¿Corro el riesgo de ser "hackeado"?

Ciudad de México, 12 de septiembre de 2024.- La seguridad cibernética se ha convertido en una preocupación primordial para los usuarios en todo el mundo. De hecho, el Reporte de Riesgos Globales 2024 del Foro Económico Mundial y Zurich Insurance Group revela que casi el 40% de los líderes mundiales coinciden en que los ciberataques son un riesgo crucial con el potencial de desencadenar una crisis material en un futuro cercano.

Esta preocupación no se limita a grandes empresas; individuos de todos los sectores también enfrentan el peligro de ser vulnerados. Según Zurich y Marsh McLennan, en un reporte emitido de manera reciente, el costo global del cibercrimen se proyecta hacia casi 24 mil millones de dólares para 2027.

Ante dicho escenario, señala el reporte, la brecha en la protección contra riesgos cibernéticos exige una acción colectiva urgente tanto del sector asegurador como del público en general. Añade que la necesidad de proteger nuestra información personal y profesional nunca había sido tan crítica.

- ¿Cómo proteger mi información?

Desde la perspectiva de Zurich México, la primera medida esencial de protección que deben implementar los mexicanos es mantener los softwares que utilizan en sus labores diarias y actividades personales debidamente actualizados.

Las actualizaciones regulares del sistema operativo, aplicaciones y antivirus no solo introducen nuevas funciones, sino que también corrigen vulnerabilidades que los hackers podrían explotar.

Generalmente los equipos de cómputo emiten recordatorios periódicos a los usuarios cuando se requieren actualizaciones; ignorarlas puede dejar tu dispositivo expuesto a amenazas conocidas que los desarrolladores ya han solucionado en versiones recientes.

Además, es crucial adoptar contraseñas robustas y únicas para cada cuenta. Una contraseña fuerte combina letras mayúsculas y minúsculas, números y caracteres especiales, y evita el uso de información fácilmente accesible, como fechas de cumpleaños o nombres de mascotas. Datos de Hive Systems indican que una contraseña débil, es decir corta y que solo emplea número y/o letras sin combinaciones de caracteres especiales, puede ser descifrada hasta en 6 segundos por cibercriminales.

También es recomendable usar una contraseña distinta para cada servicio minimiza el impacto de una brecha de seguridad en un solo sitio, reduciendo el riesgo de que tus otras cuentas sean comprometidas.

Además de una contraseña segura, hoy es fundamental emplear la autenticación multifactor (MFA) la cual añade una capa adicional de protección que requiere del uso de biométricos, como la huella dactilar, y de autorizaciones en otros dispositivos.

Esto hace que incluso si un hacker obtiene tu contraseña, aún necesitará un segundo método de verificación para acceder a tus cuentas. Configurar MFA en tus plataformas más importantes, como el correo electrónico y servicios financieros, puede ser una barrera efectiva contra accesos no autorizados.

También es importante tener cuidado con los correos electrónicos y mensajes sospechosos. Los ataques de phishing, que buscan engañar a los usuarios para que revelen información sensible, están en aumento. No hagas clic en enlaces ni descargues archivos de fuentes desconocidas, y siempre verifica la autenticidad de las solicitudes antes de proporcionar cualquier información personal.

La protección de tu red doméstica también juega un papel crucial en la seguridad cibernética. Asegúrate de que tu red Wi-Fi esté protegida con una contraseña fuerte y evita usar contraseñas predeterminadas que pueden ser fácilmente adivinadas. Considera la posibilidad de actualizar tu router a un modelo más reciente que ofrezca mejor seguridad y configuraciones más avanzadas.

Finalmente, educarse sobre las amenazas cibernéticas y estar al tanto de las mejores prácticas de seguridad puede marcar una gran diferencia. Mantente informado sobre las últimas amenazas y vulnerabilidades y participa en formaciones o cursos de ciberseguridad cuando sea posible. La preparación y el conocimiento son tus mejores herramientas para protegerte contra los ataques cibernéticos.

En resumen, la ciberseguridad es una responsabilidad que recae tanto en el sector empresarial como en los usuarios individuales. Al adoptar medidas proactivas para proteger tus dispositivos y tu información personal, puedes reducir significativamente el riesgo de ser "hackeado" y contribuir a un entorno digital más seguro para todos.

-o0o-

Zurich está transformando los seguros ya que ofrece cada vez más servicios de prevención, como aquellos que promueven el bienestar y mejoran la resiliencia climática. Reflejando su propósito de “crear juntos un futuro mejor”, Zurich aspira a ser una de las empresas más responsables y de mayor impacto en el mundo. Tiene como objetivo emisiones netas cero para 2050, y tiene la calificación ESG más alta posible de MSCI. El Grupo Zurich tiene alrededor de 60,000 empleados y tiene su sede en Zurich, Suiza.

Como empresa especializada en seguros de autos, entre otras verticales, Zurich cuenta con diferentes opciones, coberturas y asistencias para cubrir las necesidades de cada usuario. Para conocer más sobre la cartera de productos de Zurich y sobre esta alianza, visita: https://www.zurich.com.mx/es-mx