

Claves para ayudar a los adultos mayores a evitar estafas digitales

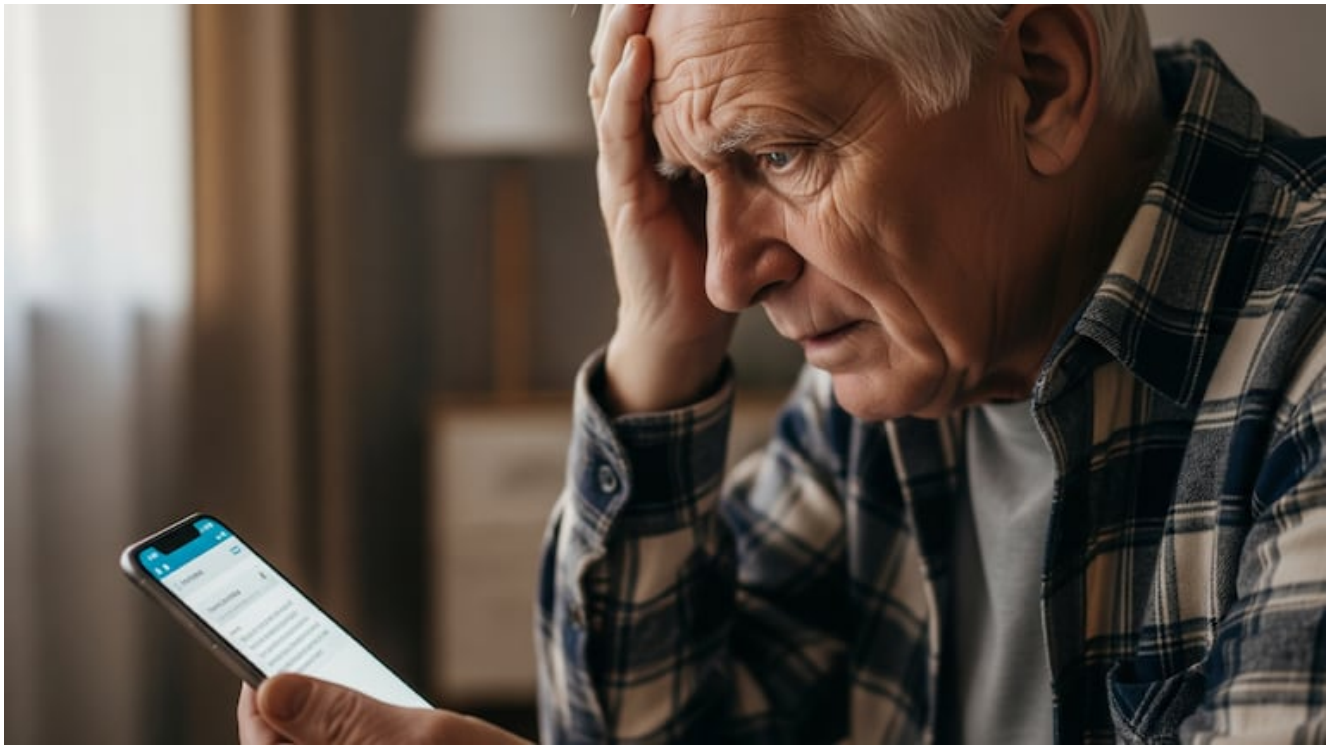
17/11/2025



Los adultos mayores son uno de los principales objetivos de los ciberdelincuentes. Desde correos con phishing y mensajes de WhatsApp que simulan llegar desde un organismo oficial o de familiares, hasta falsos descuentos exclusivos, los engaños digitales a este grupo no paran de crecer.

Los estafadores operan con una lógica simple: buscan obtener ganancias con el menor riesgo posible. En ese esquema, las personas de más edad se convierten en un blanco atractivo por múltiples factores que se combinan.

Muchos cuentan con ahorros o tienen un **ingreso estable** (jubilación). A esto se suma una **confianza generacional** en las instituciones y en la autoridad, que hace que una “llamada del banco” o un “correo oficial” no despierte sospechas inmediatas.



Claves para ayudar a los adultos mayores a evitar estafas digitales. (Imagen: GeminiAI)

La soledad y el aislamiento también abren la puerta a engaños emocionales, como las estafas románticas o los falsos vínculos personales. Además, **la sobrecarga digital** y el uso de dispositivos o contraseñas desactualizadas aumentan la vulnerabilidad frente a mensajes y sitios falsos que, cada vez más, imitan a la perfección lo real.

A todo esto, desde hace un par de años se sumó **la inteligencia artificial**, que **permite clonar** voces o crear videos falsos (*deepfakes*) que imitan a conocidos de la víctima o figuras públicas.

Los estafas más comunes

- **Phishing:** correos o mensajes que se hacen pasar por bancos, organismos de salud o el Estado. Incluyen un enlace que, al hacer clic, lleva a un sitio falso controlado por los ciberdelincuentes. Allí, pueden capturar credenciales, contraseñas, números de tarjetas de crédito, etcétera.

- **Soporte técnico falso:** muchos se publicitan en Google como ayuda para solucionar problemas relacionados a plataformas de streaming, líneas de celular o servicio de tv por cable, entre otros. Piden al usuario que instale un app que en realidad le da al estafador un acceso remoto para robar información o dinero.
- **Estafas románticas:** comienzan con un vínculo emocional que, con el tiempo, se transforma en pedidos de dinero para emergencias inventadas.
- **La estafa del familiar en apuros:** una llamada que imita la voz de un hijo o un nieto pidiendo dinero urgente. La emoción juega a favor del engaño.
- **Falsas inversiones:** promesas de rentabilidad rápida o proyectos inexistentes que terminan en pérdidas totales.

Cómo prevenir las estafas digitales: la importancia del diálogo familiar

La prevención empieza en casa. Las **conversaciones abiertas, sin culpa**, acusaciones ni juicios, son una herramienta clave para evitar el aislamiento digital. Hablar del tema con empatía puede marcar la diferencia. Al fin de cuentas, **todos podemos caer en un engaño**.

Algunos consejos para iniciar ese diálogo:

- Explicar **cómo funcionan las estafas** y cómo actúan los ciberdelincuentes con ejemplos concretos y cercanos, no con tecnicismos.
- Proponer **reglas para los llamados de emergencia** familiares como, por ejemplo, elegir una palabra clave para verificar la identidad en llamados o mensajes de WhatsApp.
- **Compartir una experiencia real** (propia o de terceros)

para normalizar la posibilidad de equivocarse.

Medidas de ciberseguridad prácticas y fáciles de aplicar

Las buenas prácticas de seguridad informática no son complicadas ni exclusivas de los expertos. Las puede aplicar cualquiera y son fáciles de aprender:

- **No hacer clic en enlaces recibidos** por email o mensajes de WhatsApp no solicitados.
- **No descargar apps** desde links recibidos en chats de soporte técnico. Solo bajar apps desde Google Play Store o Apple Store.
- En un chat de WhatsApp con un organismo oficial o una empresa, **verificar el tilde azul** al lado del nombre. No tener en cuenta la foto de perfil.
- **Usar contraseñas únicas y robustas.**
- **Activar la autenticación de dos factores (2FA)** en la app que lo permitan.
- **Encender el bloqueo de ventanas emergentes y llamadas automáticas** en el celular.

Además, es recomendable activar las **protecciones especiales que ofrecen los bancos**: límites en transferencias, alertas para familiares o doble verificación telefónica en operaciones sospechosas.

Fuente: TN