



UNIÓN COLEGIADA DEL NOTARIADO COLOMBIANO “U.C.N.C.”

MEMORANDO No. 2948

Bogotá D.C., 8 de febrero de 2021

Tema : Artículos periodísticos de interés sobre suplantación de identidad y seguridad de la información.

De : Prensa “U.C.N.C.”.

Para : Notarios del País.

Respetados Señores Notarios:

Para su conocimiento e información, me permito enviar copia de los artículos periodísticos “¿Cómo garantizar la seguridad al crear una contraseña?” y “Los posibles riesgos detrás de las versiones alternas de WhatsApp”, publicados en el Diario El Tiempo.

A través de los siguientes enlaces, puede acceder a las noticias:

¿Cómo garantizar la seguridad al crear una contraseña?

<https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/como-crear-una-contrasena-565258>

Los posibles riesgos detrás de las versiones alternas de WhatsApp.

<https://www.eltiempo.com/tecnosfera/apps/whatsapp-problemas-de-seguridad-de-las-versiones-alternas-565316>

Cordialmente,

VIVIANA ORTIZ CUENCA
Jefe de Prensa

Adjunto: Lo anunciado.
Elaboró: VOC

Tecnología



TAG HEUER Y PORSCHE SE ALIAN

TAG Heuer y la marca de carros deportivos Porsche anunciaron su alianza más estrecha, en la que trabajarán en proyectos en conjunto tanto en productos como en lo deportivo.

Los posibles riesgos detrás de las versiones alternas de WhatsApp

La semana pasada anunciaron que cerrarían las cuentas que usaran las versiones piratas de la aplicación de mensajería. Por esto no es bueno utilizarlas.

REDACCIÓN TECNÓFERA - EL TIEMPO | @tecnoferaET

WhatsApp es una de las aplicaciones más utilizadas del mundo y cuenta con más de 2.000 millones de usuarios en el planeta, que pueden comunicarse desde cualquier lugar en tiempo real. Y desde hace algún tiempo también existen diferentes aplicaciones alternas a la original que se escuchan de WhatsApp Plus y otras aplicaciones que ofrecen diferentes servicios extras, pero que son mal vistas por la plataforma original. ¿Es seguro tenerlas?

Una de las aplicaciones es WhatsApp Plus, la cual permite chatear, enviar fotos, emojis, videos y documentos al igual que la original, pero también cambiar el color de los chats y la plataforma. Además, cuenta con otras funciones que ayudan a tener una mejor experiencia de usuario.

En la última versión de esta app alterna se agregó 'habilitar chats' y 'grupos separados', ocultar el estado de visualización, cambiar colo-

res y personalizar su aplicación. También puede 'desaparecer' para algunos contactos y cambiar su última conexión a una hora diferente y personalizar su confirmación de lectura (checks azules) según el contacto.

A diferencia de la versión original, esta ofrece aún mayor personalización, tanto visual como en herramientas para ocultar diferente información a sus contactos, lo que no se puede realizar en el WhatsApp que se encuentra en las tiendas de aplicaciones.

No obstante sus nuevas funciones, la verdad es que al no ser oficial puede tener hacia el futuro muchos problemas que pueden derivar en un bloqueo de su número.

Además, tenga en cuenta que WhatsApp Plus no tiene chats cifrados, lo cual significa que cualquier persona podría acceder a sus conversaciones o las de terceros sin cuenta con protección de los datos podrían estar comprometidos para

ataques, estafas o robos en línea.

Así mismo, la aplicación accede a su lista de contactos, por lo que se podrían generar filtraciones de números o algunos problemas podrían derivarse de ciberataques a esta aplicación que podrían comprometer su seguridad.

Por esta razón, la semana pasada, los desarrolladores de WhatsApp enfatizaron en que empezarán a suspender cuentas de usuarios que estén utilizando aplicaciones como WhatsApp Plus o GB WhatsApp de forma temporal. Esta decisión, aseguran desde la compañía, está centrada en la seguridad de los usuarios y no en limitar la libertad de uso.

Cuando se entra a WhatsApp utilizando una aplicación de terceros, lo que sucede es que ya no depende de las políticas de privacidad de esa aplicación, que de una u otra manera está regulada y cuenta con protección de los datos personales de quienes la usan.

2
mil millones
de usuarios
CON ESTA CIFRA
WHATSAPP SE
CONVIERTE EN
UNA DE LAS
APLICACIONES
MÁS POPULARES.

Al utilizar estas aplicaciones de terceros, el usuario acepta los permisos de acceso a diferentes permisos en su teléfono celular, entre los cuales se encuentran las llamadas, contactos, fotos, cámara, así como ejecutar aplicaciones o cerrar otras y hasta obtener datos de uso de la red wifi. En parte, los mismos que pide WhatsApp, pero sin que sus desarrolladores estén bajo vigilancia de control para saber qué es lo que hacen con todos estos datos.

Es bien sabido que descargar aplicaciones fuera de las diferentes tiendas de aplicaciones puede representar riesgos para usted y su dispositivo.

Tanto Google Play Store como la Apple App Store tienen métodos para identificar apps maliciosas. Sin embargo, con descargas de apps no hay forma de saber qué es realmente lo que está descargando y si esto que ahora tiene instalado en su teléfono es completamente seguro.

En ese sentido, voceros de la plataforma afirmaron también que aquellas personas que fueron bloqueadas temporalmente serán bloqueadas de forma permanente en caso de no migrar a la versión oficial una vez se les vuelva a activar su cuenta.

"Las aplicaciones no admitidas, como WhatsApp Plus, GB WhatsApp, o las que afirman ser capaces de mover tus chats de WhatsApp de un teléfono a otro, son versiones alteradas de WhatsApp. Estas aplicaciones no oficiales son desarrolladas por terceros y violan nuestras condiciones del servicio. WhatsApp no avala el uso de estas aplicaciones de terceros debido a que no es posible validar sus prácticas de seguridad", dijeron desde la app.

Expertos en ciberseguridad explican que no necesariamente todas las aplicaciones que están afuera de las tiendas son peligrosas, pero que siempre existe un riesgo latente de que alguna pueda venir infectada y usted sea un objetivo vulnerable.

Recuerde que si usted ve el mensaje 'Tu número de teléfono está suspendido en WhatsApp. Contacta con Soporte para recibir ayuda', es posiblemente porque su actividad violó las condiciones de servicio. Pero si usted cree que no ha sido así, los desarrolladores señalan que deberá ir al apartado de contacto para que puedan revisar su caso y darle solución.

La mejor recomendación es utilizar la versión original de la aplicación y si usted quiere algunas características que esta no tiene, contemplar algunas alternativas de aplicaciones de mensajería instantánea que también son muy completas y seguras.



Descargar aplicaciones fuera de las diferentes tiendas puede representar riesgos para usted y su dispositivo. FOTO: HAZARDUSO / LEON, EL TIEMPO.



La doble autenticación es una opción que puede aumentar la seguridad para entrar a sus cuentas. Algunos prefieren no activarla para ahorrar tiempo, pero los expertos recomiendan hacerlo. Foto: iStock

¿Cómo garantizar la seguridad al crear una contraseña?

Tener claves sencillas les facilita a los ciberatacantes el acceso a cuentas de redes sociales, correos electrónicos y servicios financieros, con los que se cometen suplantación de identidad y fraudes.

REDACCIÓN TECNÓSFERA-EL TIEMPO @tecnosfera

Una opción corta que sea fácil de recordar, que tenga la fecha de nacimiento o el nombre de la mascota de la familia son algunas de las alternativas que normalmente prefieren los usuarios de Internet cuando crean una contraseña. Error craso.

Aunque es un paso muy común a la hora de navegar y al que no se le presta mucha atención, esa frase de un par de caracteres es la puerta de entrada a cientos de datos personales que podemos almacenar en nuestras cuentas de correo electrónico, redes sociales, servicios pagos de streaming, transacciones financieras digitales, entre otras.

Por eso, tomar medidas de seguridad se convierte en una necesidad, más aún cuando se observa el panorama de la región en este campo. Según el estudio Iceberg Digital, realizado en Latinoamérica por la empresa de ciberseguridad Kaspersky, el 22 por ciento de los latinoamericanos han sido víctimas de un intento de 'hackeo' en alguna de sus cuentas. En términos generales, Colombia ocupa, junto con México, el segundo lugar con mayor número de afectados, con el 23 por ciento, superado únicamente por Perú, que reporta el 28 por ciento de los ataques de esta naturaleza.

Errores más comunes

Hay unos patrones básicos en las principales equivocaciones que se cometen a la hora de generar una clave. Lo peor que se puede hacer cuando se crea una contraseña es buscar la facilidad, esto le ayuda a que un posible atacante la detecte de forma sencilla.

"Muchas veces, por comodidad se crean claves simples para que no se olviden o que tengan información que pueda estar relacionada con datos personales que pueden ser identificables, debido a las publicaciones que compartimos en las redes sociales, como la edad de la pareja o los hijos, una fecha de aniversario o cumpleaños. Para los atacantes va a ser mucho más sencillo poder crear opciones que contengan esos datos de manera combinada a la hora de atacar", precisa Roberto Martínez, analista de ciberseguridad en Kaspersky.

Así mismo, es frecuente que se haga una reutilización de contraseñas, es decir, usar un patrón de palabras muy similares entre una cuenta y otra en donde solo se cambie un dígito. Esto se suma a uno de los errores más tradicionales, el de usar una misma contraseña en todos los accesos que se tienen.

"Esto tiene uno de los mayores riesgos, ya que si un ciberatacante obtiene la contraseña, podrá acceder plenamente y sin problemas a todas las páginas. Lo más aconsejable es tener una contraseña diferente en cada uno de los servicios para minimizar el riesgo", detalla Alexander Ramírez, gerente de Frontech Esat Colombia, especializada en seguridad informática.

Entre las malas prácticas también figura el hecho de guardar las contraseñas en el navegador, así sea desde un computador de confianza, o de tener un archivo en el bloc de notas, un documento en Word o Excel o en línea en el cual se recopilen los accesos a las cuentas utilizadas. Según la medición Iceberg Digital, el 56 por ciento de los internautas en

¿Por qué quieren más datos si no soy importante?

No importa si uno es alguien común y corriente, que no almacena información valiosa y tiene las cuentas bancarias más vacías que llenas. Con sus datos personales los delincuentes cibernéticos pueden hacerle extorsiones a usted o a personas de su círculo cercano, montar estafas usando su nombre y hacer toda clase de fechorías. Su vida en Internet deja la cantidad de datos suficiente como para que le puedan hacer mucho daño.

Latinoamérica guarda las claves de sus redes sociales en las páginas que utilizan, el 54 por ciento de sus correos electrónicos, el 32 por ciento de los accesos a tiendas en línea y un nueve por ciento de contraseñas bancarias.

Con esta acción, los usuarios están expuestos a que ante un posible ataque de un malware que tenga la capacidad de recolectar los datos almacenados en el programa o el equipo, un atacante se quede con toda esta información.

"Hay que ser recelosos y precavidos con la información, llevar un registro convierte a la persona en un blanco fácil para que todos sus datos queden expuestos en un solo golpe", indica

Martínez.

La extensión de la contraseña juega un papel fundamental. Busque que su clave sea de mínimo 10 caracteres, aunque lo ideal sería que supere los 15, y combínelo con diferentes letras en mayúsculas y minúsculas, haga uso de números y símbolos.

"Algo que es muy práctico y seguro es pensar en una frase, no únicamente una palabra, y empezar a mezclarla con caracteres especiales o reemplazando las vocales por números. Con esto se blinda y se cierra la posibilidad de que le puedan 'hackear' o interceptar la contraseña", señala Ramírez.

Doble autenticación

Además, la mayoría de páginas y plataformas cuentan con mecanismos de doble factor de autenticación. No sea perezoso y actívelo, eso hará que aun cuando un atacante se quede con su contraseña no pueda acceder a su cuenta, ya que necesita un código aleatorio adicional, que puede llegar a su celular o a través de herramientas biométricas, como huella digital, lectura de iris o reconocimiento facial. Esta opción ya está integrada en varios modelos de teléfonos inteligentes.

Y si quiere una alternativa aún más segura y sofisticada, puede hacer uso de herramientas como gestores o administradores de contraseñas. En el mercado hay opciones gratuitas o pagas, lo importante es que siempre acceda a estas plataformas a través de páginas o aplicaciones oficiales.

Estos programas permiten que se cree una contraseña con características diferentes para cada una de las cuentas que tenga. Estas quedan asociadas a la página determinada y ni siquiera es necesario que el usuario las conozca, lo único que debe hacer es recordar la clave del gestor, que se encargará de poner la clave correcta cada vez que sea necesario. "Lo valioso de este tipo de información que está adentro está cifrada, no tiene la información visible", señala Martínez.

Por último, no olvide cambiar su clave mínimo cada tres meses. Eso le agregará una capa de seguridad más para que no sea víctima de suplantación de identidad o estafa.