



Boletín de Ciberseguridad

Fecha de Publicación

01/04/2021 - N.º 5

Mes de Abril

01/04/2021 - 11/04/2021

Índice

Introducción	pág. 2
Explotación de fallas críticas en SAP	pág. 3
Errores críticos en VPN de Fortinet.....	pág. 4
Millones de teléfonos de usuarios de Facebook publicados.....	pág. 6
Son comercializados datos de usuarios de LinkedIn.....	pág. 8
Nuevo malware en Android se aprovecha usando publicidad engañosa sobre Netflix.....	pág. 9
Node.js publica actualizaciones para vulnerabilidades criticas	pág. 11
Distribución de Ransomware a nivel mundial.....	pág. 13
Conclusiones.....	pág. 15

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de las importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta primera quincena del mes de abril se destacan 7 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 3 de fraudes activos y 2 de prevención.

Aquellas vulnerabilidades y noticias de fraude consideradas de condición crítica, a tener especial recaudo son las siguientes:

Explotación de fallas críticas en SAP

“Es una vulnerabilidad crítica que permite a atacantes ejecutar comandos OS sin autenticación y acceder a la aplicación a la vez que también a su base de datos, ganando control completo de la información de negocios y procedimientos incluidos en SAP.”

Errores críticos en VPN de Fortinet

“Dos de las tres vulnerabilidades ya parcheadas enumeradas en el aviso, CVE-2018-13379 y CVE-2020-12812, son particularmente graves porque hacen posible que los delincuentes informáticos no autenticados roben credenciales y se conecten a VPN que aún no se han actualizado.”

Millones de teléfonos de usuarios de Facebook publicados

“A fines del 2019 Facebook tuvo una brecha de seguridad a través de la explotación de una vulnerabilidad que permitía extraer nombre completo, número celular, identificador de Facebook, género, ocupación, ciudad, país, fecha de creación de la cuenta.”

Son comercializados datos de usuarios de LinkedIn

“Al igual que con la base de datos de Facebook, un atacante con todos estos datos puede llevar a cabo ataques de phishing contra nosotros al conocer nuestro nombre, correo y muchos más datos, dando un toque de realismo si se hace pasar por un banco u otra empresa con la que tengamos contratados servicios. “



Explotación de fallas críticas en SAP

CRÍTICO

Descripción

Fuentes oficiales han compartido una alerta para aquellos usuarios del sistema SAP y aplicaciones relacionadas con el programa. **Se ha descubierto fallas de consideración crítica, que en caso de ser explotadas por atacantes pueden dejar expuesta información confidencial de los usuarios.**

“Dicha alerta detalla las técnicas con que agentes maliciosos pueden ganar el control total de aplicaciones SAP que no cuentan con las adecuadas medidas de seguridad, y sufrir robo de datos sensibles, la alteración de procesos de negocio críticos, ransomware y una paralización total de sus operaciones.”

Afectados

Son varios los productos afectados, pero se destacan entre otros:
SAP Solution Manager (SolMan).
Solución CRM basada en SAP Net Weaver
El componente BC-BMT-BPM-DSK de SAP NetWeaver AS JAVA 7.5

Estado

Se ha detectado una explotación activa sobre los sistemas SAP a menos de 72 horas de que se lanzara la actualización de la falla. SAP es usado por más de una noventa por ciento de las organizaciones más grandes a nivel mundial.

Su explotación exitosa **podría resultar en ataques de denegación de servicio (DoS) y en acceso no autorizado a información confidencial.**

"Permite a atacantes remotos leer archivos arbitrarios a través de secuencias de directorio transversales, resultando en una liberación no autorizada de información y también pudiendo permitir acceso arbitrario a recursos OS, lo que podría derivar en un escalamiento de privilegios."

Es un error de consideración crítica, **podría resultar que un atacante introduzca comandos OS sin autenticarse accediendo al programa su base de datos, obteniendo un control total del equipo del cliente.**

Remediación / Referencias

Se recomienda acceder al sitio de soporte de SAP e informarse sobre parches y actualizaciones disponibles, así como sobre nuevos lanzamientos.

Soporte de SAP:

<https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html>

Por mayor información acceder a:

<https://www.csirt.gob.cl/noticias/sap2021/>

<https://www.csirt.gob.cl/media/2021/04/10CND21-00051-01-SAP.pdf>



Errores críticos en VPN de Fortinet

CRÍTICO

Descripción

Han quedado expuestos tres errores críticos en la VPN de FORTINET, esto **puede ser aprovechado por cibercriminales sin autenticación previa, pudiendo acceder a la VPN que aún no se han actualizado, robando así credenciales de acceso.**

"Si las credenciales de VPN también se comparten con otros servicios internos (por ejemplo, si son Active Directory, LDAP o credenciales de inicio de sesión único similares), el atacante obtiene acceso de inmediato a esos servicios con los privilegios del usuario cuyas credenciales fueron robadas"

Afectados

Versiones afectadas: Fortinet FortiOS VPN.

Estado

Fue confirmado que las fallas en esta empresa dedicada al desarrollo y comercialización de software, dispositivos y servicios de ciberseguridad, están siendo actualmente explotadas.

A continuación, se destaca por su gravedad la siguiente:

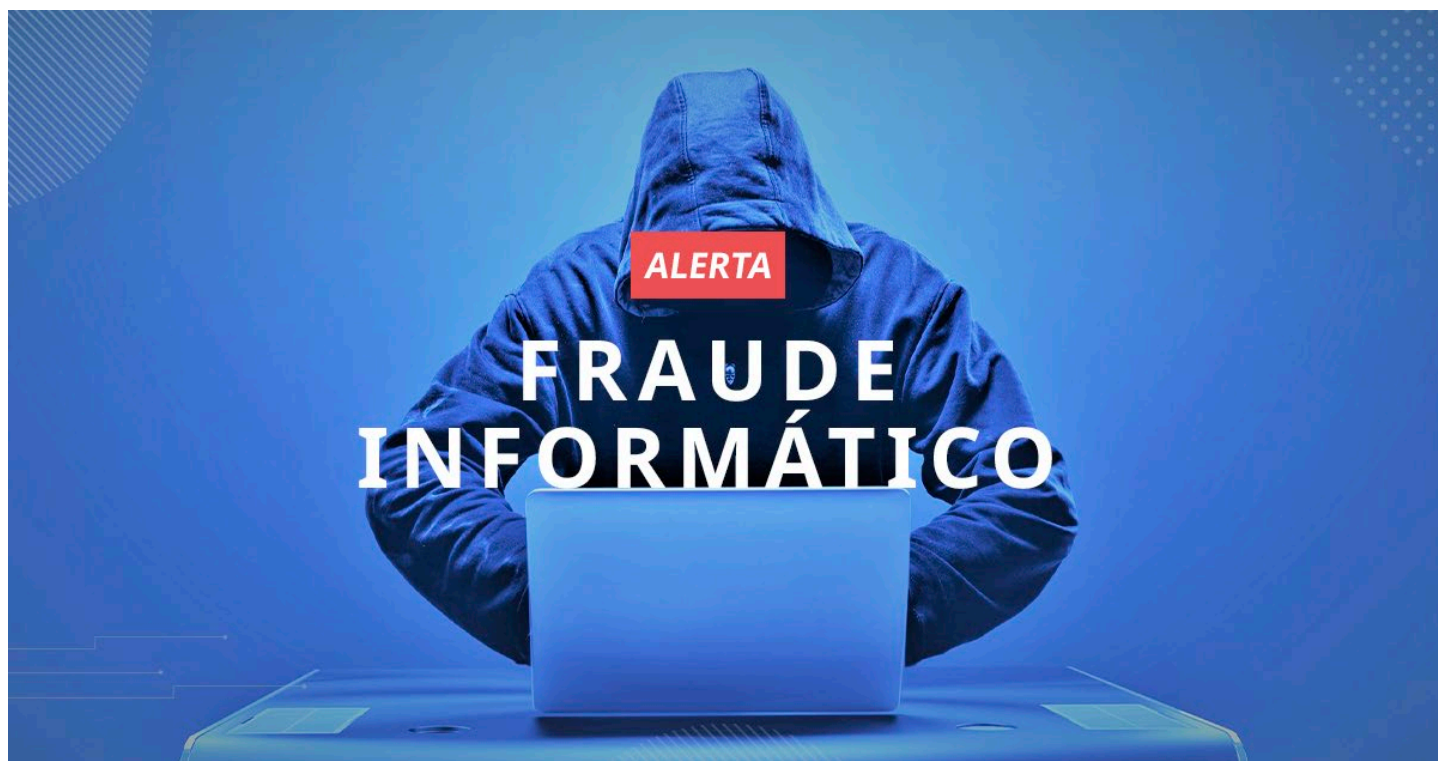
“Uno de los errores de seguridad más graves, CVE-2018-13379, fue encontrado y revelado por los investigadores Orange Tsai y Meh Chang de la firma de seguridad Devcore. Las diapositivas de una charla que dieron los investigadores en la Conferencia de Seguridad de Black Hat en 2019 lo describen como una *"lectura de archivos arbitraria previa a la autorización"*, lo que significa que permite al explotador leer bases de datos de contraseñas u otros archivos de interés. Además, hay múltiples tutoriales de explotación.”

Remediación / Referencias

Por mayor información invitamos a visitar los siguientes sitios:

<https://arstechnica.com/gadgets/2021/04/feds-say-hackers-are-likely-exploiting-critical-fortinet-vpn-vulnerabilities/>

<https://blog.segu-info.com.ar/2021/04/delincuentes-explotan-vulnerabilidades.html>

facebook **Millones de teléfonos de usuarios de Facebook publicados****CRÍTICO****Descripción**

A fines del 2019 Facebook tuvo una brecha de seguridad a través de la explotación de una vulnerabilidad que permitía extraer nombre completo, número celular, identificador de Facebook, género, ocupación, ciudad, país, fecha de creación de la cuenta. Facebook ha resuelto la vulnerabilidad al día de hoy.

La información extraída aparentemente fue comercializada entre la comunidad de ciberdelincuencia al menos desde el año pasado. En enero de este año, un bot de Telegram permitía a los usuarios buscar datos mediante una tarifa.

Pero el sábado pasado esta filtración de datos fue publicada en un foro de hacking de forma gratuita. Esta información personal de los usuarios brinda a los ciberdelincuentes la posibilidad de hacer hacerse pasar por ellos o estafarlos para que entreguen credenciales de inicio de sesión, por ejemplo.

Afectados

Datasec pudo acceder a los datos vinculados de Uruguay e identificar que son reales. Realizando un análisis extraemos algunos resúmenes:

La mayoría son de números ANTEL, luego de Movistar y finalmente de Claro. Si lo vemos por compañía:

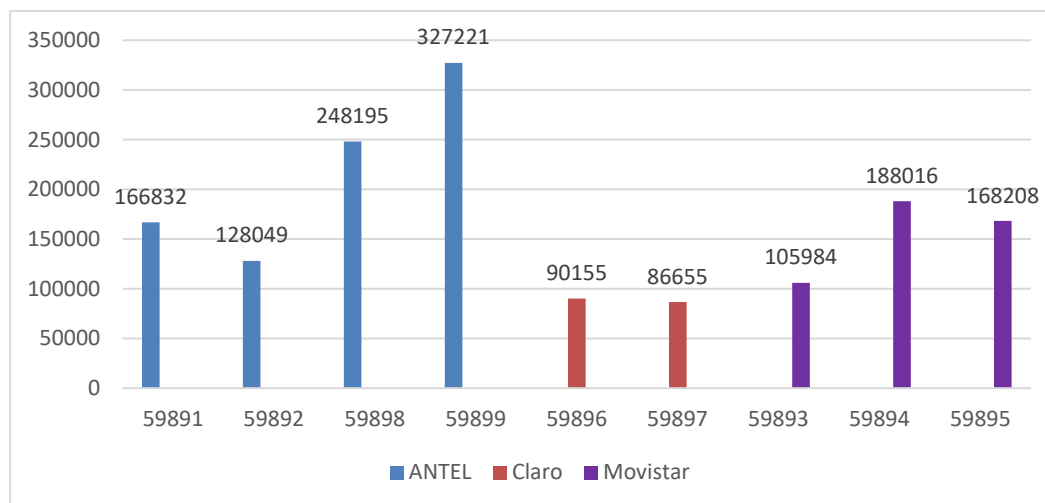
Antel: 870297

Claro: 176810

Movistar: 462208

(Hay 2 cuentas con "basura" en su número de teléfono, por lo que la suma no da el total).

Mirando los códigos asociados (5989x) por cada compañía podemos discriminarlo en un gráfico:



Si vemos por la "situación sentimental" los datos se dividen:

ESTADO	Sexo			Total, estado
	Hombre	Mujer	(vacío)	
Soltero(a)	66614	48356	3874	118844
En una relación	48674	42387	3417	94478
Comprometido(a)	10575	9353	749	20677
Casado(a)	45001	52596	2936	100533
En una relación civil	619	794	24	1437
En una pareja de hecho	2728	3012	121	5861
En una relación abierta	1024	825	45	1894
Es complicado	1819	1483	81	3383
Separado(a)	3935	3354	130	7419
Divorciado(a)	3801	4922	208	8931
Viudo(a)	1403	2916	110	4429
TOTAL, por sexo	186193	169998	11695	

Estado

La información extraída comprende 533 millones de números de celular y usuarios de 106 países, entre ellos, Uruguay.

En este país particularmente Datasec pudo acceder a los datos vinculados e identificar que son reales.

Remediación / Referencias

Esto puede dar lugar a que usuarios desprevenidos terminen viendo comprometida sus cuentas a través de ataques de phishing o ataques dirigidos. ¡A estar atentos!

Por mayor información al respecto se puede acceder a:

<https://www.datasec-soft.com/blog/millones-de-telefonos-de-usuarios-de-facebook-publicados>

Puedes verificar si tu celular fue expuesto [aquí](#).

	Son comercializados datos de usuarios de LinkedIn	CRÍTICO
--	--	----------------

Descripción

Fueron expuestos datos de millones de usuarios de LinkedIn y puestos a la venta en la Deep Web. Cibercriminales se filtraron en la red social (orientada al uso empresarial, a los negocios y al empleo), vulnerando su sistema, generando así una base de datos con información confidencial, siendo ofrecida posteriormente para su compra.

Los datos expuestos: LinkedIn IDs - Nombre Completo - Correo electrónico - Números telefónicos - Genero - Links para perfiles de LinkedIn - Links de perfiles para otras Redes de Información Profesional.

“Al igual que con la base de datos de Facebook, un atacante con todos estos datos puede llevar a cabo ataques de phishing contra nosotros al conocer nuestro nombre, correo y muchos más datos, dando un toque de realismo si se hace pasar por un banco u otra empresa con la que tengamos contratados servicios. “

Afectados

“Desde su fundación en 2002, sigue aumentando el número de usuarios en LinkedIn año tras año, tanto que las estadísticas de perfiles en LinkedIn han superado por mucho las expectativas en cuanto al número de personas conectadas a esta red (en comparación con las estadísticas de LinkedIn en 2020 de aproximadamente 722 millones de usuarios).”

En 2016 Microsoft compro LinkedIn por más de 20.000 millones de dólares, convirtiéndose en una de las compras más costosas de Microsoft después de Skype Technologies en 2011.

Estado

Se cree que los datos fueron sustraídos utilizando la técnica de scrapping. Además, no se descarta el intento de adivinar contraseñas de LinkedIn, mediante fuerza bruta. También utilizando phishing mediante llamadas telefónica y suplantando también la identidad de otras personas.

“Web scraping o raspado web, es una técnica utilizada mediante programas de software para extraer información de sitios web. Usualmente, estos programas simulan la navegación de un humano en la World Wide Web ya sea utilizando el protocolo HTTP manualmente, o incrustando un navegador en una aplicación.”

La información ha sido puesta a la venta en RaidForums, un sitio dedicado a compartir bases de datos y herramientas pirateadas, como credenciales personales.

Remediación / Referencias

Alentamos a crear contraseñas únicas y específicas para cada sitio web que use y no reutilizarlas, por si en caso de ser vulnerado, su información no quedara expuesta en su totalidad.

También se recomienda la utilización de verificación en dos pasos con aplicaciones como Google Authenticator.

Por mayor información acceder a los siguientes sitios:

<https://www.adslzone.net/noticias/seguridad/500-millones-cuentas-linkedin-filtracion-2021/>

<https://blog.segu-info.com.ar/2021/04/500-millones-de-usuarios-de-linkedin.html>

	Nuevo malware en Android se aprovecha usando publicidad engañosa sobre Netflix	IMPORTANTE
---	---	-------------------

Descripción

Se ha descubierto un malware en Google Play oculto en una aplicación falsa que es capaz de propagarse a través de los mensajes de WhatsApp y utilizando aviso falso de Netflix, para hacer phishing.

“Los investigadores encontraron el malware oculto dentro de una aplicación en Google Play llamada *“FlixOnline”*. La aplicación es un servicio falso que pretende permitir a los usuarios ver contenido de Netflix de todo el mundo en sus teléfonos móviles. Sin embargo, la aplicación está diseñada para monitorear las notificaciones de WhatsApp del usuario y para enviar respuestas

automáticas a los mensajes entrantes del usuario utilizando el contenido que recibe de un servidor de comando y control remoto (C&C)."

Este gusano de Android presenta nuevas técnicas innovadoras y peligrosas para propagarse y para manipular o robar datos de aplicaciones confiables como WhatsApp.

Afectados

A lo largo de 2 meses, la aplicación falasa "*FlixOnline*" fue descargada más de 500 veces, Google ya eliminó la aplicación de Play Store.

Estado

"Si el usuario descarga la aplicación falsa y, sin saberlo, le otorga los permisos adecuados, el malware es capaz de responder automáticamente a los mensajes entrantes de WhatsApp de la víctima con un *payload* recibido de un servidor de comando y control (C&C). Este método único podría haber permitido a los actores de amenazas distribuir ataques de phishing, difundir información falsa o robar credenciales y datos de las cuentas de WhatsApp de los usuarios, entre otras actividades."

Remediación / Referencias

En el caso de tener su equipo haya resultado comprometido, se debe eliminar la aplicación y cambiar las contraseñas.

Se recomienda estar atento, ya que usuarios desprevenidos pueden ver comprometida sus cuentas a través de ataques de phishing o ataques dirigidos. ¡A estar atentos!

Por mayor información al respecto se puede acceder a:

<https://research.checkpoint.com/2021/new-wormable-android-malware-spreads-by-creating-auto-replies-to-messages-in-whatsapp/>

<https://blog.segu-info.com.ar/2021/04/500-millones-de-usuarios-de-linkedin.html>



Node.js publica actualizaciones para vulnerabilidades críticas

PREVENCIÓN

Descripción

Se publicaron en el mes de abril actualizaciones que deben ser inmediatamente instaladas si son usuarios de node.js.

Afectados

Versiones afectadas: 14.x, 12.x and 10.x.

Todas las versiones del 10 a 15 de la aplicación.

Vector de Ataque

No se conoce actividad de explotación reciente en estas vulnerabilidades.

Se destaca entre ella la que se **encuentra en el módulo y18n npm la cual puede ser aprovechada a través de Prototype pollution o contaminación del prototipo.**

Contaminación de prototipos: es una falla peligrosa y subestimada muchas veces que afecta a las aplicaciones de JavaScript.

JavaScript está basado en prototipos: cuando se crean nuevos objetos, estos transfieren las propiedades y métodos del "objeto" prototipo, que contiene funcionalidades básicas como toString, constructor y hasOwnProperty.

La herencia basada en objetos le da a JavaScript la flexibilidad y eficiencia a los programadores web en el manejo de la aplicación, pero también lo hace vulnerable a la manipulación.

Los actores malintencionados pueden realizar cambios en toda la aplicación modificando el objeto, de ahí el nombre contaminación de prototipo.

Curiosamente, los atacantes ni siquiera necesitan modificar directamente el objeto; pueden acceder a él a través de la propiedad "__proto__" de cualquier objeto JavaScript. Y una vez que realiza un cambio en el objeto, se aplica a todos los objetos JavaScript en una aplicación en ejecución, incluidos los creados después de la manipulación.

Otra de las vulnerabilidades de gravedad afecta NULL pointer o puntero nulo. Un puntero es una variable que apunta o referencia a una ubicación de memoria en la cual hay datos.

A través del puntero se puede:
Crear la ubicación de memoria.
Acceder a los datos en dicha ubicación de referenciación.
Destruir" la ubicación de memoria.

Remediación / Referencias

Se exhorta a tomar medidas preventivas y estar atento ante nuevas publicaciones sobre el tema.

"Todos los problemas de seguridad en Node.js se tratan seriamente y deben ser reportados enviando un correo a security@nodejs.org. Este será recibido por un subgrupo del equipo central encargado de los problemas de seguridad."

Por mayor información al respecto se puede acceder a:

<https://nodejs.org/en/blog/vulnerability/april-2021-security-releases/>
<https://nodejs.org/es/security/>



Distribución de Ransomware a nivel mundial

PREVENCIÓN

Descripción

La presencia de malware y puntualmente de ransomware a nivel mundial se hace cada vez más constante y peligroso. Representando una amenaza tanto para clientes a nivel de usuarios, así como a pequeñas, medianas y grandes organizaciones independientemente del rubro a que se dediquen.

“Hoy día son conocidos los mapas de visualización de amenazas en tiempo real. Casi todos se basan en un *mapamundi* sobre el cual se dibujan los ataques que se van detectando, empleando un código de colores que muestran, como mínimo, el tipo de ataque en base a alguna clasificación.”

Se pueden seleccionar así los países para observar las detecciones de forma directa y de manera más sencilla.

Mapas: [Talos](#), [Threatbutt](#), [CheckPoint,Software](#), [Fortinet](#), [FireEye](#), [Kaspersky](#), [Bitdefender](#), [ArborNetworks](#), [Spamhaus](#), [SonicWall](#), [Netscout](#) y [LookingGlass](#).

Bitdefender hace una clasificación en tres tipos de ataques: ataque, infección y spam. Talos simplifica mostrando spam y malware. LookingGlass muestra en el mapamundi infecciones.

Otras variantes de mapa para ransomware específicamente son el mapa ofrecido por [Google](#) para casos en USA, además existen como otra opción [Statescoop](#) y [K-12 Cyber Incident Map](#).

“Statescoop mapea casos de *ransomware* conocidos ofreciendo un resumen de la información sobre los incidentes, por ejemplo, la cantidad demandada por los atacantes y si fue pagada o no. Cabe destacar que, de los mapas generales, SonicWall ha incorporado nuevos resultados como parte de sus analíticas en los cuales se puede seleccionar diferentes características. Una de ellas es el ransomware.”

Afectados

La mayoría de estos ataques son dirigidos a dispositivos conectados de manera remota mediante una red, aunque no quedan tampoco eximidos aquellos ataques realizados presencialmente de forma física, ante el descuido de un usuario en el manejo de sus credenciales, información confidencial, etc.

Vector de Ataque

Todo el tiempo son descubiertas vulnerabilidades Zero Day, que al no ser tomadas en cuenta y solucionadas en un corto plazo, le da al atacante un periodo mayor para realizar un exploit exitoso, ingeniería social, entre otras modalidades de cibercrimen.

Se ha analizado que estos grupos delictivos continúan explotando activamente los errores que van surgiendo en los distintos proveedores de servicio, expandiendo sus operaciones en todo el mundo.

Remediación / Referencias

Los ciberdelincuentes desarrollan herramientas y estrategias para vulnerar los sistemas de seguridad, lo que genera un desafío para los especialistas en estar informados para poder tomar medidas preventivas y de mitigación al respecto.

El servicio de Hacking Etico es una medida acertada para el análisis de vulnerabilidades, en la prevención ante futuros ataques.

Por mayor información al respecto se puede acceder a:

<https://www.crn.com/news/security/revil-ransomware-targets-acer-s-microsoft-exchange-server-source>

<https://blog.segu-info.com.ar/2021/04/mapas-sobre-ataques-de-ransomware.html>

Conclusiones

Esta quincena tuvimos filtraciones masivas de información privada, esto puede ser utilizado en campañas de ingeniería social dentro de las organizaciones, para reconocer puntos débiles en las personas que trabajan y colaboran. ¡No solo eso, sino que también a nivel personal podemos ser amenazados y envueltos en diversos fraudes que serán facilitados porque públicamente se conocen datos nuestros!

Las redes sociales han sido un castillo de cartas que creció muy rápido y se está dilapidando día a día, su poder es épico y los controles técnicos de seguridad implementados en las empresas están colapsando.

La responsabilidad una y otra vez más es de todos y todas; Cuidándonos de llamadas por teléfono, o de spam o correos de phishing. Para eso, lo recomendable en estos casos es extremar la precaución con las llamadas o correos que recibamos: Por ejemplo, puede que recibamos correos de hackers haciéndose pasar por LinkedIn, donde sólo buscan que les proporcionemos la contraseña y otra información para poder acceder. Lo recomendable para cerciorarnos si se trata o no de un email real es entrar en la web oficial de LinkedIn y hacer nosotros manualmente los cambios sin pinchar en ningún enlace sospechoso.

Otra recomendación es no reutilizar nunca las contraseñas entre varios servicios, ya que con que consigan hackearla en una web, pueden reutilizarla en otra para tomar el control de las cuentas si no tenemos activada la verificación en dos pasos. Para eso, es recomendable usar gestores de contraseñas con contraseñas únicas para cada plataforma. A su vez, la verificación en dos pasos con aplicaciones como Google Authenticator es recomendable siempre que se pueda, ya que es mucho más segura que usar los SMS.

¡Estemos alertas y difundamos las recomendaciones para protegernos entre todos y todas!