EL OBSERVADOR

Fecha: 14/10/2024 Audiencia: 4.500 Sección: OPINION
Vpe: $316.116 Tirada: 1.500 Frecuencia: DIARIO
Vpe pág: $1.088.000 Difusión: 1.500
Vpe portada: $1.088.000 Ocupación: 29,05%

OPINIÓN

Marcelo Mora
CEO de IDOK

La importancia de protegerse de la suplantación digital en esta era

Hoy en día la suplantación de identidad digital es una amenaza cada vez más latente. Este fenómeno, lejos de ser una simple molestia, se ha convertido en un peligro real que puede tener consecuencias devastadoras, tanto económicas como sociales, para sus víctimas, sin importar si son personas particulares o empresas.

Las cifras son alarmantes. Según un reciente estudio realizado por Javelin, una reconocida consultora de estrategia e investigación financiera, el fraude por robo de identidad en Estados Unidos alcanzó la astronómica cifra de $23 mil millones de dólares en 2023, lo que representa un aumento del 13% respecto al año anterior. Estos números son una muestra de un fenómeno mundial y que no discrimina.

Los métodos respecto a cómo opera esta "amenaza invisible" son variados. Pueden ser ataques informáticos simples, pero efectivos, hasta acciones más sofisticadas, dado que los ciberdelincuentes están en constante evolución, adaptándose a las nuevas medidas de seguridad con una velocidad vertiginosa. Casos recientes, como transferencias fraudulentas de vehículos realizadas desde la cárcel o intentos de desviar grandes sumas de dinero a cuentas falsas, demuestran la creciente sofisticación de estos delincuentes digitales.

Frente a este panorama, la clave está en la prevención y en la adopción de hábitos de seguridad digital que, aunque simples, pueden marcar la diferencia entre ser una víctima más o mantenerse a salvo en el ciberespacio.

Desde nuestra vereda, destacamos siempre la importancia de utilizar servicios de certificación acreditados de acuerdo a las legislaciones locales, especialmente al realizar trámites en línea que involucren firmas electrónicas.

Otra recomendación es la protección de nuestras claves de acceso. En la era digital, nuestras contraseñas son las llaves de nuestro castillo virtual. Compartirlas o almacenarlas en lugares inseguros es equivalente a dejar las puertas de nuestra casa abiertas de par en par. Asimismo, la desconfianza ante enlaces sospechosos y la navegación exclusiva en sitios web seguros son prácticas que deben convertirse en segunda naturaleza para todo usuario de internet.

En el ámbito empresarial, la responsabilidad es aún mayor. Las compañías, independientemente de su tamaño, deben considerar la protección de datos personales como una prioridad absoluta. La encriptación de bases de datos y la realización de respaldos regulares no son lujos, sino necesidades imperativas en un mundo donde el ransomware se ha convertido en una amenaza constante.

Desde la educación en ciberseguridad hasta la implementación de políticas públicas que protejan a los ciudadanos en el entorno digital, todos tenemos un papel que desempeñar. La tecnología avanza a pasos agigantados, ofreciéndonos oportunidades inimaginables, pero también exponiendo nuevas vulnerabilidades. Por esto, la vigilancia constante y la adopción de prácticas seguras no son opcionales, sino que una obligación para generar la mejor defensa contra las amenazas invisibles que acechan en el mundo virtual.