

Cómo reconocer una estafa por WhatsApp o redes sociales

“¡Felicidades! Ganaste un premio.”

“Necesito que me prestes dinero urgentemente.”

“Tu cuenta será bloqueada. Entra aquí para verificarla.”

“Tenemos una oportunidad de inversión que no puedes perder.”

Todos estos mensajes pueden parecer reales. Pero también pueden ser el comienzo de una estafa.

Los delincuentes digitales utilizan WhatsApp, Instagram, Facebook y otras plataformas para intentar obtener **dinero, contraseñas, códigos o información personal**.

Aprende a reconocer estas **5 señales de alerta**.

1. Te ofrecen algo demasiado bueno

Un teléfono prácticamente gratis.

Un premio de un concurso en el que nunca participaste.

Una inversión que promete ganancias extraordinarias.

Un bono inesperado.

Una oferta con un descuento increíble.

Cuando algo parece demasiado bueno para ser verdad, **detente antes de actuar**.

Pregúntate:

¿Por qué me están ofreciendo esto?

Y, sobre todo:

¿Puedo comprobar que quien lo ofrece realmente existe?

2. Te presionan para actuar rápido

Los estafadores no quieren darte tiempo para pensar.

Por eso utilizan frases como:

 "Tienes 10 minutos para responder."

 "Tu cuenta será bloqueada hoy."

 "La oferta termina ahora."

 "Debes pagar inmediatamente."

La urgencia busca que actúes por impulso.

Recuerda:

Mientras más presión sientas, más importante es detenerte.

Una empresa, banco o institución legítima debería permitirte comprobar la información utilizando sus canales oficiales.

3. Te piden un código

Esta es una señal de alerta muy importante.

Alguien puede decirte:

"Te envié un código por error."

"Dime el código para confirmar tu identidad."

"Necesitamos verificar tu cuenta."

Ese código podría permitirle entrar a tu WhatsApp, correo electrónico o alguna otra cuenta.

Nunca compartas un código de verificación que llegue a tu teléfono.

Aunque quien lo solicite parezca ser alguien conocido.

4. Un familiar o amigo te pide dinero desde un número desconocido

Recibes un mensaje:

“Hola, cambié de número.”

La conversación parece normal.

Poco después aparece una emergencia:

“Necesito que me hagas una transferencia.”

Antes de enviar dinero:

☎ Llama al número que ya tenías guardado.

☎ Habla directamente con la persona.

❓ Haz alguna pregunta que permita confirmar su identidad.

Nunca confíes únicamente en lo que aparece escrito en un chat.

Incluso una fotografía de perfil conocida puede ser copiada.

5. Te envían un enlace sospechoso

Muchas estafas intentan llevarte a páginas falsas que imitan bancos, comercios, instituciones públicas o redes sociales.

Allí pueden pedirte:

- Usuario y contraseña.
- Número de tarjeta.
- Código de seguridad.
- Información personal.
- Códigos recibidos por SMS.

No introduzcas información sensible desde un enlace recibido inesperadamente.

Si el mensaje supuestamente viene de una empresa o institución, **entra directamente a su aplicación o página oficial** y comprueba allí si realmente existe algún problema.

Una nueva señal de alerta: voces, fotos y videos pueden ser falsos

La Inteligencia Artificial permite imitar cada vez mejor la voz y la apariencia de una persona.

Eso significa que recibir un audio, una fotografía e incluso un video **ya no siempre es suficiente para confirmar quién está detrás.**

Si un familiar te solicita dinero de manera inesperada, especialmente por una supuesta emergencia:

verifica por otra vía antes de pagar.

Una llamada directa o una pregunta personal puede ayudarte a comprobar su identidad.

La regla de las tres preguntas

Cuando recibas un mensaje sospechoso, pregúntate:

¿QUIÉN? · ¿POR QUÉ? · ¿POR QUÉ AHORA?

¿QUIÉN?

¿Puedo confirmar quién me está escribiendo?

¿POR QUÉ?

¿Por qué necesita mi dinero, información o código?

¿POR QUÉ AHORA?

¿Por qué intenta que actúe con tanta urgencia?

Si alguna respuesta no tiene sentido:

DETENTE.

¿Qué hacer si sospechas de una estafa?

No respondas apresuradamente.

No pulses enlaces.

No envíes dinero.

No compartas contraseñas ni códigos.

Verifica la información utilizando otro medio.

Y si confirmas que se trata de una estafa, **bloquea y reporta la cuenta o número desde la plataforma correspondiente.**

¿Y si ya caí en la estafa?

Actúa rápidamente.

Si entregaste una contraseña, **cámbiala inmediatamente.**

Si compartiste datos bancarios o realizaste una transferencia, **comúnicate cuanto antes con tu entidad financiera utilizando sus canales oficiales.**

Si entregaste acceso a alguna cuenta, revisa las sesiones abiertas, cierra los dispositivos que no reconozcas y activa la verificación en dos pasos.

También conserva capturas de pantalla, números, mensajes, comprobantes y cualquier otra evidencia relacionada con lo ocurrido.

El consejo de Alex

“Si alguien te pide dinero, una contraseña o un código y además quiere que lo hagas rápido, no te dejes presionar. Detente y verifica por otra vía. Un minuto comprobando puede evitarte un gran problema.”

Mini reto

Habla hoy con tu familia y acuerden algo muy sencillo:

UNA PALABRA DE SEGURIDAD FAMILIAR.

Elijan una palabra o pregunta que solamente ustedes conozcan.

Si algún día alguien llama diciendo ser un familiar y pide dinero por una emergencia, pueden utilizarla como una comprobación adicional.

Y recuerda: **no compartan esa palabra en redes sociales ni con otras personas.**

Recuerda

No confíes solo porque el mensaje parece real.

No pagues solo porque parece urgente.

No compartas códigos porque alguien te los pida.

Primero verifica.

Ciudadano Digital

Detente. Verifica. Protégete.