



Centro de
Formación Docente
UVP



UVP
UNIVERSIDAD
DEL VALLE DE PUEBLA



| www.uvp.mx |

#YolohagoUVP

Recomendaciones Académicas

Boletín No. 8: ¿Qué es el zoombombing y cómo evitarlo?

M. en C. Rey Jesús Cruz Galindo
Coordinador del Centro de Formación Docente
coord.formaciondocente@uvp.mx

Introducción

La utilización de las tecnologías de la información y la comunicación (TIC), así como de las tecnologías del aprendizaje y del conocimiento (TAC) implican, hoy en día, que el profesorado cuente con las herramientas básicas para el uso adecuado de la diversidad de aplicaciones, plataformas y programas en su práctica docente.

A partir de las medidas tomadas por las instituciones educativas para el proceso de continuidad académica, se comenzaron a utilizar con mayor frecuencia algunas aplicaciones que permiten llevar a cabo una clase en modalidad virtual. En lo que corresponde a UVP, recordemos que se han utilizado Google Meet y Zoom. No obstante, es indispensable advertir de posibles ataques cibernéticos y, especialmente en la segunda aplicación mencionada.

Lo anterior tiene que ver con una nueva forma de ataque cibernético denominado “Zoombombing”, por lo “que hackers entran sin invitación a chat rooms y transmiten contenido inapropiado, como insultos verbales de índole racista, sexista o contenido pornográfico” (García-Bullé, 2020, párr. 2). También es entendido como “una forma de trolling que interrumpe las reuniones y clases en línea con lenguaje o imágenes perturbadoras a través del uso compartido de pantalla” (University of Michigan, 2020, párr. 1). En este sentido, el objetivo de este boletín es compartirte recomendaciones para prevenir el “Zoombombing” en tus clases. Es indispensable tomar las medidas de seguridad más pertinentes para evitar este tipo de situaciones en tu práctica docente.

Sugerencias para prevenir y evitar el Zoombombing

A continuación, en la figura 1 te compartimos las sugerencias que García-Bullé (2020) a través del Observatorio de Innovación Educativa de Instituto de Estudios Superiores de Monterrey, comparte para prevenir y evitar este tipo de ataques.

1. Usa los *waiting rooms* y las contraseñas

- Para controlar el acceso a los *chat rooms* se recomienda usar la función que permite proteger las juntas virtuales vía contraseña de acceso, así como hacer uso de las salas de espera en las que los participantes pueden estar mientras el host aprueba su integración a la sesión virtual.

2. Mantén el control de la pantalla

- El anfitrión debe mantener en todo momento el control de lo que se transmite en pantalla, si un participante quiere compartir contenido, es recomendable que lo envíe previamente al host para su transmisión en la junta.

3. Informa a tus invitados

- Habla con los participantes de la sesión sobre *zoombombing* y practica con ellos tanto las medidas precautorias como las posibles estrategias para detener los ataques y/o mitigar sus efectos.

4. Asigna a una co-anfitrión

- Usualmente el anfitrión está a cargo de la logística de una junta o sesión virtual, pero ante la amenaza de un ataque, la velocidad y calidad de la respuesta puede no ser idóneas, porque el anfitrión tendría que encargarse de la logística de la junta y la de la defensa de sala de chat al mismo tiempo, es recomendable tener una persona con la que se puedan dividir las tareas y organizar una defensa efectiva mientras se mantienen los propósitos básicos de la sesión.

5. Crea una atmósfera de seguridad y empoderamiento

- Aun si preparas a tu equipo, sigues todas las medidas de seguridad de la plataforma y practicas estrategias con tus invitados, no eliminarás el totalmente el riesgo de *zoombombing*. Por lo que es importante hablar previamente sobre los efectos que podría tener un ataque como este y cómo lidiar con ellos para generar respuestas que frenen la incursión. En palabras más simples, no se trata de decirles a los participantes que el espacio en el que están es 100 % seguro, sino de inspirar en ellos la confianza como para no ser inhabilitados durante un *zoombombing* y responder adecuadamente para frenar el ataque lo antes posible.

Figura 1. Precauciones que tomar para evitar el “zoombombing”.

Fuente: García-Bullé (2020, párr. 5-9).

Es importante señalar que, aunque se tomen las medidas de seguridad necesarias, es posible que, si se sufre del ataque de un “zoom bomber”, por lo que en la figura 2 te compartimos algunas recomendaciones sobre cómo actuar en caso de ser víctima de zoombombing en tus clases.

1. Problematizarlo

- Estar del otro lado de un agresor de cualquier tipo activa uno de nuestros reflejos más básicos, el de pelear o huir. Al conceptualizar una situación de *zoombombing*, como una agresión al momento en el que pasa, corremos el riesgo de responder agresivamente de acuerdo al instinto de pelear, de alejarnos de la computadora dejando el control a los atacantes, siguiendo el instinto de huir o de congelarnos ante una reacción de pánico si no pudimos escoger ninguna de las opciones anteriores. Si nos aproximamos a un ataque de *zoombombing* como un problema, en vez de una agresión, es más fácil usar mecanismos que nos ayuden a mantenernos en calma e implementar soluciones inmediatamente.



2. Coordina la defensa

- Muchos ataques de *zoom bombers* son incursiones coordinadas de equipos de *hackers* que entran a los *chat rooms* y montan ofensivas estratégicas, para contrarrestarlos efectivamente la defensa debería ser igual de coordinada y rápida. El anfitrión puede hacer uso de las medidas de seguridad, como remover a los *zoom bombers* de la junta, limitar el uso de pantallas compartidas y restringir el chat. Otros participantes deberán tomar la tarea de recabar información que ayude a identificar a los atacantes, como *screenshots* (pantallazos) y nombres de usuario, y otros manteniendo la comunicación dentro del grupo para monitorear el bienestar emocional de los invitados a la videollamada.



3. Discierne los impactos

- La idea del *zoombombing* es irrumpir en espacios virtuales y exponer a otras personas a contenido inapropiado, agresivo, y ofensivo, pero no hay un solo criterio sobre lo que puede ser ofensivo para un grupo de personas. Habrá participantes que no se sientan tan violentados o afectados por los comentarios y contenidos que los *zoom bombers* impongan en sus espacios, y habrá otros especialmente sensibles a mismo contenido.
- Es crucial tener en cuenta estas diferencias personales y tratar el problema del impacto causado por el ataque en una base de caso por caso. Establecer comunicación, diálogo, acompañamiento y un camino a buscar la ayuda adecuada, no de acuerdo a un criterio general sino a una percepción individual de cómo vivió cada uno de los participantes la experiencia de un ataque de *zoom bombers*.

Figura 2. Recomendaciones ante un zoombombing.

Fuente: García-Bullé (2020, párr. 11-16).

A manera de conclusión

Tomando en cuenta las consideraciones anteriores respecto a las sugerencias para prevenir y evitar el zoombombing, así como las recomendaciones para un buen actuar frente a un ataque en la videoconferencia, resulta necesario que, como usuarios frecuentes de Zoom, aprendamos a utilizarlo de la mejor manera posible.

De acuerdo con el blog de esta aplicación, a finales de diciembre de 2019, participaban máximo 10 millones de personas al día en videoconferencias; no obstante, para marzo de 2020 el número aumentó considerablemente a 200 millones de usuarios por día (Yuan, 2020). Por lo tanto, enseguida te compartimos otras recomendaciones para que te encuentres preparado y asegures cada una de tus videoclases.

Agradeceremos que nos puedas compartir tus experiencias y/o sugerencias ante este tipo de situaciones a los correos dir.educacion@uvp.mx y coord.formaciondocente@uvp.mx

Sitios recomendados:

- Cómo configurar ZOOM para máxima seguridad en tus videoconferencias ([ver aquí](#)).
- Cómo mejorar la seguridad de sus reuniones con Zoom ([ver aquí](#)).
- How to Secure Meetings in Zoom ([ver aquí](#)).
- Quick Start Guide: Secure Meetings in Zoom ([ver aquí](#)).
- Controles de anfitrión en una reunión ([ver aquí](#)).
- How to Keep Uninvited Guests Out of Your Zoom Event ([ver aquí](#)).

Referencias

García-Bullé, S. (2020, 11 de mayo). Cómo prevenir y frenar el "zoombombing".

Observatorio de Innovación Educativa del Tecnológico de Monterrey.

<https://observatorio.tec.mx/edu-news/como-prevenir-zoombombing>

University of Michigan (2020). How to Secure Meetings in Zoom. *Information and technology services.*

<https://its.umich.edu/communication/videoconferencing/zoom/how-to-secure-meetings#:~:text=Overview,classes%2C%20and%20community%20are%20protected.>

Yuan, E.S. (2020, 01 de abril). Mensaje para nuestros usuarios. *Zoom blog.*

<https://blog.zoom.us/wordpress/es/2020/04/01/mensaje-para-nuestros-usuarios/>