UNIÓN COLEGIADA DEL NOTARIADO COLOMBIANO "U.C.N.C."

MEMORANDO No. 2765 Bogotá D.C., 8 de septiembre de 2020

Tema : Artículos periodísticos de interés sobre protección de datos.

De : Prensa "U.C.N.C."

Para : Notarios del país.

Respetados Señores Notarios:

Para su conocimiento e información, me permito enviar los siguientes artículos periodísticos de interés, publicados en el Diario El Tiempo sobre la protección de datos en el mundo virtual.

La seguridad en las videollamadas: ¿qué se puede hacer?
https://www.eltiempo.com/tecnosfera/novedades-tecnologia/videollamadas-como-tener-una-comunicacion-segura-y-que-es-el-zoombombing-536322

Política de seguridad informática.
https://www.eltiempo.com/opinion/columnistas/guillermo-santos-calderon/politica-de-seguridad-informatica-columna-de-guillermo-santos-calderon-536326

Google Tendría que pagar $ 1.755 millones si no cumple las normas de protección de datos en Colombia.

Cordialmente,

VIVIANA ORTIZ CUENCA
Jefe de Prensa

Adjunto: Lo anunciad
Elaboró: OCF

Tecnología

UN DETECTOR DE 'DEEPKAFES'

Microsoft lanzó un *software* capaz de detectar contenidos que usan la tecnología de ultrafalsos con el fin de contrarrestar las noticias falsas antes de las elecciones en EE. UU.

La seguridad en las videollamadas: ¿qué se puede hacer?

El fenómeno *Zoombombing* se ha registrado en varios países y consiste en hacer bromas y sabotear de diferentes maneras las videollamadas.

Cuando la congresista María José Pizarro estaba interviniendo la semana pasada en uno de los debates virtuales de la Comisión Sexta de la Cámara de Representantes, fue interrumpida en varias ocasiones: primero fue insultada, y después su participación fue completamente bloqueada con videos pornográficos.

Lo mismo le pasó a Luis* cuando hace unas semanas convocó a varios de sus amigos en redes sociales para realizar unas tertulias sobre temas de género por videollamada y compartió el enlace; solo 20 minutos después de haber comenzado la conversación, el diálogo fue saboteado con música fuerte y risas, finalmente comenzaron a aparecer imágenes de contenido sexual en la pantalla de todos los asistentes.

Este panorama se ha repetido incontables veces durante los últimos meses, cuando en el aislamiento por la pandemia se aumentó considerablemente el uso de herramientas digitales para hacer videollamadas.

Este fenómeno se esparció tan rápidamente que incluso el FBI, en abril pasado, se pronunció sobre el hecho y rechazó ese tipo de comportamientos que tienen como primera finalidad molestar a las personas conectadas.

"Lo que buscan principalmente es llamar la atención", asegura Cecilia Pastorino, especialista en seguridad informática de Eset Latinoamérica.

Un nuevo fenómeno

Este tipo de casos ha crecido en una forma tan elevada y en tantos países que ya es conocido como *Zoombombing* por el nombre de la plataforma de videollamadas Zoom, que se ha convertido en una de las más usadas durante estos meses.

"El *Zoombombing* es cuando alguien ingresa a una videollamada y lo que buscan principalmente es interrumpir la comunicación. Muestran videos porno, insultos o hacen garabatos, todo con el fin de molestar e interrumpir, y en casos como el que pasó en el Congreso puede también estar relacionado con temas de activismo", detalla Pastorino.

La experta destaca que este tipo de modalidad es un "engaño de ingeniería social", así también lo confirma Axel Díaz, director del laboratorio forense de Adalid Corp., empresa especializada en seguridad de la información.

Díaz explica que lo que ocurrió en la Comisión Sexta de la Cámara de Representantes no se debió puntualmente a un 'hackeo', sino que fue un "error humano".

"Seguramente, el atacante hizo un correo muy parecido al que uno de los congresistas pudiera tener, el administrador de la comunicación lo confunde y le autoriza el ingreso. Después de esto comienzan a ejecutar sus acciones de sabotaje", indica.

Las personas que realizan este tipo de bromas buscan tener nombres muy similares o que luzcan confiables para que se les permita entrar a la llamada.

¿Qué hacer?

Lo principal en este tipo de casos es entender que en estas tecnologías existen muchos riesgos y se deben asumir con el cuidado que lo amerite.

"Hay que ser conscientes de las implicaciones que tiene el mundo virtual y tomar las mismas precauciones que tendríamos si fuera en un espacio presencial", explica Axel Díaz.

Así mismo, Pastorino señala que es muy importante antes de realizar una videollamada conocer la herramienta en la que se va a realizar, con el fin de identificar las configuraciones con las que se cuenta.

"Familiarícese con las opciones que brindan para configurarlas. Por ejemplo, si la herramienta deja poner una contraseña, hágalo", precisa Pastorino.

Por otro lado, añade que varias de estas plataformas permiten que haya "una sala de espera para que a los asistentes se les habilite uno por uno para participar" y se les otorguen ciertas características como usar el micrófono, activar la cámara o compartir pantalla.

En el caso de que sea una videollamada con un grupo más cerrado, procure que a cada invitado le llegue un enlace personalizado que es de único uso; así, una vez la persona ingrese, el atacante que quiera acceder por este vínculo no lo podrá hacer.

Otro de los errores más comunes es el de publicar en redes sociales los enlaces de las videollamadas, esto permite que los atacantes accedan sin restricciones.

"Hay que tener en cuenta que en seguridad nada es 100 por ciento confiable y siempre pueden aparecer fallas de seguridad. La idea es mitigar ese riesgo lo más que se pueda, por eso es importante el análisis y ver para qué voy a utilizar la plataforma", precisa Pastorino.

Estas herramientas también han sido utilizadas por los ciberdelincuentes para obtener información. En este caso ingresan y no interactúan, para pasar desapercibidos.

"Comparten enlaces maliciosos dentro del chat, aprovechando que las personas sienten que es un espacio seguro, con participantes autorizados", indica Pastorino.

Otro de los casos reportados es el de subir aplicaciones muy similares a las más populares para realizar videollamadas, las cuales son subidas en tiendas oficiales, y una vez se realiza la descarga la persona queda con un código malicioso.

"Es importante revisar la cantidad de descargas que tiene la *app* y cuáles son los comentarios que tiene, para descartar que no sea falsa", puntualiza la experta.

En el corazón de todos los inviernos vive una primavera palpitante, y detrás de cada noche viene una aurora sonriente.
Khalil Gibran

Opinión

Política de seguridad informática

El mundo de la tecnología

Guillermo Santos Calderón

Con el aumento de los delitos digitales a causa de la pandemia, es muy importante tomar las medidas de seguridad más adecuadas para protegerse y tener una respuesta a los clientes en caso de que los penetren y les roben datos confidenciales de ellos como claves, teléfonos, cédulas y nombres.

Algo fundamental es que las empresas deben tener políticas de seguridad informática que los empleados tienen que seguir, y que se les haga seguimiento de su cumplimiento y no se queden como un manual en un cajón.

Estas políticas deben tener en cuenta varios factores. Las claves para entrar a la red de la empresa deben exigirse con mínimo de 12 caracteres con mayúsculas, minúsculas, números y caracteres especiales. Algo vital es cada cuánto los empleados deben cambiarla. Esto depende de qué tan importante es la información que maneja el empleado. Una secretaria la podría cambiar cada 6 meses, mientras que el tesorero, contador o gerente, que procesan información muy importante, la deberían cambiar mensualmente.

Otro es la prohibición de usar memorias USB o DVD, ya que son un medio en el cual un empleado puede sacar información de la empresa. Otro riesgo de permitir su uso es que pueden estar contaminados con *software* malicioso que, una vez se conecte esta memoria, invade al computador y, por ende, la red empresarial. Esto se podría evitar vacunando la memoria con un antivirus empresarial si es necesario usarla.

Otra forma de sacar información sin que nadie se dé cuenta es mediante el uso de correos de Internet, como Yahoo, Outlook y Gmail. Esto es muy sencillo, ya que anexando un archivo a un correo, el empleado puede mandarlo a otro correo que ha creado para este efecto. Prohibir su uso en la oficina puede ser una medida que evite esto.

Los contratos de trabajo deben tener una cláusula para que el empleado sea responsable del uso de su cuenta para acceder a la red empresarial. Si se va a tomar café y se deja el equipo conectado a la red y firmado, pues un ingeniero social, que es una forma de 'hackear', puede acceder a ella y penetrar la red para establecer un *software* malicioso o robar información confidencial.

Toda política de seguridad debe estar apoyada por la alta gerencia; de lo contrario, va a fracasar. Se debería empezar a analizar qué política le conviene a la empresa, diseñarla e implementarla lo antes posible si aún no se tiene.

guillermo.santos@enter.co

Sábado

$2.300

Bogotá Colombia • 5 de septiembre de 2020

Año 109- № 38609
Afiliado a SIP y AMI
ISSN0121-9987

EL TIEMPO

Google tendría que pagar $ 1.755 millones si no cumple normas de protección de datos en Colombia

La SIC señala que la empresa incumple más de la mitad de las normas del país. Pide que implementen medidas para proteger la información de millones de usuarios.

Ayer, la Superintendencia de Industria y Comercio (SIC) emitió una orden de cumplimiento contra la compañía Google en Colombia para que implemente medidas de protección de datos, según los estándares que ya están estipulados en el país desde hace algunos años.

La SIC, en su resolución 53593, señala que la compañía de tecnología en su Política de Tratamiento de la Información (PTI) incumple con el 52,6 por ciento de los requisitos que se exigen en Colombia.

Y a través de un comunicado, la Superindustria señaló que Google hace uso de *cookies* que recolectan datos personales de sus usuarios en el territorio nacional.

Por esta razón, la Superintendencia le ordena a la compañía que "implemente un mecanismo o procedimiento apropiado, efectivo y demostrable para que al momento de solicitar la autorización a cada persona, le informe de manera clara, sencilla y expresa del tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo".

Así mismo, Google debe notificar el "carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes. Los derechos que le asisten como titular de su información y la identificación, dirección física o electrónica y teléfono del responsable del tratamiento".

Por otro lado, la Superindustria determinó que la empresa de tecnología debe crear una política de tratamiento de información que cumpla con los lineamientos del artículo 13 del decreto 1377 de 2013.

En ese sentido, Google debe también implementar un "mecanismo o procedimiento apropiado, efectivo y demostrable para dar cumplimiento a los requisitos especiales" de esta normatividad, en materia de "recolección y tratamiento de los datos personales de niños, niñas y adolescentes".

Y debe presentar la "autorización previa, expresa e informada emitida por los representantes legales de los niños, niñas y adolescentes, cuyos datos hayan sido recolectados o tratados con posterioridad a la entrada en vigencia de la ley estatutaria 1581 de 2012".

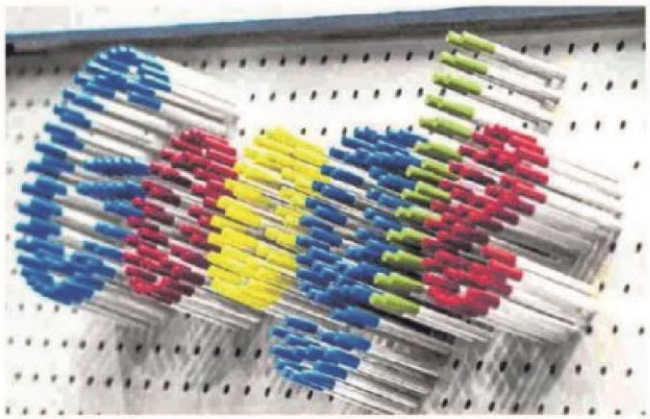
La SIC también señaló que la compañía debe registrar sus bases de datos en el Registro Nacional de Bases de Datos, que es administrado por la Superintendencia.

Por último, la Superindustria precisó que esta decisión se toma porque Google en Colombia tiene recolectados y hace uso de "los datos de 38'962.184 de colombianos mayores de edad y 1'847.592 de menores de edad".

El organismo aseguró que si la compañía de tecnología no cumple con estas órdenes, puede ser sancionado hasta con 2.000 salarios mínimos, es decir, 1.755 millones de pesos.

Por su parte, en una respuesta de Google a EL TIEMPO, la compañía aseguró que respeta la decisión tomada por la Superindustria.

"Google es respetuoso del ordenamiento jurídico colombiano aplicable. Tan pronto seamos notificados por la Superintendencia de Industria y Comercio (SIC), procederemos a evaluar los alcances de la resolución", indicó Tatiana Márquez, gerente de Comunicaciones de Google Colombia.



Google tiene recolectados los datos de 38'962.184 colombianos mayores de edad y de 1'847.592 menores de edad, según información de la Superintendencia de Industria y Comercio. FOTO: EFE