

Cómo identificar estafas en línea

Reconoce mensajes falsos, phishing y fraudes digitales · Principiante

SmartGuys.biz · smartguys.biz

Las 6 señales de alerta más comunes

- Ø=b" Urgencia extrema: "¡Actúa AHORA o perderás tu cuenta!" Los estafadores crean pánico para que no pienses con calma.
- Ø<ß• Premios inesperados: "¡Ganaste un iPhone!" Si no participaste en nada, no puedes haber ganado nada.
- Ø=Ý Links sospechosos: direcciones como "faceb00k-seguridad.com" o "banco-cr-verificacion.net" son falsas.
- Ø=Ü° Pago para recibir dinero: "Paga ¡5.000 para reclamar tu premio de ¡500.000." Nunca pagas para recibir dinero real.
- Ø=Üç Errores de ortografía: mensajes con muchos errores, texto en mayúsculas o traducción rara son señales de estafa.
- Ø=Ý Piden datos personales: tu banco NUNCA te pedirá contraseñas, PIN o números de tarjeta por correo o WhatsApp.

Tipos de estafas más frecuentes en Costa Rica

- Phishing bancario: correos o SMS que imitan a tu banco pidiendo que "verifiques" tu cuenta.
- Estafa del trabajo fácil: "Gana \$500 al día desde casa sin experiencia." Piden un pago inicial que nunca recuperas.
- Falsos técnicos de Microsoft: llaman diciendo que tu computadora tiene virus y piden acceso remoto.
- Estafa romántica: persona desconocida en redes que se enamora rápido y luego pide dinero por una "emergencia".
- Marketplace falso: venden artículos en Facebook Marketplace, cobran y nunca entregan.
- Smishing: SMS con links falsos de CORREOS, CCSS o bancos pidiendo datos.

¿Cómo verificar si algo es real?

- ' Verifica la dirección web: el sitio oficial de tu banco siempre termina en .cr o .com oficial. Busca el candado Ø=Ý .
- ' Llama directamente: si recibes un mensaje sospechoso, llama al número oficial (el del reverso de tu tarjeta).
- ' Busca en Google: copia el texto del mensaje sospechoso y búscalo. Si es una estafa conocida, aparecerán advertencias.
- ' Consulta con alguien de confianza: antes de hacer clic o pagar, consulta con un familiar o amigo.

⚡ Regla de oro

Si algo parece demasiado bueno para ser verdad, probablemente es una estafa. Tómate 5 minutos para verificar antes de actuar. Los estafadores siempre crean urgencia para que no pienses.

¿Qué hacer si caíste en una estafa?

- 1 Cambia inmediatamente las contraseñas de las cuentas afectadas.
- 2 Llama a tu banco si compartiste datos financieros o bancarios.
- 3 Reporta a la Policía Cibernética de Costa Rica: 2295-3643.
- 4 Reporta en la plataforma donde ocurrió (Facebook, WhatsApp, etc.).
- 5 No te avergüences — estas estafas están diseñadas por expertos para engañar a cualquiera.

Comparte esta información

Las estafas en línea afectan especialmente a personas mayores y a quienes tienen menos experiencia con tecnología. Comparte esta ficha con tu familia, vecinos y amigos. Puedes imprimirla y pegarla en un lugar visible.