Universidad Autónoma de Baja California Sur

10 Recomendaciones para el uso seguro de Zoom

1. **Descargar Zoom desde su página Web oficial.**

Asegúrate de siempre descargar Zoom desde su página Web oficial "www.zoom.us". Descargar la aplicación desde cualquier otra fuente es peligroso, pues puede ser una versión modificada que pone en riesgo tu equipo y tu información.

2. **Si te invitan a una videoconferencia por correo, asegúrate que sea legítima.**

Antes de unirte a una videoconferencia de Zoom, asegurate que la persona que te invitó realmente lo hizo, debido a que existen herramientas que mandan correos electrónicos imitando a personas invitándoles a acceder a sitios que resultan dañinos.

3. **Comparte los enlaces de tus videoconferencias de manera directa, y de ser necesario, aclara que el enlace no se debe compartir.**

Como anfitrión, asegúrate de invitar de manera directa a todos los participantes, evita que sean los usuarios quienes compartan el enlace.

4. **Solicita a todos los usuarios que se identifiquen.**

Como una medida extra de seguridad, es recomendable que todos los participantes se identifiquen con voz y video. De esta manera, se puede evitar tener usuarios infiltrados con propósitos distintos.

5. **Establece una contraseña para tus videoconferencias.**

Habilitar una contraseña para acceder a tus videoconferencias. En conjunto con la recomendación anterior, evitará que usuarios no deseados entren a tus eventos.

6. **Si tu videoconferencia no requiere el intercambio de archivos (Word, PDF, Excel etc.), desactiva la transferencia de archivos.**

Para desactivar esta opción accede a la configuración de tu cuenta. De esta forma, evitarás que los participantes compartan cualquier tipo de archivo, y en caso de alguna infiltración, no será posible propagar archivos maliciosos. Si requieres intercambiar archivos, solo indica las extensiones permitidas para restringir los tipos de archivos válidos.

7. Desactiva la opción de compartir pantalla para los usuarios.

Similar a la recomendación anterior, si tu videoconferencia no requiere que los participantes compartan sus pantallas, desactiva esta opción dentro de la configuración de tu cuenta. Esto evitará que los usuarios puedan compartir cualquier tipo de contenido con los demás participantes.

8. Desactiva la opción de control remoto de la cámara para evitar que otro usuario tome control de tu cámara.

En la gran mayoría de los casos, se recomienda desactivar la opción de control remoto de la cámara. Esta opción permite a los participantes controlar la cámara del anfitrión, lo cual resulta útil en muy pocos casos.

9. Mantén la aplicación de Zoom actualizada a su última versión.

Zoom trabaja constantemente en actualizaciones que fortalecen la seguridad de la aplicación, agregando nuevas opciones de configuración. Por tu tranquilidad, asegúrate de que tu computadora o dispositivo móvil tengan la versión más reciente.

10. Actualiza tu contraseña de manera constante.

Como una buena práctica de seguridad, actualiza tu contraseña con frecuencia. Con esta acción, será mucho más difícil el robo de tu información, y ésto no sólo aplica a Zoom, sino a todas tus cuentas de diferentes plataformas.

COORDINACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN