SEGURIDAD

¿Cómo protegerse de las estafas digitales?

Las estafas digitales han ido en aumento. De acuerdo con expertos en ciberseguridad hay maneras de protegerse, pero la inteligencia artificial va perfeccionando esta táctica.

TECNOLOGÍA. Imagen referencial sobre un sobre un sistema hackeado. (Foto: cortesía)

Por **Redacción La Hora,** 13 de noviembre 2025 • 12:30 hs

En el supuesto correo recibido se muestra como la supuesta entidad financiera envía una notificación por **correo electrónico**, debido a una actividad inusual. En este se piden datos personales para validar la identidad de la persona y su firma digital. Sin embargo, el usuario alertó que el correo que se emitió no corresponde a un correo oficial del banco que mostraba.

Así también, en octubre, el **Registro Civil** alertó sobre **estafas digitales**. Personas que no pertenecían a la institución realizaban llamadas ofreciendo servicios falsos de trámites para obtener la cédula de identidad.

La entidad detalló que cuando se registra la llamada y la persona acepta la supuesta asistencia, los atacantes proporcionan un número de celular al que se debe enviar una palabra clave y un código para que nuevamente sea contactado por los atacantes y que le instalen una aplicación maliciosa.

De acuerdo con la **Fiscalía**, se registraron datos desde 2015 hasta 2025, en donde las estafas han ido en incremento con el 71,5%.

En el caso de los ciberdelitos **Pichincha** lidera este ránking con 8.809 casos, y le sigue **Guayas** con 4.644 casos.

Diana Maldonado, tecnóloga en informática y técnica en **ciberseguridad**, detalla que este tipo de **delitos** han incrementado, debido a lo que los usuarios han visto en redes sociales, e incluso por lo que les ha llegado.

datos personales y bancarios para almacenar los datos ciudadanos y cometer los ciberdelitos.

2. Smishing: son estafas que se realizan por medio de mensajes de texto. Por medio de estos se ofrecen supuestos servicios de entrega. Con ello, una vez que las personas ingresan en los enlaces que son enviados a través de este sistema, se les pide llenar sus datos personales.

Maldonado aseguró que estas estafas digitales son aún más riesgosas con el auge de la inteligencia **artificial (IA)**, ya que se puede clonar una voz con tan solo unos segundos de grabación.

“Hay casos en los que se han registrado llamadas, donde la voz clonada es la grabación usada por un **ciberdelincuente**.

Maldonado alertó que con la **inteligencia artificial** estos delitos se vuelven más fáciles de realizar, para crear páginas falsas, para obtener datos de la ciudadanía o la redacción de correos electrónicos.

Para **Rafael Bonifaz, representante** de Derechos Digitales, hay varias estrategias para los delitos digitales y que van ligados a lo que se conoce como “ingeniería social”, que es básicamente engañar a alguien de diversas formas. Una de estas puede ser apelando a las emociones de la ciudadanía en las que se menciona supuestos ganadores de dinero hasta las estafas que se producen por medio de la **extorsión** con llamadas.

Bonifaz indicó que el tipo de **estafas** en las que se realizan llamadas a las personas y se infunde miedo diciendo que la persona que le llama pertenece a una banda delictiva y exige dinero, por lo que este tipo de estafa “tiene que ver con las **filtraciones de datos** que ha habido en Latinoamérica, pero también en Ecuador, en particular”.

¿Qué medidas tomar para no caer en las estafas digitales?

“Ninguna entidad bancaria va a pedir nuestros datos por correo”, enfatizó **Diana Maldonado**. Esa es la principal alerta que se debe tomar en cuenta.

También recomendó no hacer caso a mensajes que se den en cadena para transmitirlos, porque pueden contener **enlaces maliciosos** con los que pueden instalar malwares en los equipos. Además, señaló que se puede silenciar las llamadas de contactos que no se tienen registrados.

Bonifaz aconsejó que las personas deben dudar de lo que le ofrecen. Y destacó que hoy en día con la **IA**, es muy fácil hacer parecer a cualquier contenido como real.

“La recomendación es que duden, que no se entusiasmen demasiado, acudan a las fuentes y se informen por medios que sean conocidos”, dijo.

Enfatizó en que se debe evitar descargar archivos que provengan de fuentes **desconocidas** y evitar llamadas de **desconocidos**.

Estafas digitales sancionadas con prisión

De acuerdo con el artículo 190 del **Código Orgánico Integral Penal (COIP)**, quien utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones, para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, será sancionada con una pena privativa de la libertad de 1 a 3 años.

Esta misma sanción se impondrá “si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de **claves secretas** o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes”. (PSR)

Tags: Seguridad digital | Estafas digitales | Ecuador