7 mejores prácticas de seguridad para evitar un ataque de ransomware

- *Esta amenaza ha afectado al 30% de las empresas que ha sufrido un ataque cibernético.*

Las amenazas y virus cibernéticos son tan antiguos como la historia misma de las computadoras y el internet. Sin embargo, pocos ataques son tan generalizados y perjudiciales en la actualidad como el ransomware.

El también llamado “software de rescate” es un programa informático malicioso que tuvo su primera aparición en 2013 y ha afectado al 30% de las empresas que ha sufrido un ataque cibernético, esto de acuerdo con una encuesta de Sophos a 3,100 organizaciones que aparece en el estudio *How to Stay Protected Against Ransomware*.

Este virus tiene la finalidad de encriptar los ficheros informáticos y restringir el acceso a determinadas partes o archivos del sistema que infecta. Por su parte, los afectados quedan obligados a pagar una suma de dinero a los hackers para recuperar el uso y control de sus datos, a pesar de que cuenten con cierto nivel de seguridad. De hecho, de acuerdo al estudio, 9 de cada 10 de los encuestados señalaron que su seguridad estaba al corriente cuando sufrieron un ataque.

Por lo anterior, **Sophos**, el líder mundial en seguridad cibernética de última generación, ha enlistado las 7 mejores prácticas de seguridad para evitar un ataque de ransomware y que tu empresa u organización se encuentren siempre protegidos:

1.- Usa parches
El malware que no ingresa a través de un archivo, lo hace a través de errores de seguridad populares, incluyendo aplicaciones como Office, diversos navegadores, Flash y etcétera. En cuanto más parches de seguridad sean instalados, más difícil será para los intrusos tomar control de tus sistemas e información y hacer mal uso de los mismos.

2. Haz copias de seguridad
Independientemente del ransomware, existen decenas de formas en las que puedes perder tu información de manera repentina. Por eso, es fundamental que cifres una copia de seguridad y elabores un plan de recuperación ante desastres que cubra la restauración de datos y sistemas completos.

3. Examina los archivos JavaScript (.JS) en un bloc de notas

Al abrir un archivo JavaScript en el Bloc de notas, se bloquea la ejecución de scripts maliciosos y te permite examinar el contenido del archivo.

4. Ten cuidado con los archivos adjuntos no solicitados
Los hackers confían en el dilema que enfrentas cuando recibes un archivo adjunto. En caso de que tengas duda sobre el remitente, ¡no lo descargues ni abras!

5. Monitorea los derechos de administrador
Revisa constantemente los derechos de administrador y administrador de dominio. No permanezcas conectado como administrador por mucho tiempo y evita navegar, abrir documentos u otras actividades laborales regulares mientras estás en una sesión con derechos de administrador.

6. Regula el acceso a tu red externa
No dejes tus puertos expuestos al mundo. Bloquea el acceso RDP de tu organización y otros protocolos de administración. Además, usa la autenticación de dos factores y asegúrate de que los usuarios remotos se autentiquen a través de una VPN.

7. Usa contraseñas seguras
Suena lógico, pero muchas veces pasa desapercibido. Una contraseña débil y predecible puede dar acceso a los hackers a toda tu red en cuestión de segundos. Se recomienda tengan al menos 12 caracteres de largo, incluyan una combinación de mayúsculas y minúsculas, y algún signo de puntuación aleatorio.

Finalmente, una de las mejores prácticas de protección contra hackeos es contar con un sistema de ciberseguridad de última generación que te permita tener el control de tus operaciones de forma permanente. En este caso, puedes optar por el Intercept X de **Sophos**, el cual combina tecnologías de vanguardia, *Deep Learning* y la detección y respuesta para *endpoints*, ofreciendo una protección inigualable contra el malware, los exploits y el ransomware desconocidos.

Si quieres conocer más, visita https://www.sophos.com/es-es.aspx y conoce más sobre ciberseguridad de última generación.

# # #

Sobre Sophos
Como líder mundial en seguridad cibernética de última generación, **Sophos** protege a casi 400 mil organizaciones de todos los tamaños en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrollado por SophosLabs -un equipo global de *Threat Intelligence* y *Data Science*- las soluciones nativas de la nube y mejoradas por IA de Sophos, aseguran protección en puntos finales (computadoras portátiles, servidores y dispositivos móviles) y redes contra tácticas y técnicas cibercriminales en evolución, incluidas las filtraciones de adversarios activos y automáticos, ransomware, malware, exploits,

exfiltración de datos, phishing y más. La galardonada plataforma basada en la nube de Sophos Central integra toda la cartera de productos de **Sophos**, desde la solución de punto final, Intercept X, hasta el Firewall XG, en un único sistema llamado Seguridad Sincronizada. Los productos de **Sophos** están disponibles exclusivamente a través de un canal global de más de 47 mil socios y proveedores de servicios gestionados (MSP).

Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido, y cotiza en la Bolsa de Londres bajo el símbolo "SOPH". Más información está disponible en www.sophos.com

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/Sophos
LinkedIn: https://www.linkedin.com/company/sophos/
Instagram: https://www.instagram.com/sophossecurity/?hl=es-la
Youtube: https://www.youtube.com/user/SophosProducts

Contacto

Fernanda Cornejo
fernando.cornejo@another.co
M.: 55 2916 7477

Mario García
mario@another.co
M.: 55 3930 2474