https://latam.kaspersky.com/resource-center/threats/video-conferencing-security-how-to-stay-safe

Videollamadas y videoconferencias en línea: cómo mantenerse a salvo de los hackers

Desde la llegada de la Covid-19, muchas actividades presenciales pasaron a hacerse a distancia. Desde la educación de los niños y el teletrabajo a gran escala hasta mantener el contacto con familia y amigos, confiamos cada vez más en la internet para mantenernos conectados, y parece ser una tendencia que va a continuar creciendo.

Las videoconferencias cumplen un rol principal en esto. En abril del 2020, Zoom anunció que tenía 300 millones de participantes de reuniones diarios, anteriormente 10 millones diarios en diciembre de 2019, algo que implica un aumento de 30 veces el número de participantes en solo 4 meses. La pandemia hizo que la aplicación Zoom sea una de las más descargadas en los meses recientes. Estudiantes, maestros, familiares y grupos de comunidades de todos los tamaños usan videoconferencias para llevar a cabo tareas y actividades. También lo hacen usuarios de alto perfil como Alan Greenspan, expresidente de la reserva federal de Estados

Unidos, y Boris Johnson, primer ministro Británico. Pero ¿qué tan seguros son los servicios de videochat y qué pude hacer para mantener su seguridad?

Exploraremos los problemas relacionados con la seguridad de las videoconferencias y qué puede hacer para que las videollamadas sean más seguras.

¿Qué tan seguras son las videollamadas y las teleconferencias en línea?

El gobierno de Estados Unidos considera que la tendencia del trabajo remoto es un asunto de seguridad nacional debido al riesgo que representan los hackers. La Agencia de Seguridad Nacional (NSA) de Estados Unidos publicó recientemente una evaluación de las 13 herramientas de videochat más populares.

Algunos de los criterios de evaluación fueron:

- ¿Usa el servicio cifrado de extremo a extremo, lo que limita la posibilidad de que otros espíen la llamada?
- ¿Usa autenticación de factores múltiples, una opción que asegura de forma efectiva las cuentas de los usuarios?
- ¿La tecnología en la que se basa es de código abierto que puede inspeccionarse, lo que se considera más seguro que el software de propietario imposible de inspeccionar?
- ¿Comparte la herramienta información con terceros o afiliados?
- ¿Pueden los usuarios borrar de forma segura datos del servicio y de sus repositorios cuando lo necesiten (tanto el cliente como del lado del servidor)?

Puede leer el informe completo aquí pero, en resumen, la NSA concluye que cada uno de los servicios de videochat tiene al menos una falla de seguridad. Por ejemplo:

- Google G Suite y Microsoft Teams no tienen cifrado de extremo a extremo y no usan código abierto
- Cisco WebEx, Zoom, Slack y Skype Empresarial tienen políticas de eliminación de datos que están lejos de ser óptimas
- GoToMeeting no tiene opción de autenticación de factores múltiples

La NSA le otorgó sus puntajes más altos a WhatsApp de Facebook, Signal (cuyo código usa WhatsApp) y la aplicación de chat Wickr. Aunque el informe de la NSA no sea concluyente, es útil como una descripción general de los principales problemas asociados con la seguridad en las videoconferencias, y resalta el hecho de que ninguno de los productos que se encuentran hoy en el mercado reunen todas las características que garanticen la seguridad.

Preocupaciones comunes relacionadas con la seguridad en videoconferencias

Las preocupaciones comunes relacionadas con la seguridad en las videoconferencias incluyen:

¿Hay cifrado de extremo a extremo?

Es decir, videoconferencias cifradas, lo que asegura que la comunicación solo es accesible por los usuarios involucrados y nadie más, ni siquiera por la misma aplicación. Para saber más sobre el cifrado de los datos y cómo funciona, lea nuestro artículo "¿Qué es el cifrado de datos?".

¿Pueden las videollamadas ser interceptadas y grabadas por terceros?

¿Pueden otros espiar la llamada e incluso grabarla? ¿Quiénes pueden unirse a sus llamadas y cómo pueden hacerlo? A medida que las instituciones educativas migran a Zoom para dar clases en línea, es posible que las violaciones a la privacidad lleven a problemas relacionados con la seguridad de los niños. Las reuniones de Zoom pueden accederse con un URL corto basado en números que los hackers pueden fácilmente generar o adivinar.

¿Cómo se usan los datos de su cuenta?

Hasta dónde se cumplen los acuerdos de privacidad como el Reglamento General de Protección de Datos de la Unión Europea o la Ley de Privacidad del Consumidor de California. ¿Qué tan transparentes son las aplicaciones con sus usuarios sobre los datos que recopilan y qué terceros tienen acceso a ellos?

¿En qué lugar de la computadora o del teléfono se almacenan los datos asociados a la aplicación de videollamadas?

Esto es especialmente relevante si tiene que lidiar con información y documentos con contenido confidencial.

Por ejemplo:

- En Skype, las fotos que recibe se guardan en su dispositivo a menos que cambie la configuración. (Ir a Mensajes en Configuración en Android o iOS para cambiar la opción).
- En Zoom, si descarga el registro de conversaciones que acompaña a una videollamada, también se incluirán las conversaciones privadas entre los participantes de la llamada. Esto puede presentar un problema en las llamadas laborales, en las que puede mantener conversaciones que no quiere divulgar a otros.

¿Hay medidas de monitorización dentro de la aplicación?

Por ejemplo, se ha criticado a Zoom por su función para "rastrear que se preste atención", la cual permite a un anfitrión saber si un usuario sale de la pantalla de Zoom por 30 segundos o más. Esta función puede permitir que los empleadores revisen si los empleados están realmente prestando atención a una reunión laboral, o que los maestros sepan si los estudiantes están mirando una presentación de forma remota.

¿Hay potencial de que se descargue malware sin que lo note y que eso resulte en ataques informáticos?

Por ejemplo, ¿podrían los usuarios descargar sin querer aplicaciones que tengan acceso a la cámara y al micrófono? La aplicación o malware podría divulgar información personal a un hacker, quien luego podría publicarla.

En Zoom en particular, se reportaron varias fallas de seguridad en el pasado. Por ejemplo, en 2019, se reveló que Zoom había instalado un servidor web oculto en los dispositivos de los usuarios que permitía que se agregara un usuario a una llamada sin su permiso. Otro error permitía a los hackers tomar el control de la Mac de los usuarios de Zoom, lo que incluía acceder a la cámara web y al micrófono. Como respuesta a esto, Zoom trabajó mucho para responder a las preocupaciones por la seguridad, y publica actualizaciones de forma regular en el blog de la empresa.

Ejemplos de hackeos en videos en línea

Uno de los ejemplos más comunes recientes de acceso sin permiso a llamadas es el de los "Zoom bombings". Es cuando los hackers ingresan a salas de chat para gritar insultos racistas o amenazas violentas. Aunque el término "Zoom bombing" viene de la aplicación Zoom, han sucedido incidentes similares en otras plataformas de videoconferencias, incluidas WebEx y Skype. El 30 de marzo de 2020, el FBI anunció que estaba investigando el número creciente de accesos sin permiso a videollamadas.

En foros como Reddit o Discord, hubo intentos coordinados de interrumpir sesiones de Zoom. En Twitter, hay varias cuentas que compartieron contraseñas de videoconferencias que eran vulnerables a que se unieran personas sin permiso. En algunas instituciones educativas, estudiantes fomentaban la idea de acceder sin permiso como una forma de interrumpir las clases en línea.

Las reuniones de Zoom afectadas (a las que usuarios no invitados ingresan para interrumpir la sesión con insultos obscenos, racistas o antisemitas y que llevan a que el anfitrión finalice la sesión) se comparten posteriormente en plataformas de video, como TikTok o Youtube.

Anteriormente, simples búsquedas en Google de URL que incluyeran "Zoom.us" podían dar como resultado conferencias que no estaban protegidas por contraseñas, lo que facilitaba que los hackers se unieran sin ser invitados.

Aunque el acceso de este tipo a las reuniones puede ser molesto para los participantes, hay una amenaza que puede ser más grave: los intrusos que espían sin revelar su presencia, lo que implica un riesgo muy serio tanto para la seguridad corporativa como para la privacidad individual.

Forbes reportó recientemente que un hacker vendió más de 500 000 credenciales de Zoom robadas, entre ellas URL privados de reuniones y contraseñas de anfitriones de Zoom. Es posible que un gran porcentaje de esas credenciales fueran contraseñas reutilizadas que los hackers obtuvieron de otras fuentes.

Como respuesta, Zoom declaró que:

"*Ya contratamos a múltiples empresas de inteligencia para encontrar estos contenedores de contraseñas y las herramientas usadas para crearlos, además de a una empresa que ha cerrado miles de sitios web que pretendían engañar a los usuarios para que descargaran malware o para que compartieran sus credenciales. Continuamos investigando, estamos asegurando cuentas que descubrimos que estaban en riesgo, les pedimos a los usuarios que cambien su contraseña a una más segura y buscamos implementar soluciones tecnológicas adicionales para impulsar nuestros esfuerzos*".

Cómo proteger los datos de sus llamadas de Zoom

Aunque Skype es muy conocido y hace mucho que existe y FaceTime era la aplicación que la gente estaba acostumbrada a usar para videollamadas con amigos, la aplicación de videoconferencia más popular desde que comenzó la crisis por la Covid-19 es Zoom.

El rápido incremento en la cantidad de usuarios hizo que aumentara también el número de críticas sobre que Zoom no se toma en serio las preocupaciones de seguridad de las videoconferencias de los usuarios. Causó preocupación el hecho de que Zoom no posee, como muchos habían creído, cifrado de extremo a extremo. Zoom compartió guías para proteger las reuniones en una publicación en un blog y un video, pero continúan haciendo a los usuarios responsables de su propia seguridad.

Siete consejos para ayudar a proteger sus llamadas de Zoom

1. **Proteja la sala de la reunión con contraseña y exija que se use autenticación.** De esta forma, solo las personas que usted quiera entrarán en la llamada. Quite a los participantes no invitados y que interrumpieron la reunión.
2. **Deshabilite la opción de compartir pantalla.** De esta forma, solo las personas que usted elija pueden compartir su pantalla.
3. **Tenga cuidado de no hacer clic en los enlaces o abrir los documentos que le envían**. Verifique por otro canal de comunicación que el remitente sea el que le haya enviado el enlace o documento.
4. **Tenga cuidado con lo que muestra en el fondo**. Por ejemplo, traslade de lugar objetos personales o fotografías de sus hijos para que no se vean. Zoom también

ofrece la oportunidad de cambiar el fondo. (Otras aplicaciones para reuniones, como Skype, le dan la opción de hacer borroso lo que tenga detrás de fondo.)

5. **Tenga cuidado con lo que tiene en la pantalla antes de usar la función para compartir pantalla**. Por ejemplo, si tiene abiertas pestañas, ventanas de chat privadas o documentos que muestren información financiera o personal confidencial. Tenga cuidado de no mostrar por accidente un correo electrónico con su dirección o planos cercanos de su tarjeta de identificación, tarjeta de crédito o cualquier otra cosa que no quiera que sea visible para desconocidos.
6. **Revise sus configuraciones.** Hay opciones de seguridad que no se activan por defecto. Zoom tiene diferentes configuraciones para escritorio y para dispositivo móvil. La configuración de escritorio es más detallada y brinda más control que para la versión móvil. Por ejemplo, los anfitriones tienen más herramientas de gestión, y los usuarios pueden gestionar cuentas bloqueadas solo en la versión de escritorio.
7. **Manténgase informado sobre noticias y actualizaciones de la aplicación.** Estar informado le dará una mejor idea de cuáles son las distintas funciones de seguridad disponibles.

Cómo asegurar que los videochats estén protegidos contra hackers

Las formas específicas de cómo asegurar cada videochat varían para cada plataforma, por lo que es importante estudiar los detalles de la plataforma que elija. Sin embargo, muchos de los principios más generales son iguales, sin importar la aplicación de videochat que use.

Estos son consejos para la seguridad de videochat:

-Sea cuidadoso con lo que comparte

Tenga cuidado con lo que comparte en línea, inclusive lo que dice o hace en videollamadas. Debido al riesgo de que otros obtengan una grabación de la llamada o de que entren sin permiso, tenga cuidado con lo que muestra o dice. No mencione información personal propia a menos que sea estrictamente necesario.

Tenga cuidado al compartir el enlace del a invitación

No lo comparta de forma pública en las redes sociales, correos electrónicos grupales, perfiles en línea o cualquier otro lugar donde otros puedan verlo. Invite personas que sean parte del software de videoconferencia y dígales que no compartan los enlaces.

Active alertas para cuando se reenvían invitaciones

Configure alertas para que sepa cuando se reenvían a otros las invitaciones a reuniones por correo electrónico. De esta forma, puede evaluar si los invitados adicionales están aprobados o averiguar más información si no lo están. Si fuera necesario, programe una nueva reunión con nueva información de ingreso.

Elija una contraseña fuerte

La mayoría de las aplicaciones de videollamadas le ofrecen la capacidad de proteger las llamadas con contraseña. Elija una contraseña fuerte y no una fácil de adivinar. Use contraseñas diferentes fuertes para todas las aplicaciones y servicios.

Elija herramientas de videoconferencia con cifrado de extremo a extremo

Esto asegura que nadie más pueda acceder a sus comunicaciones. Las aplicaciones de video más importantes con cifrado de extremo a extremo son, entre otras:

- Google Duo
- FaceTime de Apple
- WebEx de Cisco
- GoToMeeting
- WhatsApp
- Signal

Mantenga el software actualizado

Actualice las aplicaciones con frecuencia. Las brechas en la seguridad y los abusos de privacidad normalmente aparecen en versiones antiguas o no actualizadas de las aplicaciones. Las actualizaciones suelen incluir reparaciones de errores y parches de seguridad para solucionar problemas y corregir aspectos vulnerables. Mantener actualizada su aplicación de videoconferencia es una de las mejores formas para garantizar la protección contra hackers, ya que cuando una empresa lanza un parche para arreglar un error de seguridad, se aplica con la actualización. Esta es una precaución que debe aplicar en todos los entornos, no solo con las aplicaciones de videochat y videoconferencia. Mantener actualizados sus dispositivos y aplicaciones es algo sencillo en todas las grandes plataformas. La mayor parte del tiempo, solo necesita confirmar las actualizaciones. Asegúrese de que los participantes de las reuniones utilicen la versión más actualizada que esté disponible.

Cierre las reuniones una vez que hayan ingresado todos los participantes

Sin embargo, si un participante invitado se desconecta, vuelva a abrir la reunión para que ingresen nuevamente, y ciérrela de nuevo.

Use las funciones de sala de espera en el software de videoconferencia

Estas funciones colocan a los participantes en una sala virtual separada antes de la reunión y permiten que el anfitrión deje ingresar solo a los que deben estar en la sala. El líder o anfitrión en la reunión debe controlar quiénes ingresan. Pida a los asistentes que hablen al comienzo de la llamada para identificar posibles invitados desconocidos.

Conozca las reglas

Es útil saber todo lo posible sobre un software de video antes de usarlo, así que investigue. Tómese el tiempo de revisar todas las configuraciones, y revise su perfil de usuario y todo lo demás a lo que tenga acceso para ver si debe cambiar algo. Si algo le parece confuso y no sabe bien qué hacer, anótelo para buscarlo más tarde y ver si necesita hacer algo al respecto.

Activar funciones adicionales de privacidad

Siempre es bueno que usted mismo revise la configuración de videochat para ver si hay funciones adicionales de privacidad que quiera activar.

Por ejemplo:

- **En Skype,** puede elegir si otros usuarios lo encuentran por número de teléfono o por dirección de correo electrónico.
- **En FaceTime**, puede controlar si otros lo encuentran por número de teléfono o por dirección de correo electrónico. Si no quiere que lo contacten viejos amigos de la escuela o conocidos lejanos, puede serle útil desactivar esta opción.
- **En Google Duo,** está la función Toc toc, que le muestra a sus contactos la transmisión de video antes de que contesten la llamada. Si no se siente cómodo con esto, toque los tres puntos en la parte superior derecha en la interfaz principal de la aplicación Duo, luego en Configuración y en Toc toc para desactivarlo.

Siempre descargue aplicaciones de la App Store oficial

Descubra cómo identificar aplicaciones falsas. Revise las calificaciones y las críticas de los usuarios, y tenga cuidado con las aplicaciones de sitios no autorizados.

Converse solo con gente que conoce

Asegúrese de que la persona en la que está en una videoconferencia sea de confianza antes de compartir algo privado. No acepte solicitudes ni llamadas de personas que no sean amigos. No responda llamadas de personas desconocidas.

Configure la autenticación de factores múltiples

Hace que sea más difícil para los hackers acceder a los dispositivos o cuentas en línea de una persona, ya que no alcanza con solo saber la contraseña y necesitan un PIN de números adicional.

Cuando no esté en una llamada, asegúrese de que la aplicación no se esté ejecutando

Las empresas espían todo lo que pueden, así que no les facilite el trabajo si puede evitarlo. Cubra su cámara web cuando no la use y asegúrese de cerrar la aplicación o el programa por completo una vez que haya terminado de usarlos.

Evite la grabación de las reuniones

Desactive la opción para grabar la reunión para todos excepto para el jefe o anfitrión, o active las alertas para identificar qué asistente comenzó a grabar.

Desactive todo lo que le de permisos excesivos a la aplicación

Por ejemplo, cualquier cosa que permita que se comparta información con terceros y cualquier cosa que declare que mejorará su experiencia al proveer acceso a sus datos para anunciantes o asociados. Desactive las configuraciones que permiten a desconocidos encontrarlo, enviarle solicitudes de amistad, unirse a su grupo o a su sala, o enviarle mensajes. Desactive todas las opciones que permitan que lo graben. Use contraseñas para todo.

No use la función de video en una llamada si no es necesario

Desactivar su cámara web y usar solo el audio impide que se vean objetos en el fondo que podrían revelar información. Usar solo el audio también ahorra ancho de banda de la conexión a internet, lo que mejora la calidad general del audio y de las imágenes de la reunión.

Si hay muchos asistentes, evalúe usar funciones de webcast en lugar de una reunión por videollamada

Un webcast es una conferencia o presentación hecha por internet. Los participantes pueden ver la presentación y enviar preguntas al orador o interactuar con otros delegados. Los webcast le dan el control al anfitrión y a los oradores seleccionados, lo que ayuda a tener más control en reuniones más grandes.

Tenga cuidado al usar redes públicas de Wi-Fi

Las mismas características que convierten los puntos de acceso Wi-Fi gratuitos en deseables para los consumidores los hacen atractivos para los hackers; en concreto, la ausencia de requisitos de autenticación para establecer una conexión de red. Esta característica ofrece una oportunidad a los hackers para obtener acceso sin restricciones a los dispositivos no seguros de la misma red. Tenga cuidado al usarlas.

No le dé su teléfono a alguien que no sea de confianza

Alguien con acceso físico a su teléfono puede fácilmente instalar aplicaciones para hackear y causarle problemas.

Recuerde: los hackers y los criminales cibernéticos aprovechan las oportunidades. Por eso, el uso más extendido de las videoconferencias llevó a que se convirtieran en un objetivo. A medida que evoluciona la tecnología de videollamadas, los actores más importantes tendrán que mantener sus esfuerzos para garantizar la seguridad de los usuarios.

Mientras tanto, la protección antivirus de Kaspersky, que lo protege de virus en sus equipos personales y dispositivos Android, cuida y almacena sus contraseñas y documentos privados, además de cifrar los datos que envía y recibe en línea con una VPN.