uses, have been carefully reviewed by in-house security experts to offer attendees the safest possible experience provided by the software. Others can be free accounts that don't necessarily protect users in the same way. That's not to say that they are unsafe, but it is accurate to say that they are less safe.

Please consider these perennial cybersecurity tips when using any online platform, including Zoom: Keep up-to-date and install software updates as soon as possible; use passwords to protect your meeting; and be on the lookout for phishing.

Editor's note: The NJSBA now uses Zoom for section, committee and division meetings and webinars, as well as NJICLE seminars. The NJSBA is committed to the online safety of its members and customers and adheres to best practices and recommended security protocols.

FBI Safety Tips to Follow

The Federal Bureau of Investigation offers following steps to mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

A Window into Trouble

In addition to the FBI alert, it is helpful to know about Windows security issues related to Zoom. These concerns are legitimate, depending on the way Zoom is used—when Zoom is set to an open chat forum for all users (a setting security experts discourage), a user can send a link out via the chat to all attendees and encourage them to click on it (possibly saying it's a resource that complements the program, etc.) When a user on a Windows machine clicks on that link, their user name and password could be exposed (although the password would be encrypted).

Additional Resources

Here is the FBI press release about staying safe.
https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

The essential steps in this *Forbes* article are helpful.
https://www.forbes.com/sites/kateoflahertyuk/2020/04/03/use-zoom-here-are-7-essential-steps-you-can-take-to-secure-it/#648f935c7ae1

Read about Zoombombing here.
https://www.npr.org/2020/04/03/826129520/a-must-for-millions-zoom-has-a-dark-side-and-an-fbi-warning