COMUNICADO

zoom y la seguridad en las clases online de inlingua

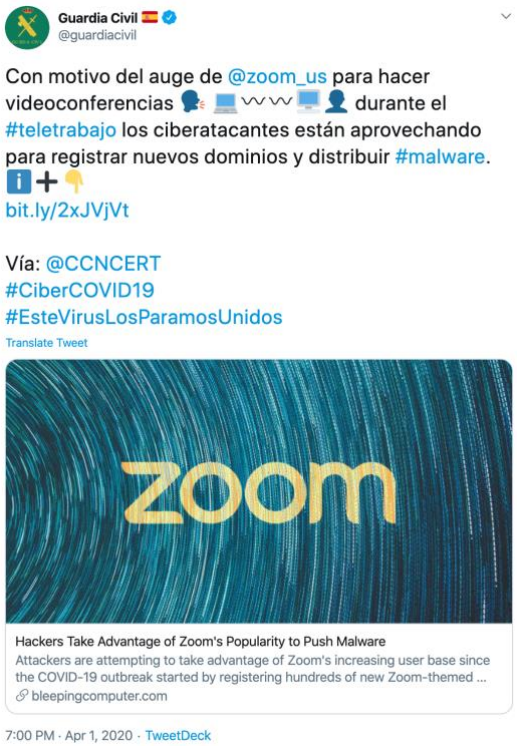
Granada, 10 de abril de 2020

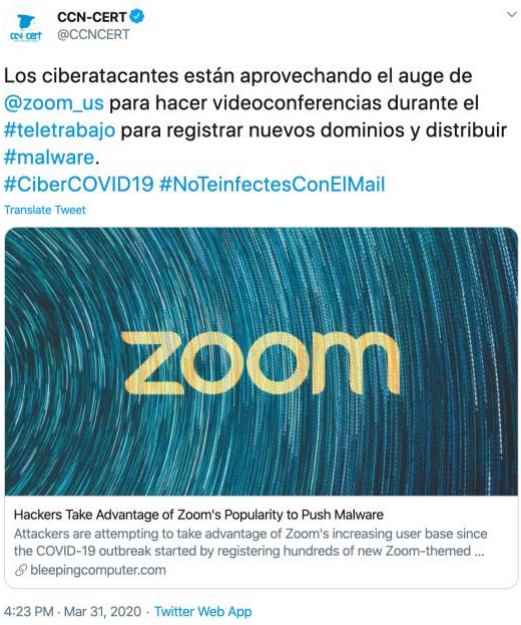
Estimados padres, madres y alumnos:

En los últimos días, diferentes medios se han hecho eco de una serie de supuestos problemas de seguridad del software de reuniones y videollamada *zoom* que inlingua usa para sus clases online. Además, han empezado a circular ciertos rumores y bulos por redes sociales y aplicaciones de mensajería como *WhatsApp*, instando a desinstalar dicho software de todos nuestros dispositivos para evitar males mayores.

Desde inlingua Granada queremos, en primer lugar, hacer una llamada a la tranquilidad. Para nosotros, la seguridad de nuestros alumnos y clientes es primordial, y más aún tratándose de un asunto que concierne a menores de edad. Por ello, nos gustaría tratar ciertos temas que arrojen claridad al asunto y despejen todas las dudas que puedan surgir.

En sus cuentas de la red social *Twitter*, tanto la Guardia Civil (@guardiacivil) como el Centro Criptológico Nacional (@CCNCERT), entre otros, alertaban a principios de mes de cómo los ciberatacantes podrían aprovechar ciertas vulnerabilidades en *zoom*:





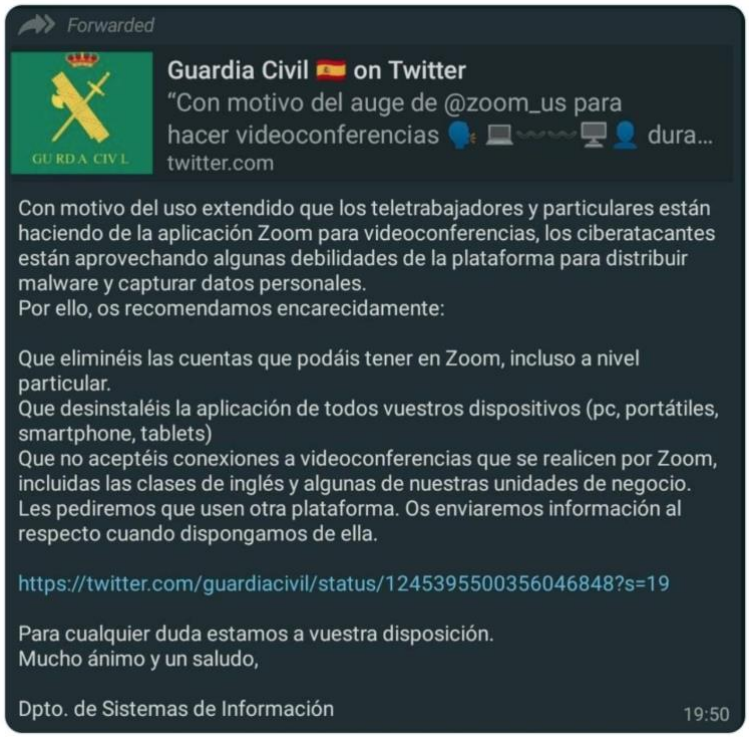
inlingua Granada | Centro
Calle Ángel Ganivet, 15 – 1ª
18009 Granada (Spain)
T +34 958 216 457

inlingua Granada | Kids
Calle Nueva de San Antón, 8
18005 Granada (Spain)
T +34 958 252 947

inlingua Granada | Albayda
Calle La Palmita, 28
18014 Granada (Spain)
T +34 958 092 534

info@inlinguagranada.es
www.inlinguagranada.es

Como podéis ver, las autoridades no instan en ningún momento a que el usuario desinstale la aplicación de sus dispositivos, tal y como hace entender esta cadena que ha sido compartida en redes sociales y mensajería:



Otros medios se han apresurado a desmentir este y otros bulos que han ido circulando en la última semana, como el usuario que aseguraba que su cuenta bancaria había sido atacada por haber usado *zoom*. Sí que es totalmente cierto que en épocas de crisis, los ciberdelincuentes están más activos que nunca, y es en este mundo extremadamente conectado donde tenemos que tomar todas las precauciones posibles.

Volvamos a la noticia que enlazaban tanto Guardia Civil como el CCN, titulada "Hackers take advantage of zoom's popularity to push malware" ("Los hackers se aprovechan de la popularidad de zoom para colar software malicioso"). El principal riesgo se presenta accediendo a páginas web que se hacen pasar por *zoom* y que hacen descargar herramientas que dicen ser *zoom* pero no lo son. Recordad que nuestras web seguras para la descarga de *zoom* son únicamente https://online.inlinguagranada.es y https://inlinguagranada.zoom.us , y que debéis siempre tener actualizada la aplicación a la última versión. En el caso de que la tengáis instalada en dispositivos móviles como tablets o teléfonos, recordad descargar siempre las aplicaciones oficiales. Podéis encontrar más información en nuestra guía de conexión para padres y alumnos: https://docdro.id/bCakB70 Estos intentos de engaño por parte de hackers también están sucediendo con otras herramientas de la competencia como *Microsoft Teams* o *Google Classroom*, y es que los ciberatacantes intentarán aprovechar el desconocimiento de los usuarios para perpetrar sus ataques. inlingua Granada **nunca** os enviará correos electrónicos para que descarguéis *zoom* por otros canales o accedáis a páginas que piden datos personales (más allá del nombre del alumno) como usuarios, contraseñas, correos electrónicos, etc.

Una de las principales vulnerabilidades del software *zoom* se basa en lo que los medios expertos han venido a llamar '*zoombombing*', que consiste en usuarios anónimos que se unen a las reuniones sin haber sido invitados. El medio online especializado en tecnología *Xataka* publicaba este artículo al respecto: https://www.xataka.com/privacidad/zoombombing-nuevo-pasatiempo-internet-asi-incursiones-extranos-videollamadas-zoom-asi-difunden ('*Zoombombing' es el nuevo pasatiempo de Internet: así son las incursiones de extraños en videollamadas de Zoom y así lo difunden*). En dicho artículo se comenta lo siguiente:

- *[…] usuarios desconocidos se pueden sumar a una videollamada si disponen de la URL de esta y si el anfitrión no ha tomado las medidas de protección necesarias.* Por suerte, en inlingua Granada sí hemos tomado las medidas de protección necesarias, que detallamos más abajo.

- *Si una videollamada se establece como pública, es evidente que cualquier persona puede entrar disponiendo del enlace.* Nuestras videollamadas no son públicas y solo nuestros padres, madres y alumnos cuentan con el ID de reunión para acceder a ellas.

- *La plataforma ha publicado una detallada guía de cómo evitar esto. Hay muchos consejos que se ofrecen […] Por ejemplo, es posible permitir la entrada de usuarios sólo con contraseña, crear una sala de espera desde la que aprobar o no la entrada de nuevos usuarios, desactivar los vídeos y el audio de los huéspedes o desactivar los chats privados.* Entre estas medidas de seguridad, se adoptó desde un principio la de usar una sala de espera virtual desde la que aprobar o no la entrada de nuevos usuarios. Nadie puede unirse a nuestras clases sin que el profesor dé permiso de manera manual. Nuestros profesores únicamente dan acceso a la reunión a alumnos que puedan identificar (de ahí la importancia de que el alumno escriba su nombre en la pantalla de bienvenida). En el supuesto caso de que alguien intentara suplantar la identidad de un alumno, el profesor se daría cuenta rápidamente y podría expulsar al intruso en cuestión de segundos sin que la seguridad de la clase se vea comprometida. En cualquier caso, vamos a dar un paso adelante y e implementaremos contraseñas de acceso a las clases a partir del lunes 20 de abril (más información abajo). Estimamos que no es necesario desactivar el vídeo y el audio de los participantes, aunque los chats privados (para que unos alumnos se comuniquen con otros sin que el profesor lo vea) ya están desactivados por defecto, sobre todo para evitar potenciales casos de acoso escolar.

Como menciona el artículo, *"La mayoría de los ataques en Zoom sin embargo no son por carencias de seguridad en el servicio, sino más bien por la falta de opciones de privacidad o la configuración incorrecta de estas."* La compañía se está poniendo las pilas y anunció recientemente una serie de medidas encaminadas a mejorar su seguridad, como se explica en este otro artículo: https://www.xataka.com/aplicaciones/zoom-anade-nuevas-herramientas-seguridad-para-intentar-frenar-numerosas-dudas-respecto-a-su-privacidad (*Zoom añade nuevas herramientas de seguridad para intentar frenar las numerosas dudas respecto a su privacidad*). Algunos otros problemas que se mencionan en otros artículos hablan de filtraciones de usuarios y contraseñas de *zoom*, pero vosotros no tenéis que estar preocupados por esto, puesto que accedéis a la plataforma como usuarios externos, sin introducir ningún usuario o contraseña, sino simplemente el *ID de reunión* que os proporcionamos desde inlingua. Por último, se habla de que las comunicaciones de *zoom* no están cifradas de punto a punto, sino que pasan primero por los servidores centrales de *zoom*. Solo en el caso de un improbable ataque a escala masiva a los servidores de la compañía (lo que en los círculos se conoce como "ciberterrorismo"), podría verse comprometida la privacidad de los usuarios, y en

cualquier caso, esto afectaría a los clientes como inlingua pero no directamente a usuarios externos como nuestros alumnos. En el peor de los casos, un ciberatacante podría asistir a una de nuestras clases sin ser detectado por el profesor, pero es obvio que para cuando eso pasara, los técnicos de seguridad de *zoom* (hablamos de una compañía con más de 2000 trabajadores, en su mayoría informáticos) ya habrían sido alertados y habrían suspendido el servicio de manera temporal, por no mencionar que un ciberatacante tendrá objetivos más interesantes que una mera clase de inglés con inlingua…

Como ya sabréis, la aplicación *zoom* es usada por más de 13 millones de usuarios activos en todo el mundo, y miles de empresas y escuelas en los cinco continentes confían en ella para sus soluciones de comunicación (en inlingua Granada, por ejemplo, la usamos desde hace ya más de un año). Algunas compañías como *Google* (que, por cierto, tiene un software propio al que hace competencia *zoom*) y ciertos organismos gubernamentales como el Senado de los EE.UU. han desaconsejado el uso de esta herramienta hasta que se solventen las vulnerabilidades de seguridad. Es entendible puesto que se asume que la información que se trata en esos entornos debe contar con una seguridad de altísimo grado y es más vulnerable a que ciberatacantes intenten acceder a ella. Volvemos a decir que no es el caso de unas simples clases de inglés con inlingua…

En cualquier caso, volvemos a llamar a la tranquilidad y os hacemos una serie de recomendaciones generales para que mantengáis e incluso reforcéis vuestra seguridad en el ámbito digital:

- inlingua Granada **nunca** os enviará correos electrónicos con enlaces que os pidan información personal como nombres de usuario, contraseñas, números de cuenta, etc. La única información personal que requiere *zoom* para entrar en la clase es el nombre y el apellido del alumno, nada más. Si recibís alguna comunicación que parece proceder de inlingua pero no estáis muy seguros, no dudéis en contactar con nosotros a través de nuestros canales habituales.

- La manera más segura de acceder a nuestras clases es abriendo la aplicación *zoom* e introduciendo el *ID de reunión*, compuesto de 10 dígitos. A partir de este mismo lunes, y para dotar de más seguridad al sistema, **eliminaremos** la modalidad de acceso mediante acceso directo web (es decir, la manera de acceder haciendo clic en enlaces del estilo de https://inlinguagranada.zoom.us/j/8732595297 o https://inlinguagranada.zoom.us/my/teacher.zoe).

- A partir del **lunes 20 de abril**, todas nuestras clases a través de *zoom* estarán protegidas mediante una contraseña de acceso que el sistema os pedirá al intentar entrar en la clase. En los próximos días recibiréis un correo electrónico con dicha contraseña. En el improbable caso de que un ciberatacante pudiera hacerse con el *ID de reunión* de alguna de nuestras clases, e incluso suponiendo que el profesor le diera acceso manual por error, no podía acceder del todo a la clase puesto que no dispondría de dicha contraseña. Hablamos ya de un acceso a nuestras clases no con uno ni con dos, sino con **tres filtros de seguridad**.

- Nunca hagáis clic en enlaces cuya procedencia desconocéis (por ejemplo, si vienen de un remitente desconocido o de una web no oficial) ni abráis archivos adjuntos en correos electrónicos sospechosos. inlingua Granada **nunca** os enviará archivos ejecutables de ningún tipo, puesto que prácticamente los únicos adjuntos que contienen nuestros correos electrónicos son documentos en formato PDF.

- Aseguraos de que contáis siempre con las últimas actualizaciones, no solo de vuestras aplicaciones más usadas, sino también las de seguridad de Windows, las últimas versiones de vuestro software antivirus, etc. La *Oficina de Seguridad del Internauta* recomienda siempre contar con la última versión de *zoom* que, como sabéis, podéis descargar a través de https://online.inlinguagranada.es o https://inlinguagranada.zoom.us, haciendo clic en el enlace "Descargar aplicación" de la barra inferior. Dejamos aquí un enlace al comunicado de la *OSI*: https://www.osi.es/es/actualidad/avisos/2020/04/actualiza-la-ultima-version-de-zoom

Consideramos útil que os informéis con regularidad a través de la *OSI* puesto que en estos tiempos, la ciberseguridad es algo que nos concierne a todos y es muy importante estar protegidos ante posibles amenazas: https://www.osi.es/es

Esperamos que esta comunicación, sin entrar demasiado en tecnicismos innecesarios, haya arrojado un poco de luz sobre el asunto y haya conseguido tranquilizaros a todos. Volvemos a hacer énfasis en que la seguridad de nuestros alumnos y clientes es lo más importante para nosotros. Si queréis aclarar alguno de los puntos tratados, no dudéis en contactar con nosotros por teléfono (incluyendo *WhatsApp*) y redes sociales.

Os deseamos que disfrutéis de este fin de Semana Santa junto a vuestros seres queridos y os esperamos a todos en nuestras clases online a partir del lunes 13 de abril.

Un cordial saludo,

Pedro Montiel
Jefe de estudios

inlingua Granada
Ángel Ganivet, 15 - 1 · 18009 Granada
+34 958 216 457
www.inlinguagranada.es