

Protecting Your Zoom Meetings from Unauthorized Recording

The Issue

A company called WebinarTV has been scanning the internet for public Zoom links, sending bots into meetings as silent attendees, recording everything, and publishing the results as AI-generated podcasts, without notifying participants. This isn't a data breach in the traditional sense: no passwords were stolen. WebinarTV treated your meeting link as a public invitation.

The culprits are browser extensions with calendar access combined with publicly posted meeting links. If your meeting link was never public and no attendees had compromised extensions, the risk is lower. For most organizations hosting educational webinars with broadly shared links, though, the risk is real. These steps address the known vectors.

Immediate Actions

1. Treat your meeting link like a key, not a flyer. If you wouldn't post it on a public bulletin board, don't share it in a newsletter, social post, or broadly forwarded email. The link itself is the attack surface. WebinarTV and similar services crawl for publicly accessible Zoom URLs.

2. Require registration and manually approve attendees. This is the most effective single control for sensitive calls. Bots register with fake email addresses, often at unusual domains. Manual review catches them before they join. Enable under Zoom: Security > Registration > Manually approve.

3. Audit every browser extension with calendar or meeting access. AI note-taking tools, transcription assistants, and meeting automators are the primary vector. Any extension with calendar permissions can read your meeting invitations and links. Open your browser's extension list, remove anything unfamiliar, and turn on permission prompts so extensions must ask before accessing calendar data.

4. Search for yourself on WebinarTV.us now. Search your name and your organization's name. If anything appears, request removal at remove@webinartv.us and document everything before submitting.

Zoom Settings to Enable

Watermarking. Zoom's watermarking embeds participant information into video, creating accountability and deterring unauthorized recording. Account Settings > Recording > Watermark.

Recording consent notifications. This prompts participants when recording starts and requires acknowledgment. It doesn't stop external screen recorders, but creates a documented notification event. Settings > Recording > Recording Consent.

Revision #1

Created 6 June 2026 02:20:51 by Josh

Updated 6 June 2026 02:29:50 by Josh