

TikTok no se libra de las estafas: aprende a esquivarlas

La red social favorita de los jóvenes eliminó 73 millones de cuentas falsas el año pasado. **«Los usuarios bajan la guardia porque solo buscan entretenerse»**

JOSÉ CARLOS CASTILLO



«Muchos no distinguen bien entre contenido orgánico, publicidad encubierta, afiliación comercial o recomendación interesada»

Pensar en adolescentes y redes sociales es hacerlo en TikTok, una plataforma que ya supera los 1.000 millones de usuarios activos mensuales a nivel global. Se trata además del espacio digital preferido por los menores de 18 años en nuestro país, lo que llama irremediablemente la atención de los ciberdelincuentes. El último informe publicado por el banco digital Revolut así lo demuestra: recoge cómo en 2025 el porcentaje de estafas originadas en esta aplicación se multiplicó por seis de un año para otro.

Los responsables de la red social tampoco se esconden. Según reporta la firma de análisis Statista, 73 millones de cuentas falsas (creadas con propósitos engañosos) fueron eliminadas durante el primer trimestre del año pasado. ¿Qué es lo que les gusta a los estafadores de esta red social? «Además de su capacidad de alcance —explica Fernando Checa, profesor del Máster en Redes Sociales de la Universidad Internacional de La Rioja (UNIR)—, TikTok alberga elementos atractivos para el fraude como un consumo rápido y una relación muy emocional con el contenido». Los usuarios «bajan la guardia porque no sienten que estén 'buscando' algo peligroso, sino simplemente entreteniéndose. El video breve permite generar confianza muy deprisa: cara, voz, promesas directas y llamada a la acción. Para el ciberdelincuente, eso es lo más sencillo», continúa el experto.

Sorteos y criptomonedas

No extraña entonces que sólo en Estados Unidos las pérdidas por fraude vinculadas a redes sociales ascendiesen a más de 2.100 millones de dólares en 2025, señala Checa. ¿Y de qué artimañas hablamos? «Las más habituales en TikTok son los falsos sorteos, las promociones de productos milagro, las suplantaciones de influencers o empresas y las falsas inversiones, especialmente en criptomonedas o supuestas plataformas de 'trading'».

A estas se suman los engaños ligados a TikTok Shop, el apartado de compras de la aplicación, donde abundan las tiendas que suplantán a marcas legítimas: «Los malhechores digitales utilizan videos cada vez mejor editados, testimonios falsos, comentarios comprados, perfiles clonados y, lo que es aún más peligroso, páginas de pago convincentes. El fraude se parece cada vez más a una acción de marketing profesional, pero sin producto ni empresa real detrás», alerta el docente.

En esta amalgama de engaños, los menores resultan especialmente vulnerables al mezclarse socialización, identidad y consumo en un mismo espacio, prosigue Checa. «Les afectan los fraudes económicos, pero también la exposición a desconocidos, la presión de grupo, los retos peligrosos, el cibercoso, la manipulación emocional y la sobreexposición de datos personales. Muchos no distinguen bien entre contenido orgánico, publicidad encubierta, afiliación comercial o recomendación interesada». Sobre esto, TikTok ha introducido configuraciones específicas para adolescentes, como cuentas privadas por defecto en determinadas franjas de edad y restricciones de interacción, pero los especialistas en ciberseguridad advierten: no sus-

El modo 'seguro' de detectar tiendas falsas

Una investigación de la firma CTM360 cifró en más de 10.000 el número de tiendas falsas en Facebook y TikTok, motivo por el que el experto en ciberseguridad Tomás Sierra pide tomar precauciones específicas antes de sacar la tarjeta de crédito. «Debemos desconfiar de los precios increíblemente bajos respecto a otras tiendas; las páginas con errores ortográficos o gramaticales; las imágenes de baja calidad y la falta de información detallada sobre la política de devoluciones», señala. Por esto mismo, se aconseja buscar el nombre de la tienda en Google (seguido de palabras como 'estafa' o 'fraude') y pagar únicamente con métodos que ofrezcan garantías, evitando las transferencias.

tituyen en ningún caso al acompañamiento de los adultos, quienes tienen la responsabilidad de alfabetizar a sus hijos en el mundo digital.

La inutilidad del algoritmo

Podría pensarse que el algoritmo de TikTok (las instrucciones que determinan qué contenidos se muestran a qué perfiles de usuarios) rema en contra de las estafas, ocultando aquellas publicaciones mínimamente sospechosas, pero el experto de la UNIR expone una realidad bien distinta: «Si un video engañoso consigue retención, comentarios, compartidos o curiosidad inicial, puede encontrar públicos similares antes de que la plataforma lo detecte. Ahí está el problema, puesto que las estafas están diseñadas para explotar señales de 'engagement'».

Por fortuna, existen pistas para identificar los videos malintencionados. Checa pide desconfiar de aquellos que denoten urgencia ('solo hoy', 'últimas plazas'), desproporción («premios enormes, descuentos absurdos o rentabilidades garantizadas») o intenten sacarnos de la aplicación mediante «páginas web extrañas, con formularios en los que a menudo se solicitan datos personales».

La configuración ideal

Desde el Instituto Nacional de Ciberseguridad (Incibe) se ofrecen además algunos ajustes destinados a blindar la experiencia de usuario en TikTok. «Una de las configuraciones de privacidad más importantes es establecer tu cuenta como privada (solo las personas que apruebes podrán seguirte y ver tus videos), además de comprobar que todas las opciones del apartado 'verificación de seguridad' (dentro de 'Seguridad y permisos') se encuentran en verde».

Por su parte, Checa recomienda «revisar quién puede comentar, reutilizar o descargar nuestras publicaciones, hacer dúos y enviarnos mensajes». También «desactivar la sugerencia automática de la cuenta a contactos, limitar la visibilidad de la lista de seguidores y consultar los permisos de sincronización de agenda». Finalmente, en el caso de los menores, no está de más activar las opciones modo restringido, tiempo de pantalla y, cuando proceda, sincronización familiar.

ADOBE STOCK