Zoombombing is a crime, not a prank, prosecutors warn



Charlotte Nation / Getty

reader comments

73 with 48 posters participating

Share this story

Coronavirus-related social distancing measures have given a big popularity boost to Zoom, a video conferencing platform that’s known for its ease of use but not necessarily strong security or privacy protections. Internet trolls and other troublemakers have responded with “Zoombombing”: joining Zoom meetings uninvited and disrupting them. Zoombombers have exposed themselves to schoolchildren and shouted racial slurs.

In a Friday statement, federal prosecutors in Michigan warned

the public that Zoombombing isn’t a harmless prank; it’s a crime.

“Hackers are disrupting conferences and online classrooms with pornographic and/or hate images and threatening language,” wrote the US Attorney’s Office for the Eastern District of Michigan. “Anyone who hacks into a teleconference can be charged with state or federal crimes.”

Possible charges include “disrupting a public meeting, computer intrusion, using a computer to commit a crime, hate crimes, fraud, or transmitting threatening communications,” the prosecutors warn. All of these charges come with the potential for fines and jail time, the authorities say.

The exact charges a Zoombomber faces would presumably depend on how they gained access to a Zoom meeting and what they did to disrupt it. For example, some Zoom meetings are advertised publicly, which might make it hard to make a computer intrusion charge stick. But someone could still be prosecuted for things they said or did to disrupt the meeting after joining it.

“You think Zoombombing is funny? Let’s see how funny it is after you get arrested,” Michigan US attorney Matthew Schneider said in Friday’s release. “If you interfere with a teleconference or public meeting in Michigan, you could have federal, state, or local law enforcement knocking at your door.”

In a recent story, Ars Technica security reporter Dan Goodin explained how Zoom users can protect themselves from Zoombombing attacks. He noted that meetings can be password-protected, and he advised against announcing login information on social media or other public channels.

Goodin notes that hosts can disable Zoom’s “Join Before Host” setting to ensure that the host is in control of a meeting from the outset. Zoom also has a “waiting room” feature,

allowing a host to verify participants before allowing them to join the meeting.

https://arstechnica.com/?p=1665930