Usan IA para robar datos sensibles: cómo evitar la estafa virtual que es cada vez más popular en Argentina

11/02/2025

Gracias al rápido avance de la inteligencia artificial, los estafadores logran clonar voces, crear mensajes de texto altamente realistas y producir videos falsos para suplantar a personas de confianza. Ahora, esta tecnología permite la elaboración de **una nueva estafa tan efectiva como peligrosa**.

La mentira que está circulando actualmente tiene que ver con **Gmail**, donde una operadora falsa con un acento extremadamente realista llama por teléfono solicitando datos sensibles para desbloquear la cuenta.

Estafa con Gmail, el correo electrónico de Google. Foto: Unsplash.

Cada vez más organismos públicos y empresas populares están

lanzando advertencias y precauciones para los clientes y usuarios debido a la **gran cantidad de estafas virtuales** que se están propagando en la web, ya sea a través de llamados telefónicos, mensajes de WhatsApp camuflados o con mail repletos de enlaces sospechosos.

Lo más peligroso de esta moda es que buscan a sus víctimas en base a la vulnerabilidad, ya que **saben quiénes son los más propensos a caer en estos robos**: gente mayor, sola y sin conocimiento de las nuevas tecnologías y sus peligros.

Cómo evitar la estafa con IA. Foto: Unsplash

Cómo evitar caer en la estafa de phishing

El **phishing** es un delito cibernético que consiste en engañar a las personas para obtener información personal. Los ciberdelincuentes se hacen pasar por una empresa o entidad de confianza para robar datos como contraseñas, números de tarjeta de crédito, números de cuenta bancaria, entre otros.

En este caso, hacen lo propio haciéndose pasar por operadores de Gmail. **Para evitar caer en la estafa, es necesario tomar algunas precauciones y cuidados:**

- **Nunca responder correos electrónicos** que soliciten datos personales y no hacer click en enlaces compartidos
- **Nunca un banco o un organismo público pedirá que se cambien los datos personales** o claves por internet, a través de un enlace enviado en un correo, por redes sociales o mediante un llamado telefónico.
- **Estar atento a la redacción del mensaje** o en el enlace enviado. Muchas veces, es casi imperceptible, pero en algún lugar dejan ver el fraude con faltas de ortografías u alteraciones en la URL que supuestamente es oficial

- **No confiar en avisos promocionales**, regalos, descuentos, préstamos o algún corte de servicio.
- **Usar el doble factor de autenticación** en todas las aplicaciones
- Si hay que cambiar la contraseña, asegurarse de hacerlo **siempre desde el sitio oficial** del banco o de la aplicación.

Fuente: Canal 26