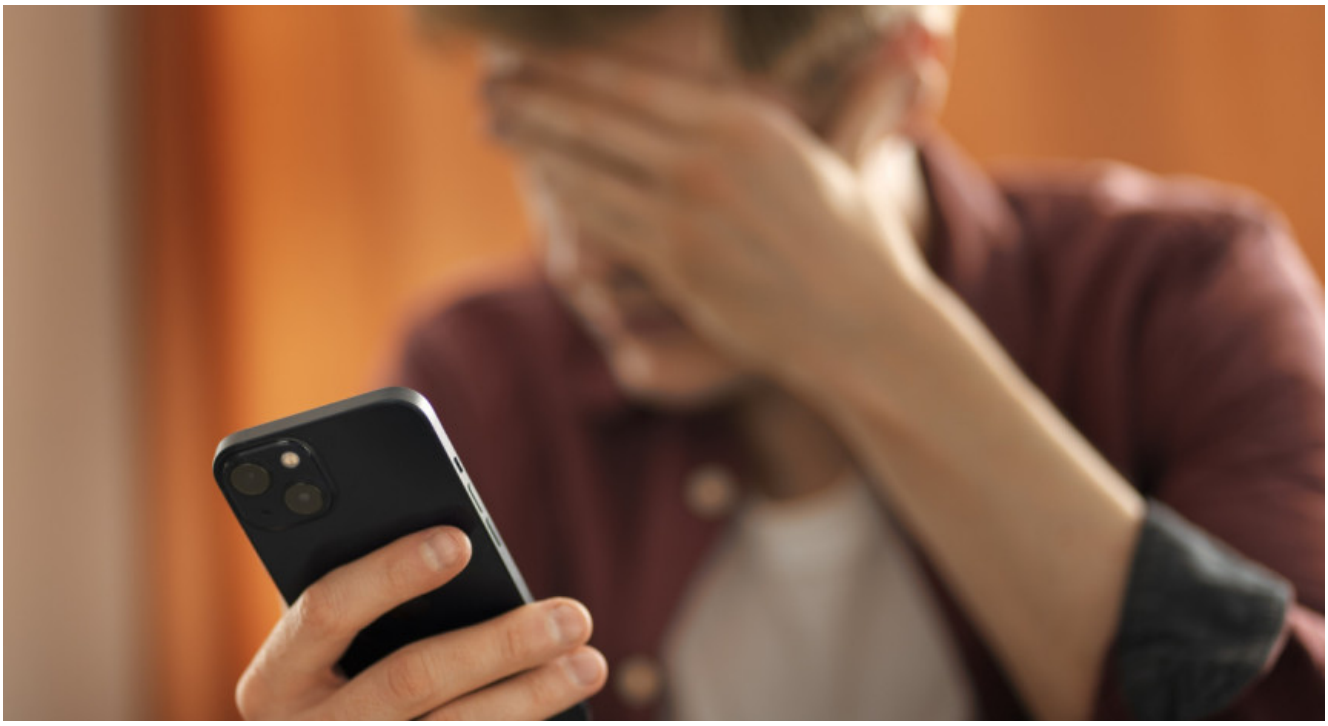
Ola de ciberestafas: la pregunta clave para reconocer el posible robo de datos

11/04/2025



Las estafas telefónicas crecen cada día más y se van transformando a medida que se van **descubriendo** las técnicas que implementan los ciberdelincuentes. Una de las más utilizadas en la actualidad es la **clonación de voz** con ayuda de la inteligencia artificial. Tras realizar un escaneo previo de los contactos, es posible **imitar tonos de voz y modismos,** haciendo **creer a la víctima** que está hablando un familiar o pariente.

Estas estafas telefónicas tienen el objetivo de inducir a la víctima a que **revele cualquier tipo de información o contraseña.** En algunos casos, incluso logran engañar a las personas para que hagan una **transferencia bancaria o revelen datos confidenciales.**

Ante esta ola de estafas, los expertos informaron que hay una

pregunta clave que puede ayudar a determinar si la llamada proviene de un estafador o de alguien de confianza: **«¿Cuál es el nombre de mi primera mascota?».**

Estafa telefónica. Foto: Freepik.

Esta pregunta es ideal ya que se considera que los ciberdelincuentes **no tienen forma** de saber cómo se llamaba tu primera mascota o si en realidad alguna vez tuviste una. Si la respuesta no es satisfactoria, es probable que sea una estafa. En ese momento, se recomienda **cortar la comunicación de inmediato** y hacer la denuncia correspondiente si se brindó algún dato confidencial.

¿Cómo reconocer una estafa telefónica?: las tres frases más utilizadas por los ciberdelincuentes

Especialistas en ciberseguridad explicaron que los delincuentes suelen utilizar preguntas específicas que pueden funcional como **señales de alerta** para darse cuenta de que es un engaño, como por ejemplo:

1. **“Vamos a simular un crédito”.** Esta frase es para aparentar que se está ofreciendo un servicio a cambio de los datos personales.
2. **“Le enviamos un código de seguridad a su teléfono”.** Esta es otra de las frases más utilizadas por los estafadores, ya que le permite el acceso a cuentas bancarias o billeteras virtuales.
3. **“Vamos a instalar una aplicación”.** Con esta opción, el estafador logra inducir ala víctima a que instale un software con el cual puede acceder a su información personal y financiera que esté cargada en el celular.

Estafa telefónica. Foto: Freepik.

Cómo aumentar la seguridad

Para **aumentar la seguridad** es muy importante tener agendados a todos los contactos conocidos. Si tenés un llamado inesperado o con un perfil sospechoso, atendelo pero con los recaudos necesarios o, directamente, **cortá la llamada**. Si el llamado proviene de alguien que conocés, podrá c**onectarse por otros medios.**

Además, cabe recordar que ni los bancos ni ningún organismo te pedirá información confidencial. En tal caso, te lo pedirán mediante un **correo verificado** o de **forma presencial** en las respectivas sucursales habilitadas.

Fuente: Canal 26