Únete al Día del Internet Seguro y sigue estos 5 consejos para no caer en manos de los hackers

Con el objetivo de concientizar acerca de un uso responsable, crítico y creativo de las herramientas tecnológicas, cada año diversas organizaciones alrededor del mundo unen esfuerzos para conmemorar el día del internet seguro (o Safer internet Day) el 11 de febrero, dado que las amenazas cibernéticas están en constante evolución.

De acuerdo con el reporte “El rompecabezas imposible de la ciberseguridad” de Sophos, 2 de cada 3 empresas son víctimas de ciberataques cada año. Por esta razón, siempre es importante mantenerse actualizado y estar preparado frente a nuevas amenazas que muestran ser cada vez más complejas y

sofisticadas como el ransomware, el cual aprovecha las vulnerabilidades de los mismos sistemas de seguridad mediante un proceso automatizado para el secuestro de información valiosa.

Por ello, en el marco del **Día Internacional del Internet Seguro**, Sophos, líder mundial en seguridad cibernética de última generación habilitada para la nube, comparte 5 consejos básicos para evitar caer en manos de los hackers:

1. Mantén tus parches de seguridad actualizados

De entrada, contar con parches de seguridad para la protección de información en tu negocio u organización es fundamental. Sin embargo, su actualización sigue siendo una práctica poco usual en los departamentos de TI, resultando en un alto grado de vulnerabilidad debido a los "agujeros de seguridad" que presentan versiones anteriores. Recuerda: los delincuentes nunca posponen sus ataques.

2. Refuerza tu estrategia de respaldo

A diferencia de los parches de seguridad, es preferible no invertir demasiado tiempo en crear muchas copias de seguridad, pues una práctica bastante común hoy en día entre los delincuentes es buscar esos respaldos en línea para desencadenar sus ataques. Asegúrate de que tu estrategia también incluya copias de seguridad tanto offline como offsite.

3. Refuerza tu configuración de privacidad

La gran mayoría de aplicaciones y plataformas en línea utilizados en los espacios de trabajo, cuentan con una serie de configuraciones de privacidad y seguridad que ayudan a controlar la amplitud con que se comparten e indexan infinidad de datos personales. Sin embargo, todas ellas lo hacen de manera diferente, por lo que es necesario ajustar cada uno de ellos para asegurarse de brindar una protección eficaz.

4. Lleva un control cuidadoso en los equipos de tu empresa o negocio

Reutilizar equipo antiguo para sacarle el máximo provecho y de paso reducir algunos costos siempre es una buena idea; sin embargo, debes llevar un registro minucioso de todo lo que hay en tu inventario. De hacerlo, mantén actualizado sus sistemas de seguridad en todos estos dispositivos, pues hoy en día los criminales han encontrado en ellos una nueva vía de ataque para obtener información.

5. Toma seriamente el uso de contraseñas adecuadas

Aunque pueda parecer un consejo obvio y repetitivo, la verdad es que el uso de contraseñas “poco fiables” (Ej.: 1234567890) aún representa una gran ventana de oportunidad para los ataques. Cuando se trata de protección corporativa también supone una gestión correcta de accesos, lo que significa cancelar rápidamente las cuentas de empleados inactivos, así como animar al personal a reportar si su contraseña les permite ver datos que no deberían para reducir el riesgo de una posible filtración de datos.

La seguridad en la información de tu negocio no es cuestión de

un solo día, debe ser una actividad constante en las buenas prácticas de las organizaciones. Los criminales también mejoran cada día la efectividad en sus ataques, por ello, es importante llevar la seguridad cibernética al siguiente nivel, no importa lo protegido que creas que estás.