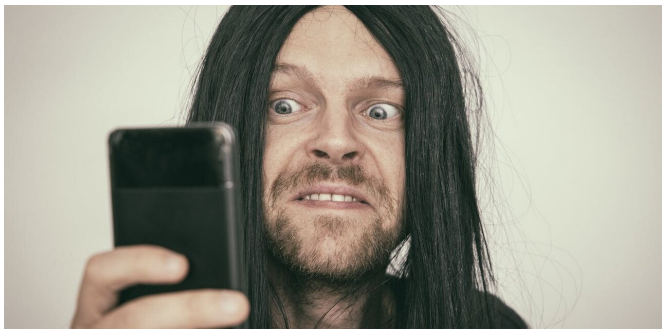
How to stop 'Zoombombers' from trolling your online meetings

3 April 2020, by David Tuffley



Credit: StanWilliams/Pixabay, Author provided

"Zoombombing" in case you haven't heard, is the unsavoury practice of posting distressing comments, pictures or videos after gatecrashing virtual meetings hosted by the videoconferencing app Zoom.

With hundreds of millions around the world now reliant on the app for work, this unfortunate trend is becoming more common, often involving a bombardment of pornographic imagery.

In some cases, online trolls have crashed alcohol support group meetings held via the app. "Alcohol is soooo good," the trolls reportedly said to one group of recovering alcoholics.

In another incident, a Massachusetts-based high school teacher conducting an online class had someone enter the virtual classroom and shout profanities, before revealing the teacher's home address.

Easy targets

The problem is that Zoom meetings lack password protection. Joining one simply requires a standard Zoom URL, with an automatically generated nine-digit code at the end. A Zoom URL looks something like this: zoom.us/j/xxxxxxxxx

Gatecrashers may only have to try a handful of code combinations before successfully landing a victim. The meeting's host doesn't need to grant permission for others to join. And while hosts can disable the screen share function, they'd have to be quick. Too slow, and the damage is done.

Last week, Zoom upgraded security on its default settings, but only for education accounts. The rest of the world needs to do this manually.

Video conferencing is incredibly valuable

Video conferencing technology has matured in recent years, driven by massive demand even before COVID-19.

With social distancing restriction, virtual meetings are now the norm everywhere. Platforms like Zoom, Microsoft's Skype and others have stepped up to meet demand.

Zoom is a cloud-based service that allows users to freely talk to and share video (if bandwidth allows) with others online. Notes, images and diagrams can also be shared to collaborate on projects. And meetings can have up to hundreds, even thousands, of participants.

How to stop the trolls

Zoom is primarily a corporate collaboration tool that allows people to collaborate without hindrance. Unlike social media platforms, it was not a service that had to engineer ways to manage the bad behaviour of users—until now.

In January, Zoom issued a raft of security patches to fix some problems. If you get a prompt from Zoom to install updates, you should—but only if these updates are from Zoom's own app and website, or via updates from Google Play or Apple's

App Store. Third-party downloads may contain malware (software designed to cause harm).

While up-to-date software is your first line of defence, another is to keep your meeting URL away from public forums such as Twitter. Anyone with meeting's URL can join, after which they're free to post comments, pictures and videos at will. If you're hosting a meeting that gets Zoombombed, disable the "screen sharing" option as quickly as possible.

Another option for more security is to use the "waiting room" function. This makes people wanting to join visible to the host, but keeps them out of the main meeting until they're allowed in. This option is turned off by default. You can enable it by signing-in to your Zoom account at https://zoom.us/ and clicking "Settings."

Other tips:

- ensure screen sharing is possible for the host only
- turn off the function that allows file transfer
- turn off the "allow removed participants to rejoin" setting
- turn off the "join before host" setting
- turn on the "require a password" setting for meetings.

Who are the trolls?

With many Zoomombing attacks being on educational institutions, it's likely a large number of these trolls are simply mischievous students who obtain meeting URLs from other students or chatrooms.

But zoombombing is by no means restricted to the classroom. With the world in lockdown, extremists of all kinds are finding ways to relieve their confinement frustration. We've known for some time that being able to operate anonymously on the web does not bring out the best in people.

At present, it doesn't appear Zoombombing is an organised criminal activity. That said, it's probably only a matter of time before someone finds a way to leverage financial reward from the practice. This could take the form of business intelligence gleaned from listening in to the meetings of rivals and competitors, in a similar fashion to planting a "bug" in the room.

Similarly, we could see a black market for Zoom URLs emerge among professional hackers, who would have new incentives to hack various systems to obtain valuable URLs.

Cybersecurity experts, privacy advocates, lawmakers and law enforcement are all concerned Zoom's default privacy settings don't do enough to protect users from malicious actors.

The bottom line

As the COVID-19 pandemic leads the world to do their work online in isolation, the technology that allows this freedom must come under close scrutiny.

Zoombombing is progressing from a student prank to more serious incidents of racist, sexist and anti-semitic hate speech.

Fortunately, safeguards aren't difficult to build into such videoconferencing technologies. This just requires a willingness to do so, and needs to be done as a matter of urgency.

Provided by The Conversation

APA citation: How to stop 'Zoombombers' from trolling your online meetings (2020, April 3) retrieved 1 December 2020 from https://techxplore.com/news/2020-04-zoombombers-trolling-online.html