# Avoiding Zoom-Bombing in the New Age of Meetings

PUBLISHED ON
**April 2, 2020**

An unwelcome intruder who infiltrates the workplace or classroom and disrupts a meeting by acting erratically and blurting out epithets poses a threat to everyone's wellbeing and safety.

A few weeks ago a physical intruder would be more likely to create risk exposure. But work and school have moved to virtual platforms in light of the global pandemic, and risk exposure has followed.

Platforms like Zoom, Skype, Blackboard Collaborate, Microsoft Teams, and WebEx allow classes, meetings, health visits, business meetings or other gatherings to continue in ways that were unimaginable just a few decades ago. However, with the positives also come the negatives and this rapid transition to a virtual landscape has released video teleconferencing hijackers, allowing us to coin a new term: "Zoom-bombing."

Zoom-bombing is when a virtual meeting is disrupted by graphic or threatening messages or actions, which often include harassing hate speech or pornographic materials. The intrusions cause liability exposure based on the highly offensive harassment. While the term refers to the popular virtual meeting platform, any platform is likely susceptible to some type of security threat. These instances have quickly garnered attention across the country as virtual classes, support groups, and religious gatherings have been hijacked.

Protecting students, employees, clients and other members of the community from discriminatory harassment is a moral and legal obligation. Title VI, Title VII, Title IX, and other state and federal civil rights laws require covered businesses, organizations, and public entities to prevent discriminatory harassment.

While many aspects of these programs are outside of a user's control, users should implement the following of these tips and other best practices to decrease the risk of a virtual intruder:

**Become acquainted with the technology you will be using.** If you are new to the virtual landscape, or are using a new program, it is important to test it before your meeting so that you can maintain control.

**Use a program that only allows authenticated users.** For schools and conducting internal business, programs like Blackboard Collaborate and Microsoft Teams work well because they are connected to the individual's authenticated email and require participants to be added to the group by an administrator. It is important to find a program that works well for your community and objectives, but that also ensures some level of protection.

**Do not make meetings or classrooms public**. Instead, require a meeting password or use the waiting feature to control the admittance of guests to the room. Avoid reusing meeting identifiers, as a permanent identifier creates an analog to a physical room and can be entered and re-entered.

**Do not share the link to the room in an unrestricted, publicly visible place.** Instead, provide the link

directly to individuals who will be joining you. Ask participants not to share the meeting link or code without obtaining permission.

**Disable the "join before host" setting.** This will prevent others from using your meeting ID without you.

**Manage screen-sharing options.** Use the host-only mode, so that no one else in the room can share their computer screen besides the person who created the group unless permission is granted.

**Use the latest technology.** Be aware of updates that will produce new security enhancements. For example, some updates have blocked the ability for individuals to "scan" for rooms to join and have added passwords as defaults for meetings.

Given that in-person gatherings aren't advised at this time, our virtual spaces need to remain safe. If your organization is moving to a virtual platform for gatherings, it is important to stay literate with the technology you are using and planning for possible risks that could arise as you would with any physical gathering.

If you have any questions on this or any other topic, please reach out to any member of the Barley Snyder Education Practice Group.

**DISCLAIMER**: As we face an unprecedented time of legal and business uncertainty, we are working to provide updates on the status of important legal news related to COVID-19. It is important to note that the situation is changing rapidly and the information provided in our alerts is not intended to create an attorney-client relationship. The information contained in our alerts is for general informational purposes only and should not be construed as legal advice or a substitute for legal counsel. If you have questions about your legal situation or about how to apply information contained in this alert to your situation or about how any other information found on our website may affect your business, you should reach out to one of our attorneys. We assume no responsibility for the accuracy or timeliness of any information provided herein or by any linked site. As information changes rapidly, users are strongly advised to verify any information before relying upon it.

**WRITTEN BY:**

**Katelyn E. Rohrbaugh**

Associate

Tel: (717) 814-5006

Email: krohrbaugh@barley.com