Subject: Important Update on Unauthorized Webinar Scraping & Strengthened Zoom Security Measures

Dear CFUW Members,

We are writing to inform you of an important issue that was brought to our attention yesterday regarding unauthorized reposting of some of our CFUW-hosted Zoom webinars by a platform called **WebinarTV.us**. We want to ensure full transparency, explain what we have learned, outline the steps we are taking, and provide clear guidance on what you can do to help prevent this from happening again.

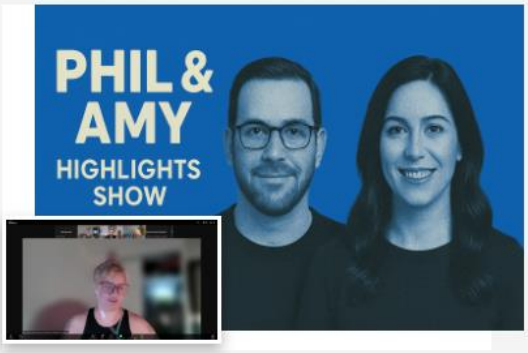
What Happened

We discovered that **WebinarTV.us has been scraping and reposting webinars** from a wide range of organizations, including ours. Independent cybersecurity reports confirm that WebinarTV is actively **scraping both public and private Zoom webinars without organizers' consent**, often gaining access through **fake registrations or third-party AI transcription tools** inadvertently connected to Zoom meetings.

In many reported cases—including ours—organizations first learned that their webinars had been taken only after receiving an email from someone claiming to be **"Sarah Blair"**, notifying them that their video was available on Webinartv.us and offering a link to remove it. This pattern aligns with what others have documented across multiple Zoom-related reports. Below is an example of one of the received emails.

Hi,

Your webinar is featured on the Phil & Amy Show. They talk about the highlights from your webinar - without giving away too much - to entice viewers. To listen to the show, click Highlights tab on the OnDemand page or click here.



Let me know if you have any questions!

Note: WebinarTV is designed to promote and market public webinars. If you don't want to participate, go here and click the Remove button. Your webinar will be automatically removed and future webinars avoided.

— Sarah
WebinarTV.us

Important:

✓ **This is not a hacking incident.**

✓ The webinars that were reposted were **public webinars only**.

✓ **No email addresses, phone numbers, or personal identifying information were leaked.**

✓ The issue results primarily from **unauthorized participants joining via disguised emails or AI bots**, not through any breach of our systems.

What We Are Doing on the CFUW Side

We are taking strong, immediate steps to safeguard all clubs and national accounts going forward:

1. Removing Unauthorized Content

We have already removed most reposted webinars using the platform's takedown requests and reached out directly to Webinartv.us to remove the remaining ones.

2. Strengthening All CFUW Zoom Security Settings

In accordance with Zoom's own security best practices including enabling passcodes, waiting rooms, and avoiding public posting of join links, we have made sure to have:

- Enabled **passcodes on all Zoom meetings**.
- Enabled the **Waiting Room** in every CFUW Zoom account (recommended by Zoom as a primary defense).
- Ensured **no direct Zoom meeting links** will be posted publicly on our website, only registration links.
- Closely reviewed registrant lists and have begun **blocking suspicious email domains** at the Zoom account level.

3. Monitoring and Proactive Screening

We are manually reviewing all registration lists ahead of events and adding any suspicious accounts to our blocklist. Reports from cybersecurity experts show that unusual or newly created email domains (e.g., *lightconnect.space*, *bestwest.space*) have frequently been used in scraping incidents.

What You Can Do to Help

To reduce risk when using the national Zoom account for your club events, we kindly ask all hosts and coordinators to take the following steps:

1. Carefully Review Registrant List Before Each Meeting

Scraping almost always occurs through a registrant who joins silently and records through a bot. Carefully **deny any suspicious or unidentifiable registrants and** report them to us so we can block them. This matches ongoing advice from cybersecurity organizations encouraging organizers to screen attendees.

2. Do Not Allow Third-Party AI Transcription Tools

Reports indicate that unauthorized AI-powered transcription or note-taking bots can join meetings without the participant's awareness and leak data to third-party platforms like WebinarTV. Instead:

- Request CFUW to enable **Zoom's built-in transcription**, or
- Request the meeting recording afterward if needed.

3. Share Recordings Only with Registered Attendees

After events, please do **not post recordings publicly** unless approved. Cybersecurity guidance strongly warns against publicly accessible links because they can be scraped and reposted automatically.

4. Check Your Junk Mail for "Sarah Blair / Webinartv.us" Notifications

If you receive an email stating your webinar was posted on their platform, please use the removal link if it pertains to your event.

5. Always Use Registration Links with Screening Questions

If you are inviting multiple people or external guests, **require registration** and use screening questions to identify legitimate participants. Zoom and security experts emphasize avoiding direct join links and instead requiring registration to prevent uninvited guests.

Reassurance

We want to emphasize again:

- **Your data is not compromised.**
- **No CFUW accounts have been breached.**
- **This is an external scraping issue affecting many organizations internationally**, and we are actively on top of it.

Our Zoom rooms remain secure, and enhanced protections are already in place.

If you have questions, concerns, or if you notice suspicious registrants or emails, please contact us immediately. Thank you for your cooperation and vigilance as we work together to keep CFUW's virtual spaces safe.

Warm regards,
CFUW National Office

Resources:

To learn more about how webinar scraping occurs and recommended security practices, you may consult the following reputable sources:

- **CyberAlberta Report on WebinarTV Scraping**
  Detailed overview of how WebinarTV gains access to webinars (often through third-party tools or fake registrations) and why many organizations are affected.
  https://cyberalberta.ca/zooming-out-webinartvs-rampant-scraping-of-online-meetings
- **Zoom's Official Security Guidance**
  Zoom's own recommendations for preventing uninvited guests, securing meetings with passcodes and waiting rooms, and managing registration securely.
  https://www.zoom.com/en/products/virtual-meetings/resources/securing-your-meetings/

Email:

Hi (Name),

I'm reaching out to let you know that we recently discovered your CFUW webinar that you hosted on Zoom …. was reposted without authorization on a third-party website called **WebinarTV.us**. This issue has affected many organizations, and reports show that WebinarTV obtains access by registering for events under disguised or automated email addresses, or through third-party AI transcription tools that inadvertently expose meeting information. I want to reassure you right away that this was **not a hack**, only **public webinars** were affected, and **no personal information—such as email addresses or phone numbers—was leaked**.

As soon as we became aware of this, we submitted takedown requests for all posted CFUW content through Webinartv's removal links and contacted the company directly. We will continue to follow up until everything is removed, as others have noted that persistence is sometimes required. We have also strengthened all national Zoom account security settings—passcodes, waiting rooms, and tighter registration controls—aligned with Zoom's recommended best practices to prevent uninvited participants from joining going forward.

If you haven't already, please check your inbox and junk mail for an email from **Sarah Blair** or **@webinartv.us**, which many organizations receive when their webinar is posted. If you find one, you may use the link provided to request removal from your side as well. Additionally, please avoid allowing any third-party AI transcription or note-taking tools in future meetings, as several scraping cases have been linked to unintended access through these extensions. If you ever need transcription, please use Zoom's built-in version instead.

I want to emphasize again that your information is safe, the issue is external, and you did absolutely nothing wrong. This situation is unfortunately affecting many organizations, but we are actively addressing it and improving our security measures, so our virtual spaces remain safe and trusted. Please feel free to reach out if you have questions or would like assistance with anything related to this matter. We are here to support you.

Warm regards,
CFUW National Office