What is “Zoom Bombing?”
Media Manipulation and Sociotechnical Vulnerabilities

Hosted by Joan Donovan, PhD, Research Director of the Shorenstein Center and Director of the Technology and Social Change (TaSC) Research Project
The Technology and Social Change Research Project (located at the Shorenstein Center) aims to understand how media manipulation is a means to control public conversation, derail democracy, & disrupt society.

The Media Manipulation Case Book aims to contribute to public literacy about media manipulation, political polarization, and content moderation.
Speakers

Today’s webinar speakers will be:

+ Dr. Joan Donovan, Research Director, Shorenstein Center
+ Gabby Lim, Researcher, Technology and Social Change Research Project, Shorenstein Center
+ Brian Friedberg, Senior Researcher, Technology and Social Change Research Project, Shorenstein Center
Overview

- **Joan Donovan** explains Zoom bombing and its roots in hacker cultures
- **Brian Friedberg** reviews recent cases of Zoom bombing
- **Gabby Lim** provides some tips for preventing Zoom bombing
- **Brian Friedberg and Gabby Lim** will provide tips for improving cybersecurity at home
- **Q&A**
Definitions

**Zoom Bombing:** The act of hijacking a virtual meeting disrupt communication, sometimes just for fun, but also for more targeted reasons.

**Sociotechnical Vulnerabilities:** Sociocultural and technical conditions, that while not inherently vulnerabilities, when combined lead to unique exploits that can be taken advantage of by threat actors.
Life Cycle of a Manipulation Campaign

1. Manipulation campaign planning

2. Seeding campaign across social platforms and web

3. Responses by industry, activists, politicians, and journalists

4. Changes to information ecosystem

5. Adjustments by manipulators to new environment
Media Manipulation
From Phone Mobs, Online Raids, to Zoom Bombing

(image credit artist Kotryna Zukauskaite)
Who are Zoom bombers?

+ Zoomers: Trolls, Gen Z students stuck at home

Matthew
@Matthew4Office

Wow if you Keyword search “zoom code” on twitter you can find many classrooms to join! How strange

10:53 PM · 01 Apr 20 · Twitter for iPhone
Where are attacks coordinated?
+ Discord, 4chan, Reddit, Private Messaging
Where are attacks coordinated?
+ New Discord servers dedicated to Zoom bombing

Business Insider

‘Alcohol is soooo good’: Trolls are breaking into AA meetings held ...

"Alcohol is soooo good," an intruder said to recovering alcoholics during a Tuesday AA meeting on Zoom.
Where are the attacks shared?
+ Youtube, TikTok, Twitch, Twitter & Instagram
Networked harassment on Zoom
+ How should platforms and journalists respond?
Tips to Prevent Zoom Bombing

(image credit artist Francesco Ciccolella)
Tips to Prevent Zoom Bombing

Before the call - Centralize control

✔ Only allow hosts to control video/audio
✔ Begin call with all video/audio muted
✔ Only allow hosts to screen share
✔ Do not reuse old Zoom links
✔ Set chat setting so participants can only message the hosts

(image credit artist Kotryna Zukauskaite)
Tips to Prevent Zoom Bombing

Before the call - Raise barriers to entry

✔ Require registration
✔ Ask people to sign up for a Zoom account with a recognizable name or nickname
✔ Send link to the call about 30 mins ahead of time
✔ Add a meeting password
✔ Disable join before host

(image credit artist Kotryna Zukauskaite)
Tips to Prevent Zoom Bombing

During the call:

✔ Keep everyone’s audio/video off (except for the hosts)

✔ Lock the meeting after participants have joined

✔ Avoid sharing sensitive information

(image credit artist Kotryna Zukauskaite)
Tips to Prevent Zoom Bombing

After the call - if you’ve been zoombombed:

✔ Gather evidence (screenshots, Zoom recording, chat logs, participant list)
✔ Report event to local IT admin and Zoom
✔ Remove all Zoom links from website and public calendars
✔ Don’t feed the trolls - refrain from reacting in the moment or publicly

(image credit artist Kotryna Zukauskaite)
Cyber attacks on the rise

+ There has been an uptick in hacking attempts worldwide.
+ Scammers are exploiting the infodemic and impersonating the CDC.
+ Be wary of other trolling campaigns targeting public officials, educators and journalists.

Tips and resources

+ Protect your accounts with secure password management
+ Be alert for hacking, phishing and impersonation
+ Practice safe browsing
+ Check in on the cyberhealth of friends and family
Democracy During a Pandemic

Joan Donovan  Setti Warren  Nancy Gibbs  Rob Faris

***

Sign up for Meme War Weekly and the Shorenstein Center email newsletter to be notified of the dates of these upcoming webinars
Thank You!

Sign up for Meme War Weekly
shorensteincenter.org/memewar

For more information contact
manipulation@hks.harvard.edu

Learn more about TaSC and the Media Manipulation Case Book [here](https://shorensteincenter.org/memewar)

(image credit artist: [Ana Hill](https://anahill.com))