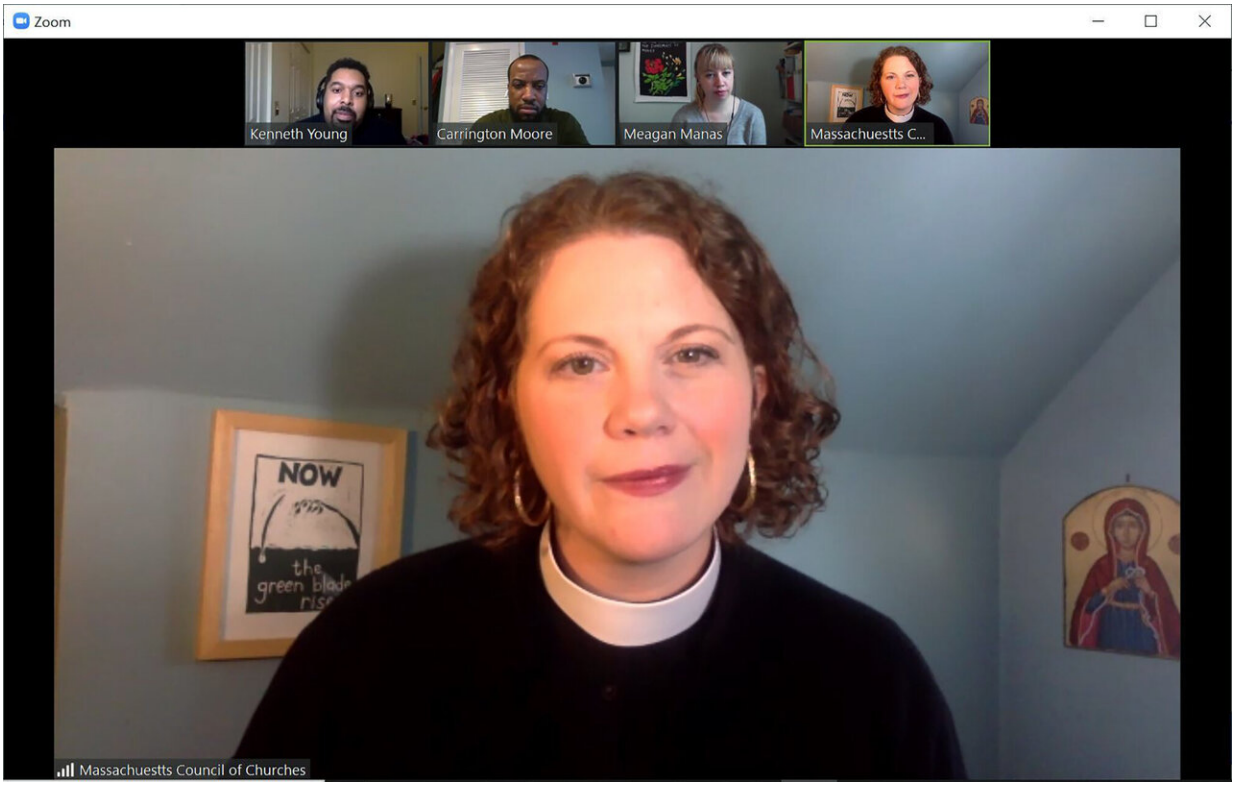
Hackers' new target during pandemic: video conference calls

April 7 2020, by Regina Garcia Cano and Aaron Morrison



In this April 2, 2020, frame from a Zoom video, the Rev. Laura Everett in Boston delivers a sermon for Boston's First Baptist Church. As Everett delivered a previous sermon, a user who had seen the church service advertised entered the video conferencing session and shouted homophobic and racist slurs. Everett said she had tweeted the link to the sermon because she wanted "the doors of the church to be open to every weary soul who is looking for a word of comfort." (The Rev. Laura E. Everett via AP)

Ceri Weber had just begun to defend her dissertation when the chaos began: Echoes and voices interrupted her. Someone parroted her words. Then Britney Spears music came on, and someone told Weber to shut up. Someone threatened to rape her.

Hackers had targeted the meeting on the video conference platform Zoom while Weber was completing the final step of her doctoral degree at Duke University. The harassment lasted 10 minutes—the result of an increasingly common form of cyber attack known as "Zoom bombing."

As tens of millions of people turn to video conferencing to stay connected during the coronavirus pandemic, many have reported uninvited guests who make threats, interject racist, anti-gay or anti-Semitic messages, or show pornographic images. The attacks have drawn the attention of the FBI and other law enforcement agencies.

"It seemed like someone was just being silly," but then the intrusions "started to get more serious and threatening," Weber recalled. "I was really in the zone and kept presenting." She said she was more concerned about others in the chat who could have been scared. She was interrupted despite having selected "mute all" in the settings for the meeting she conducted from her home in Durham, North Carolina.

A Massachusetts high school reported that someone interrupted a virtual class on Zoom, yelled profanity and revealed the teacher's home address. Another school in that state reported a person who accessed a meeting and showed swastika tattoos, according to the FBI.

The agency's field office in Boston recommended that users of video-teleconference platforms prioritize their security by ensuring that hosts have sole control over screen-sharing features and meeting invitations.

In New York, Attorney General Letitia James sent a letter to Zoom with

questions about how users' privacy and security are being protected. In a separate later, Sen. Richard Blumenthal of Connecticut sought information about how the company handles users' personal data and guards against security threats and abuse.

Zoom has referred to trolls as "party crashers," which some critics have taken as a sign the company is downplaying the attacks.

In a statement issued last week, the company told The Associated Press it takes the security of meetings seriously and encourages users to report any incidents directly to Zoom. The company suggested that people hosting large, public meetings confirm that they are the only ones who can share their screen and use features like mute controls.

"For those hosting private meetings, password protections are on by default, and we recommend that users keep those protections on to prevent uninvited users from joining," the company said. Zoom recently updated the default screen-sharing settings for education users so that teachers are by default the only ones who can share content.

Despite the update, Nevada's Clark County School District, which includes all public schools in Las Vegas, and the New York City Department of Education, which is responsible for the largest school district in the U.S., have told teachers to stop using Zoom.

Zoom-bombing was always a threat given how the video conferencing app was configured—geared more toward user-friendliness than privacy, said Justin Brookman, director of privacy and technology policy at Consumer Reports.

When shelter-at-home mandates suddenly converted Zoom into a lifeline for tens of millions of families, it became a juicy target for mischief, he said.

For years, "the usability issues outweighed the potential security issues because society was less reliant on them. Obviously, that has changed dramatically over the last month," Brookman added.

Some Zoom-bombers have been able to randomly guess meeting IDs and crash conferences not configured to keep out interlopers, he said.

In other cases, inexperienced users have exposed meeting IDs online, including U.K. Prime Minister Boris Johnson, who tweeted a screenshot of a Zoom Cabinet meeting that showed the ID and everyone's screen name.

Brookman said Zoom can do more to boost privacy protections for a massive user base that now ranges from elementary school children to senior citizens discussing their wills with attorneys.

"A lot of people, including us, are critical of how they enable hosts to surveil users to make sure they are paying attention to the screen, or reading DMs or recording the call when it's not entirely clear," Brookman said.

A mother in Georgia told a local TV station that her son was "embarrassed and a little hysterical" after someone hacked into his online class and showed pornography to the children and teacher.

The Rev. Jason Wells was holding a publicly advertised forum recently on Zoom when a troll entered and used the chat box to post a racial slur so many times that it made the feature unusable for other participants.

"I would not say this was a random vandal hoping to interrupt somebody," said Wells, who is executive director of the New Hampshire Council of Churches in Concord and co-chair of a state chapter of the Poor People's Campaign, part of a movement pioneered by the Rev.

Martin Luther King Jr. The intruder was eventually removed and blocked.

As the Rev. Laura Everett delivered a sermon via Zoom for Boston's First Baptist Church, a user who had seen the church service advertised entered the video conferencing session and shouted homophobic and racist slurs. Everett said she had tweeted the link to the sermon because she wanted "the doors of the church to be open to every weary soul who is looking for a word of comfort."

"This was, for all intents and purposes, a house of worship that was violated," she said. "Zoom and every other business bears the primary responsibility for users' safety."

In Oakland, California, Malachi Garza reported an attack on a Zoom conference she hosted for roughly 200 participants, including formerly incarcerated people who have experience with solitary confinement and are struggling with the pandemic's stay-home orders.

The conference organized by the philanthropic Solidare Network was interrupted by racist, anti-transgender language, and pornographic images were flashed on a shared screen.

Zoom needs to "tell the truth and call this what it really is," Garza said. "It's racial terror, not party crashers."