5 consejos de ciberseguridad para empresas y hogares en el Día del Internet Seguro

- *En 2020 el 34% de las organizaciones en el mundo fueron víctimas de malware, el 29% sufrieron exposición de datos sensibles y el 28%, de ransomware*

CIUDAD DE MÉXICO. 9 de febrero de 2021.- Este 9 de febrero se conmemora el Día Internacional del Internet Seguro, una fecha para generar consciencia sobre los riesgos que implica navegar por internet sin establecer las medidas de seguridad cibernética necesarias ante la creciente ola de amenazas que acechan tanto a negocios como a equipos domésticos.

Sin embargo, la ciberseguridad no es cuestión de un día, ya que las amenazas maliciosas se propagan a diario y en cualquier momento. De hecho, según el Reporte de Amenazas 2021 de Sophos, el 34% de las organizaciones en el mundo fueron víctimas de malware el año pasado, mientras que el 29% sufrieron exposición de datos sensibles y el 28% de ransomware, siento las principales amenazas.

Por ello, estar alertas debe convertirse en un hábito para todos. Desde Sophos, emitimos 5 recomendaciones, tanto para empresas como para usuarios domésticos, con el fin de fomentar las buenas prácticas de seguridad cibernética a diario:

1. Mantente al día en cuanto a parches de seguridad
La mayoría de las empresas tienen el hábito de instalar parches de seguridad, pero aún existen quienes no se toman el tiempo necesario para hacerlo o actualizarlos. Cabe recordar que los delincuentes trabajan constantemente en encontrar huecos dentro de la red, por lo que no actualizar los parches de seguridad en semanas o meses vuelve vulnerable a tu negocio.

En el caso de las familias también aplica esta recomendación, ya que por lo general sus equipos son los que pasan más tiempo sin este tipo de actualizaciones, en ocasiones por desconocimiento. En ese sentido, es importante mencionar que los parches de seguridad no únicamente deben instalarse en su laptop, sino que también se debe poner especial atención en los dispositivos móviles, como celulares y tabletas, además de otros dispositivos conectados como cámaras de seguridad, asistentes domésticos, entre otros.

2. Necesitas saber lo que tienes
Ya sea en un registro de activos, inventario de TI o una simple lista de los equipos y *software* que se utilizan, es necesario que al interior de la empresa siempre se debe de saber qué se tiene conectado a su red. Esto con el fin de identificar equipos antiguos o desactualizados que podrían ser el blanco de un cibercriminal.

Lo mismo pasa en los hogares, en donde además de estar pendientes de la protección de sus computadoras, se debe poner especial énfasis en los *smartphones* y tabletas conectadas a la red doméstica, ya que en recientes años se han vuelto un foco de atención para los ciberdelincuentes.

3. Configura una línea directa de seguridad

Incluso las empresas más pequeñas necesitan un contacto directo con el personal de ciberseguridad de la organización para reportar anomalías en la operación. No necesariamente debe ser un número telefónico, puede tratarse de una dirección de correo electrónico fácil de recordar a la que de inmediato se avisa sobre posibles amenazas de ciberataque y situaciones extrañas en sus equipos.

Para los hogares es importante tener a la mano contactos como el de la Policía Cibernética de la Secretaría de Seguridad Pública, por mencionar un ejemplo. Esta institución brinda atención a los habitantes de la Ciudad de México, y a la que se pueden denunciar fraudes cibernéticos, *phishing*, acoso en línea, entre otros delitos. Si se cuenta con un proveedor de ciberseguridad doméstico, también se debe de tener a la mano un correo electrónico de atención al cliente de su proveedor de ciberseguridad doméstico, esto con el fin de solicitar soporte cuando se encuentre alguna anomalía mientras navega.

4. Establece una estrategia de respaldo adecuada

Es importante fomentar la generación constante de copias de seguridad de los equipos, sobre todo aquellos que trabajan con información sensible que podría ser objetivo de ciberdelincuentes. También, se debe de contar con copias de seguridad sin conexión y fuera del sitio, aparte de aquellas que se almacenan en la nube. Esto para evitar el riesgo de que los ciberdelincuentes las encuentren en la red y las destruyan antes de propagar un ataque.

Para las familias es importante mencionar que este tipo de copias de seguridad se pueden hacer desde su computadora con el fin de proteger los datos de dispositivos extraviados o robados, y no necesariamente por ciberataques.

5. Elige las contraseñas adecuadas

Parece muy obvio, pero es importante reiterar que una contraseña adecuada no debe incluir parámetros fáciles de adivinar como fechas de nacimiento o nombres de mascotas. También debemos recordar que se debe evitar que estas contraseñas se repitan para tener acceso a distintas plataformas, esto tanto para negocios como familias.

Otra recomendación, para familias y negocios por igual, es utilizar la autenticación de doble factor. Este tipo de herramientas generan códigos de 6 dígitos que se envían por mensaje de texto a los teléfonos celulares de las personas, vía correo electrónico, o mediante otros canales. Cuando al usuario se le hace llegar ese código, se le notifica que existe un intento de acceso a su cuenta en un dispositivo, con el fin de que la persona escriba el código en la

plataforma a la que desea entrar, o en su defecto notifique que no se trata de él y evite que los ciberdelincuentes logren entrar a su cuenta.

La ciberseguridad es todo un viaje, no un destino. Es decir, la protección debe ser constante y evolucionar conforme las propias amenazas cambian también, sin importar qué tan seguro creas que ya estás.

###

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (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. Para obtener más información visita www.sophos.com.

Síguenos en:

Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/