



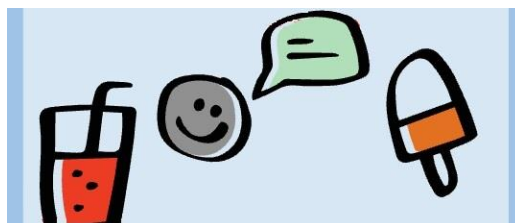
SOBRE LA SEGURIDAD DE USO DE LA PLATAFORMA ZOOM

Argumentario del equipo organizador de las Meriendas Filosóficas

Mucha es la información que ha circulado estos días sobre la plataforma Zoom, pero no toda esa información es cierta, está actualizada o sigue siendo un problema. Os contamos nuestra experiencia e investigación sobre este tema.

Índice

1. **Bulos que circulan.**
2. **Qué hay de verdad y de mentira en los problemas de seguridad y privacidad y otras vulnerabilidades de Zoom**
3. **Recomendaciones de seguridad en el uso de internet y de cualquier plataforma de videollamadas (para organizadores y para participantes)**
4. **En resumen: ¿es necesario desinstalar la aplicación Zoom y cerrar nuestras cuentas de usuario?**



1. Bulos que circulan

Empecemos descartando algunos de los bulos que circulan:

- Sobre el **mensaje de la Guardia Civil** circulando por WhatsApp, invitando a desinstalar el programa: resulta que aprovecharon una publicación de la Guardia Civil, pero añadieron el texto sobre la desinstalación del programa, como si esto fuera una recomendación oficial. La propia Guardia Civil lo desmiente en el siguiente tweet:

<https://mobile.twitter.com/guardiacivil/status/1248626191898013698>

Además, añadir que en todos los tweets de la Guardia Civil que han publicado hablando sobre Zoom, la propia plataforma Zoom ha contestado en sus hilos informando de la situación. De hecho, en el tweet del [1 de abril](#) sobre las vulnerabilidades de Zoom, la plataforma responde diciendo que están trabajando en ello (y, desde entonces, han publicado dos actualizaciones); en el tweet del [8 de abril](#) hablando de una vulnerabilidad concreta, la Guardia Civil publica información desactualizada, pues Zoom les contesta diciendo que esa vulnerabilidad fue resuelta, en menos de 24 horas, el 1 de abril. El [10 de abril](#), la Guardia Civil transmite el mensaje de Zoom y de OSI diciendo que se debe mantener actualizada la app Zoom para estar al día en las correcciones de seguridad y privacidad.

- Sobre el audio que habla de una **estafa de banco**, información publicada también en periódicos y radio: en realidad, la investigación no asegura aún que el fraude haya sido cometido a través de la app de Zoom; tampoco se sabe si esta persona instaló la app original, o algunas de las apps fraudulentas que circulan (recomendamos descargar la app siempre de la página oficial: <https://zoom.us/download>); y tampoco se sabe si fue causado por un uso (responsable o imprudente) que hicieron las hijas de esta pareja con el teléfono y Zoom. Podéis leer la información contrastada por Maldita Hemeroteca, web especializada en contrastar informaciones y bulos:

<https://maldita.es/malditobulo/2020/04/10/robo-zoom-19000-euros-guardia-civil-aplicacion-estafa-fraude-banco/>

En este punto, os pedimos, siempre, comprobar la información en fuentes originales y oficiales. Sabemos que es trabajoso, y que no siempre tenemos ganas y tiempo para ello... Pero difundir noticias falsas, o asustarse ante informaciones no contrastadas, genera alarmismo, miedo y pánico, y nos consume mucho más, cerrándonos posibilidades y pudiendo perjudicar a asociaciones, proyectos o empresas que estén utilizando esta plataforma, intentando aportar su granito de arena y ayudar en estos tiempos difíciles.

2. Qué hay de verdad y de mentira en los problemas de seguridad y privacidad y otras vulnerabilidades de Zoom

Es cierto que la aplicación ha tenido una serie de fallos de seguridad y privacidad desde que, en el mes de marzo, empezará la cuarentena global y aumentara el número de usuarios de la misma de manera muy masiva. La mayor parte de esos problemas han sido subsanados, y han sido numerosos los comunicados de la plataforma, que ha detenido el desarrollo de sus aplicaciones para centrarse en la reparación de estos fallos. De hecho, desde el 1 de abril, se han publicado ya varias actualizaciones de la aplicación, en las que se reparan muchos de estos problemas. Y siguen trabajando en ello.

Por otro lado, trascienden noticias de que muchas organizaciones (entre ellas, el famoso Google) han dicho a sus trabajadores que desinstalen la aplicación de todos sus dispositivos y de que no la usen en sus empresas. Esta cuestión debe ser valorada en contexto: por un lado, Zoom ha tenido que cambiar su política de privacidad, ya que no estaba del todo claro para qué podían utilizar los datos e informaciones que recopilaban de los usuarios. Siendo así, ninguna empresa va a arriesgarse a que otra empresa, en este caso Zoom, pudiera tener información importante, sin saber qué hacían con ella.

No nos olvidemos tampoco de la "guerra comercial" que se ha librado entre muchas empresas de telecomunicaciones y videollamadas, siendo Zoom la que estaba en el ojo del huracán, al ser la plataforma que mayor crecimiento y popularidad había alcanzado en este tiempo de cuarentena. Por tanto, sin entrar en temas de ética profesional ni acusaciones directas, es comprensible que cualquier noticia que pueda perjudicar el nombre y marca de Zoom (como que Google le ha dicho a sus trabajadores que desinstalen Zoom de sus dispositivos) será aplaudida por las marcas competidoras.

Siguiendo con los problemas surgidos en Zoom, algunos de estos se pueden atribuir a la propia aplicación, pero otros son más genéricos y afectan a medidas de seguridad que siempre deben tenerse en Internet. Los primeros, como ya hemos dicho, han sido subsanados en su mayor parte, y siguen trabajando en ello; los segundos, que afectan no sólo a Zoom, sino a cualquier otra aplicación, dependen del uso responsable de los usuarios y de las medidas de precaución que estos tomen con sus contraseñas y su forma de interactuar en Internet.

Respecto a los primeros, os compartimos este enlace de Maldita Hemeroteca, donde hacen una recopilación bastante completa:

<https://maldita.es/malditatecnologia/2020/04/09/brechas-seguridad-aplicacion-zoom/>

Respecto a los segundos, os compartimos en el siguiente apartado unas cuantas medidas de precaución que se deben tener siempre.

3. Recomendaciones de seguridad en el uso de internet y de cualquier plataforma de videollamadas

Lo que queremos transmitir es que hemos elegido esta plataforma para las Meriendas Filosóficas porque creemos que es una plataforma suficientemente segura para esta actividad, tanto como otras, siempre que se tomen unas medidas de precaución suficientes. Por ello, os enviamos estas medidas de seguridad generales y básicas:

Para organizadores de reuniones

- Llevad un control de quién asiste a las reuniones y procurad no difundir los enlaces de conexión a las reuniones públicamente: en todo caso, procurad llevar un seguimiento de quién se conecta y se desconecta, para tener la seguridad de que no se conecta una persona malintencionada;
- Supervisad en todo momento lo que se publique en el chat, no permitiendo que se compartan archivos ni enlaces sin permiso de la organización (para evitar la difusión de enlaces o archivos maliciosos).
- Configurad la plataforma para evitar el envío de chats privados directamente entre usuarios, para evitar que alguien pueda estar mandando mensajes por privado con enlaces o archivos maliciosos, a espaldas de la organización del evento;
- Vigilad lo que sucede en las cámaras de la reunión durante la duración de la misma, para evitar actos desagradables o sensibles de personas malintencionadas.
- Os compartimos, además, estas medidas de seguridad compartidas por la propia plataforma Zoom para configurar las reuniones, de la manera más segura (en inglés): https://twitter.com/zoom_us/status/1248541667742924802

Para los usuarios (tanto para Internet como para videoconferencias)

- Tened siempre las aplicaciones actualizadas a su última versión (las actualizaciones corrigen problemas de seguridad y privacidad, en muchos casos). Os compartimos esta recomendación dada por parte de la Oficina de Seguridad del Internauta, en esta línea: <https://www.osi.es/es/actualidad/avisos/2020/04/actualiza-la-ultima-version-de-zoom>;
- No clicar nunca en ningún enlace o archivo enviado en el chat de una reunión pública que no haya sido verificado por las personas que organizan dicha reunión, o cuando no se tenga la seguridad de que la persona que lo envía es de confianza (esto sirve igual para cualquier enlace o archivo que encontremos en Internet, en cualquier web);

- No guardar en el navegador ni en un archivo de texto del ordenador datos ni contraseñas que sean de uso sensible o que se quiera evitar su posible robo (contraseñas de banco, contraseñas de tarjetas de crédito, y ya cada cual que valore la importancia de la contraseña de su correo o redes sociales);
- Se recomienda procurar no tener la misma contraseña para todo, pues si te robaran una, ya podrían acceder a cualquiera de tus cuentas registradas. También es medida habitual de seguridad cambiar las contraseñas periódicamente.
- Ninguna empresa va a solicitar datos personales como nombres de usuario, contraseñas o cuentas de banco por un chat, un email o por whatsapp. En caso de recibir algún mensaje sospechoso en esta línea, intentad consultar fuentes oficiales antes de hacerlo: consultad la página oficial de la empresa, o llamad al teléfono de atención al cliente.
- Mantened actualizados vuestro antivirus y vuestros programas anti-malware, y haced escaneos periódicos para eliminar cualquier tipo de virus o archivo malicioso que haya podido instalarse en vuestro dispositivo.
- Comportaos siempre de manera razonable cuando estéis en el mundo virtual (en Internet o en cualquier red social o plataforma de videollamadas), del mismo modo que lo haríais en la calle, en casa o en vuestra vida cotidiana: no confiéis de primeras en personas que no conocéis de nada; no deis datos personales ni información sensible (contraseñas, cuentas de banco) a personas desconocidas; no aceptéis ofertas o "regalos" de personas que no sean de confianza; no difundáis mensajes en cadena que sean sospechosos de ser bulos, que den información falsa, o que no hayan sido verificados con fuentes oficiales y legítimas. La analogía con nuestra vida cotidiana, y el uso razonable de Internet, es la mejor manera de ser responsables y de mantener nuestra seguridad, y la del resto. Pensad que la vía más habitual para instalar un virus o un troyano (sí, como el caballo de Troya) en vuestro dispositivo, y poder acceder al control e información de vuestros dispositivos, casi siempre requiere de la participación del usuario, cuando éste clicka en alguna parte o da directamente sus datos personales.

Esperamos, con esta información y estas recomendaciones, transmitir os la seguridad y confianza que nuestra organización siente en esta plataforma Zoom, y que le ha llevado a seguir utilizando esta herramienta en sus proyectos y actividades, además de por haberla valorado mejor y más adecuada que las otras muchas que hay en la Red.

4. En resumen: ¿es necesario desinstalar la aplicación Zoom y cerrar nuestras cuentas de usuario?

Creemos que no hay motivos suficientes para ello. Otras aplicaciones (como WhatsApp) han tenido problemas de seguridad y privacidad en el pasado, pero no por ello la hemos desinstalado de nuestros dispositivos, o nos hemos cambiado a otras aplicaciones que cuidan más de la privacidad (como Telegram, por ejemplo). Del mismo modo, sabemos que cuando abrimos un perfil en una plataforma cualquiera (como Facebook, Instagram, o el mismo Google), aceptamos unas condiciones de uso, seguridad y privacidad que, en la mayor parte de las ocasiones, no hemos leído, autorizando al uso e incluso venta de nuestra información personal y privada por parte de estas empresas. ¿Acaso lo que sucede con Zoom es algo diferente?

Ningún programa ni plataforma informática es plenamente segura, ni ninguna está libre de sospecha para poder tirar la primera piedra: Zoom tampoco, pero no es la única. Por tanto, creemos que lo sucedido con Zoom, y aceptando sus fallos cometidos, sólo responde a una situación particular, en la que todos y todas estamos algo nerviosos, exagerando y sobredimensionando el problema, perdiendo la perspectiva y el contexto (y, quizá, siendo "víctimas" de una "guerra comercial" entre plataformas).

Dicho esto, cada cual es libre de dar o no su confianza a esta o cualquier otra plataforma, y actuar en consecuencia: esto es sólo una forma de compartir la perspectiva de este equipo de las Meriendas Filosóficas, para justificar por qué seguimos usando esta plataforma, y por si ayuda a alguien a aclarar este problema. Pero, hagáis lo que hagáis, no os olvidéis nunca de seguir las recomendaciones básicas que os hacemos sobre difusión de informaciones, y sobre seguridad y privacidad en Internet: creemos que son fundamentales para todo usuario y usuaria de la red, se decida lo que se decida.

Esperamos que el uso de la plataforma Zoom no sea un inconveniente para vuestra participación en nuestra actividad.

Equipo organizador de las Meriendas Filosóficas.