GUÍA

ESTAFAS DIGITALES: CÓMO RECONOCERLAS Y PROTEGERTE



ECUADOR Chequea
PERIODISMO CON RIGOR

ChequeaLab

GUÍA PARA IDENTIFICAR ENGAÑOS EN INTERNET Y CUIDAR TU INFORMACIÓN PERSONAL



Las estafas digitales forman parte de los riesgos más comunes en internet. Pueden llegar por mensajes de texto, correos electrónicos, llamadas, redes sociales, anuncios o aplicaciones de mensajería. A veces prometen premios, ofertas o ayudas económicas.

Otras veces usan el miedo, la urgencia o la suplantación de identidad para que una persona entregue datos personales, dinero o acceso a sus cuentas.

Este manual explica de forma sencilla cómo funcionan estos engaños, cuáles son sus señales más frecuentes y qué hábitos pueden ayudarte a protegerte.

¿Qué son las estafas digitales?

Las estafas digitales son engaños que ocurren a través de medios tecnológicos con el objetivo de obtener dinero, datos personales, contraseñas o acceso a cuentas.

Pueden adoptar muchas formas: mensajes que se hacen pasar por bancos, enlaces falsos, supuestas promociones, ofertas de empleo, inversiones milagrosas, ventas inexistentes o contactos que intentan manipular a la víctima para que actúe sin pensar.

Aunque cambien de formato, casi todas comparten la misma lógica. Buscan generar confianza o presión para que la persona entregue algo valioso.

A veces lo hacen aparentando ayudar. Otras veces imitan instituciones, empresas o personas conocidas para parecer legítimas.

¿Por qué importan?

Las estafas digitales no solo afectan el bolsillo. También pueden exponer información sensible, comprometer cuentas personales y generar consecuencias emocionales importantes.

Una persona puede perder dinero, quedar expuesta a robo de identidad o perder acceso a sus redes, su correo o sus aplicaciones bancarias.

Además, estos engaños se adaptan con rapidez. Aprovechan momentos de necesidad, desconocimiento o urgencia.

Por eso pueden afectar a cualquier persona, incluso a quienes usan internet con frecuencia. No se trata de ingenuidad, sino de que muchas estafas están diseñadas precisamente para parecer convincentes.

¿Cómo circulan?

Estos engaños suelen llegar por canales cotidianos. Pueden aparecer en mensajes de WhatsApp, llamadas, SMS, correos electrónicos, publicaciones patrocinadas, enlaces compartidos en redes sociales o perfiles que se hacen pasar por negocios y servicios reales.

También pueden venir en forma de supuestas alertas de seguridad, ofertas con tiempo limitado o pedidos urgentes de un familiar o conocido.

Su fuerza está en que se parecen a situaciones reales. Por eso muchas veces una estafa no se ve extraña a primera vista.

Se presenta como algo habitual, cercano o urgente para que la víctima responda rápido y no se detenga a revisar.





¿Cómo funcionan?

Crean urgencia para que actúes rápido



Una de las estrategias más comunes es ‘apurarte’. El mensaje dice que tu cuenta será bloqueada, que tienes un premio por reclamar de inmediato o que debes hacer un pago urgente para evitar un problema.

Esa sensación de apuro busca que no pienses con calma ni revises los detalles.

Cuando una persona siente presión, es más probable que haga clic, comparta información o transfiera dinero sin verificar. Por eso la urgencia es una de las herramientas más efectivas en las estafas digitales.

Se hacen pasar por alguien confiable



Muchas estafas imitan a bancos, empresas de mensajería, instituciones públicas, tiendas, plataformas digitales o incluso personas conocidas.

Pueden usar nombres, logotipos, fotos de perfil o estilos de escritura que parecen auténticos.

En algunos casos, también copian páginas web o perfiles de redes sociales para que luzcan casi iguales a los verdaderos.

El objetivo es simple: que la víctima baje la guardia porque cree que está hablando con una fuente legítima. La apariencia de confianza es una parte central del engaño.

Prometen beneficios demasiado buenos



Otra táctica frecuente es ofrecer premios, descuentos extraordinarios, empleos fáciles, inversiones con ganancias rápidas o ayudas económicas inmediatas.

Estas promesas buscan activar el entusiasmo o la esperanza para que la persona actúe antes de cuestionar la oferta.

Cuando algo parece demasiado conveniente, demasiado rápido o demasiado perfecto, conviene revisar con más cuidado. En internet, lo llamativo no siempre es una oportunidad real.

Piden datos o accesos sensibles



Muchas estafas están diseñadas para obtener información valiosa. Pueden pedir números de tarjeta, claves, códigos de verificación, datos bancarios, fotografías de documentos o acceso a cuentas personales.

En otros casos buscan que la persona descargue un archivo, haga clic en un enlace o instale una aplicación que luego compromete su dispositivo.

La petición puede parecer razonable si el mensaje imita una situación real. Por eso es importante recordar que la mayoría de instituciones serias no solicita claves ni códigos sensibles por mensaje o llamada.



¿Qué puedes hacer?

Hacer una pausa antes de responder

La primera defensa frente a una estafa digital es detenerse. Si un mensaje genera miedo, emoción o presión, lo mejor es no responder de inmediato.

Tomarse unos minutos para revisar puede marcar la diferencia entre detectar el engaño o caer en él.

Las estafas dependen de la reacción rápida. La pausa rompe ese mecanismo y permite mirar con más atención.

Revisar quién está contactando

Antes de confiar en un mensaje, conviene verificar quién lo envía. Es útil revisar el número, la dirección de correo, el perfil, la página web o el enlace desde donde llega la información.

Muchas veces, al mirar con calma, aparecen detalles extraños: errores en el nombre, direcciones poco claras, dominios raros o cuentas recién creadas.

Cuando el contacto dice representar a una empresa o institución, lo más seguro es buscar sus canales oficiales por separado y confirmar la información allí, sin usar el enlace recibido en el mensaje.

Proteger tus datos personales

Una regla importante es no compartir contraseñas, códigos de verificación, datos bancarios ni fotos de documentos por canales no verificados.

Tampoco conviene entregar acceso remoto al celular o a la computadora a desconocidos que llaman con supuestas alertas técnicas o bancarias.

Cuidar los datos personales es una parte esencial de la protección digital. Una vez que esa información cae en manos equivocadas, puede usarse para nuevas estafas o para comprometer otras cuentas.

Confirmar antes de pagar o transferir

Si un mensaje pide dinero, solicita una transferencia o cambia de repente una cuenta de pago, lo más prudente es confirmar por otra vía. Esto es especialmente importante cuando el pedido parece venir de un familiar, un amigo o un negocio con el que ya existía contacto.

Confirmar por una llamada directa, un canal oficial o una conversación previa ayuda a evitar engaños que se aprovechan de la confianza.

Señales de alerta



El mensaje te presiona o te asusta

Una señal muy común es el tono de urgencia. Si el mensaje insiste en que debes actuar ahora mismo, que perderás una cuenta o que habrá consecuencias inmediatas si no respondes, conviene sospechar. La presión es una herramienta clásica para reducir la capacidad de revisar.



Hay errores o detalles extraños

Algunas estafas tienen errores de redacción, saludos genéricos, enlaces raros o nombres que no coinciden exactamente con los de la empresa o institución que dicen representar. Otras están mejor hechas, pero aun así suelen tener pequeños detalles inconsistentes. Esos indicios pueden ser una pista importante.



Piden información que no deberían pedir

Si alguien solicita tu clave, un código de seguridad, un token, datos completos de tu tarjeta o acceso a tu dispositivo, hay una señal de alerta clara. Las instituciones serias no suelen pedir esa información por mensajes improvisados ni por llamadas inesperadas.



La oferta parece demasiado buena o demasiado fácil

Los engaños también pueden llegar disfrazados de oportunidad. Premios que nunca solicitaste, inversiones con ganancias garantizadas, empleos con pagos altos y pocas condiciones o ventas con precios absurdamente bajos son escenarios que merecen una revisión cuidadosa. Cuando algo parece hecho para atraerte demasiado rápido, conviene desconfiar.





Las estafas digitales suelen presentarse de formas muy atractivas: ofertas laborales, créditos "imperdibles" o premios que parecen reales, pero que buscan engañar al usuario para obtener datos, dinero o acceso a cuentas.

Entender cómo funcionan estas estafas implica seguirles el rastro dentro de las propias redes donde nacen. Eso hizo Ecuador Chequea al sumergirse en TikTok y rastrear durante meses los videos que prometen créditos inmediatos, préstamos "sin buró" y oportunidades financieras que parecen hechas a la medida de la desesperación.

Lo que apareció no fue un conjunto de casos aislados, sino un ecosistema que crece y se sostiene en el tiempo.

Entre enero de 2022 y el 19 de noviembre de 2025, aparecieron más de 4.500 registros, que, una vez depurados, dejaron 719 videos únicos publicados por 156 cuentas distintas.



En conjunto, ese universo supera los 145 millones de reproducciones. Son cifras que no pasan desapercibidas: casi 5 millones de "me gusta", más de 920.000 compartidos y alrededor de 221.000 comentarios demuestran que el contenido engancha, circula y encuentra audiencia.

No todas las cuentas tienen miles de seguidores.

Muchas, de hecho, apenas superan el millar. Pero hay perfiles que han logrado consolidar comunidades enteras alrededor del discurso del crédito fácil: algunos superan los 100.000 seguidores, sin verificación ni información clara sobre quién está detrás de ellos.

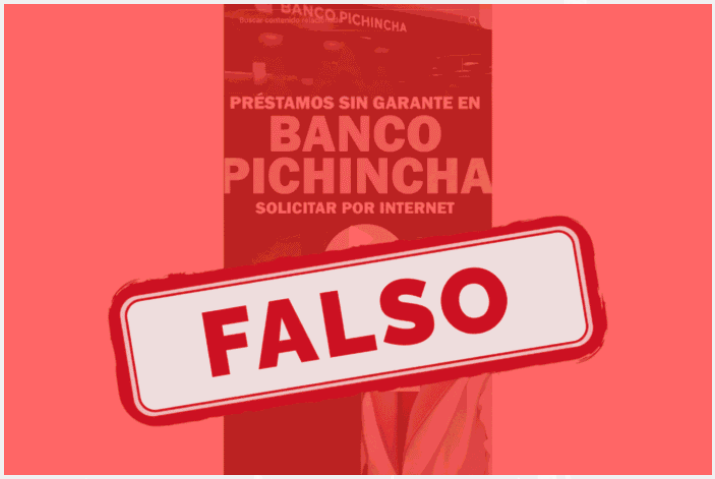
En sus biografías abundan las palabras "créditos", "dinero rápido", "préstamos sin buró" y números de teléfono que redirigen a WhatsApp.

Varias publicaciones replican diseños y tipografías que imitan a medios de comunicación, una estrategia que suma un barniz de credibilidad y convence a quienes buscan una alternativa financiera inmediata.

Lee la investigación completa aquí:
https://ecuadorchequea.com/las-estafas-digitales-tambien-llegan-con-la-desinformacion/

OTROS EJEM-PLOS

Una falsa oferta de créditos del Banco Pichincha circuló en TikTok. Ecuador Chequea verificó que el banco no difundió ese producto en sus canales oficiales y que las condiciones del supuesto crédito no coincidían con las reales.



También se verificaron falsas vacantes del mismo banco y del Banco de Guayaquil, mostrando cómo estas ofertas falsas operan en TikTok y otras redes sociales.



Este caso es útil para ilustrar que las estafas digitales a menudo llegan como oportunidades atractivas, no como amenazas directas.

¿Cómo se verifica?

Ecuador Chequea recomienda estos pasos:

1. **Contrastar con fuentes oficiales:** revisar el sitio web del banco o el LinkedIn corporativo.
2. **Analizar el enlace:** mirar la URL antes de hacer clic y desconfiar de dominios sospechosos.
3. **Buscar señales de legitimidad:** publicaciones con sueldos, créditos o beneficios que no aparecen en canales institucionales son sospechosas.
4. **Búsqueda inversa de imágenes:** detectar si el material visual circula en otros contextos o ha sido reutilizado.

Herramientas útiles

[Whois Lookup]

[Google Safe Browsing]



Safe Browsing
Google

[Google Imágenes]

Google
Images

Protegerte también es aprender a desconfiar con criterio

Reconocer estafas digitales no significa vivir con miedo, sino desarrollar hábitos simples para moverse con más seguridad en internet. Hacer una pausa, revisar la fuente, no compartir datos sensibles y confirmar antes de pagar son acciones pequeñas que pueden prevenir problemas mayores.

La protección digital no depende de saberlo todo, sino de actuar con calma cuando algo parece extraño, demasiado urgente o demasiado conveniente.



Una pregunta útil antes de responder

Frente a un mensaje inesperado, una llamada sospechosa o una oferta que parece irresistible, conviene hacerse una pregunta sencilla:

¿esta persona o institución realmente necesita que actúe así, tan rápido y por este canal?

Esa duda puede abrir el espacio necesario para verificar y evitar el engaño.

ECUADOR Chequea
PERIODISMO CON RIGOR

ChequeaLab

EN INTERNET, PROTEGERSE NO SIEMPRE CONSISTE EN BLOQUEARLO TODO, SINO EN APRENDER A RECONOCER CUÁNDO ALGO NO ENCAJA. ESA ATENCIÓN PUEDE HACER UNA GRAN DIFERENCIA.



Quito - Ecuador
2026