Centro de Informática, Facultad de Economía, abril de 2020

Recomendaciones de seguridad

Este documento se emite como una recomendación para el uso correcto de zoom, que puede extenderse a las demás herramientas de videoconferencia como meet de Google, webex de Cisco, etc., el documento busca crear las condiciones mínimas de seguridad en los anfitriones de las videollamadas debido a las recientes vulnerabilidades de zoom, por lo cual se emiten las siguientes recomendaciones:

Instalar actualizaciones

- Instalar la última actualización (versión de software) de zoom , esto funciona para la mayoría de las aplicaciones, la de zoom se puede descargar del siguiente sitio web: https://support.zoom.us/hc/es/articles/201362233--D%C3%B3nde-puedo-descargar-la-%C3%BAltima-versi%C3%B3n-

- Mantener actualizado nuestro dispositivo (pc, tableta, teléfono) con la última versión del sistema operativo disponible para cada uno de los sistemas

- Actualizar el antivirus, se disponen de varias versiones gratuitas por un año y se pueden renovar, dentro de las muchas herramientas gratuitas que existen, la UNAM pone a disposición de los usuarios las siguientes: https://www.software.unam.mx/categoria-producto/antivirus/

Contraseñas seguras

- **Generar una contraseña nueva para esta aplicación**, es lo mas recomendable ya que si por alguna razón se llega descifrar una contraseña de zoom y esta contraseña se utiliza en otras aplicaciones (correo, facebook, twitter, etc.) será más fácil el robo de datos personales de esa persona.

- Seguir las recomendaciones de generación de contraseñas, para ello existen diversas guías sencillas las cuales llevan pruebas de laboratorio (desencriptado) y hacen recomendaciones en base a su experiencia, para poder hacer contraseñas más seguras existen los siguientes links:
  https://www.seguridad.unam.mx/guia-para-contrasenas-seguras-0
  https://revista.seguridad.unam.mx/numero-15/password-fu-gu%C3%AD-f%C3%A1cil-para-contrase%C3%B1-realmente-seguras

- Jamás compartir una contraseña con los usuarios y/o asistentes a una clase virtual

No compartir datos

- Siempre **es importante no publicar datos** que puedan comprometer información de los usuarios y de la cuenta, si se planea hacer una conferencia abierta a todo el público es preferible usar zoom para los ponentes y utilizar facebook live para su difusión a la comunidad interesada, para ello deberá tener una cuenta de facebook (se recomienda crear una cuenta de facebook para ese propósito y no usar la cuenta personal), los pasos a seguir se detallan en el siguiente enlace: https://support.zoom.us/hc/es/articles/115000350406-Transmisi%C3%B3n-de-un-seminario-web-en-Facebook-Live

- Zoom crea un ID el cual es diferente a la contraseña para acceder a la cuenta, el ID personal de reunión (Personal Meeting ID o PMI) debe evitarse hacerse público para que no se difunda y se intente acceder a la reunión sin invitación

Seguridad de la cuenta

- Si aun así, el usuario cree, que su perfil de zoom está comprometido, la aplicación pone a su disposición el siguiente enlace para cambiar su contraseña **no es necesario hacerlo si la contraseña cumple con lo anteriormente descrito y la aplicación funciona correctamente.**

  Cambio de contraseña: https://support.zoom.us/hc/es/articles/115005166483-Cambiar-mi-contrase%C3%B1a

Información adicional

Si necesita más información sobre la utilización de zoom existen los tutoriales en video y texto del sitio de zoom:

Texto: https://zoom.us/docs/es-es/covid19.html

Videos: https://support.zoom.us/hc/es/articles/206618765-Tutoriales-de-Zoom-en-video

Seguridad (tips): https://latam.kaspersky.com/blog/zoom-security-ten-tips/18363/

Para solicitar ayuda pueden escribir al siguiente correo: aulavirtual@economia.unam.mx