Zoom Meeting Attack
By: Michael Smith, Mike Tech Show,
https://mikenation.net
10/08/25

If a Zoom call is hacked—such as through unauthorized disruptions, "Zoom bombing," or a suspected breach—respond quickly to protect participants and secure your data.
Immediate Response Steps

- Start recording the session to preserve evidence of the incident, including any threats or harassment.
- Remain calm and talk over disruptive content, clarifying to meeting attendees that the behavior is unsanctioned.
- Remove the disruptive participant using host controls, and if necessary, pause or end the meeting briefly to reconfigure security settings.
- Report the incident directly to Zoom's Trust & Safety team using their online reporting form to assist with further investigation.

Account and Data Protection

- Change your Zoom account password immediately, ensuring it is unique and strong.
- Enable two-factor authentication (2FA) for your Zoom account and any related services.
- If meeting links/passwords were publicly posted, reset those credentials and distribute new invites through secure channels.
- Monitor your Zoom and email accounts for unauthorized activity and reset passwords for any other accounts that may use similar credentials.

Remove a disruptive participant

To remove a disruptive participant during a meeting (such as Zoom or Teams), open the participant list, find the disruptive individual, and use the in-meeting controls (often represented by three dots next to their name) to remove them from the session immediately. This action will eject them from the meeting and typically prevent them from rejoining, especially if you have enabled settings like "Allow removed participants to rejoin: OFF".

Steps for Quick Removal

- Locate the participant list or attendee panel in your meeting platform.
- Click on the three dots or options menu next to the disruptive participant's name.
- Select "Remove," "Eject," or the equivalent action to instantly remove the person.
- Optionally, use features such as muting microphones, disabling chat, or suspending participant activities while identifying and removing the disruptor, particularly in Zoom.

Prevention for Future Meetings

- Enable waiting rooms and use meeting passwords to limit access to trusted participants.
- Avoid posting meeting links or passwords on public forums or websites.
- Familiarize hosts/co-hosts with security controls, such as muting and removing participants, and locking meetings once all invited members have joined.
- Update Zoom to the latest version to ensure you benefit from current security patches and features.
- Following these practical steps helps mitigate the impact of a Zoom hack and reinforces meeting security going forward.