

Principales errores que exponen sus datos a estafas online

En el mundo digital la protección de datos financieros privados se ha convertido en una preocupación primordial.

Según la **División de Investigación de Delitos de Alta Tecnología (Divindat)**, en el **Perú** se registran más de 300 denuncias al mes por delitos informáticos. “La información personal es cada vez más valiosa para los **ciberdelincuentes**, y por ello emplean diversas técnicas para aprovecharse de la falta de conocimiento y descuido de las personas”, indicó la gerente de Seguridad de la Información de **Rímac**, Johanna Cuba.

Precisó que es importante mantener informadas a las personas sobre los principales errores y descuidos que pueden exponer sus datos personales, ser robados o exponerlos a estafas, así como sobre las recomendaciones clave para evitar convertirse en una víctima más de los ciberdelincuentes.

Lea también: Ciberseguridad: Cinco claves para evitar robos en internet

A continuación, se enumera los principales errores en las que incurren las personas:

1. No ingresar usuarios o claves personales desde

dispositivos ajenos o contactándose a redes de internet públicas, ya que esto puede facilitar el acceso no autorizado de terceros a sus cuentas, aplicaciones, etc. La recomendación es utilizar únicamente equipos de su propiedad y acceder a internet vía redes seguras.

2. **No abrir correos ni enlaces desconocidos o no solicitados**, porque estos pueden contener **malware** (software malicioso) o pueden redirigir a sitios web falsos con el fin de robar sus datos personales, usuario, claves, etc. Es recomendable abrir solo correos conocidos o, mejor aún, solo aquellos cuyo origen haya podido confirmar, y nunca hacer click en enlaces, links o similares que no haya solicitado.
3. **Usar contraseñas seguras y autenticación de dos factores**: Una contraseña robusta debería tener no menos de 8 caracteres (combinando números, letras mayúsculas y minúsculas, signos, etc). Además de mantenerla en absoluta reserva, es recomendable que configure factores de autenticación adicionales, es decir que además del usuario y clave, ingrese por ejemplo una respuesta que solo usted conozca o un código variable que se genere en un token o que reciba vía mensaje o similar.
4. **Descargar aplicaciones únicamente de tiendas oficiales**: Los **ciberdelincuentes** optan por desarrollar aplicaciones para descarga gratuita a través de las que capturan su información o acceden ilícitamente a sus equipos o aplicaciones. Para reducir ese riesgo debe descargar aplicaciones únicamente de tiendas oficiales como **Google Play** o **App Store**.

Lea también: Ciberdelincuencia: Tips para proteger tu dinero

«Recuerde que los bancos, compañías de seguros, tiendas oficiales online y otras plataformas de servicios de empresas formales, nunca solicitarán sus datos de usuario, **contraseñas, claves, códigos o datos de identidad personales a través de mensajes de texto, de WhatsApp o por redes sociales.**», agregó Johanna.