Desde este **viernes 28 de noviembre** se realizará una nueva edición del **Black Friday**, instancia en la que **más de 460 marcas participarán con promociones y descuentos** en diversos productos.

Al respecto, **el volumen de ofertas suele aumentar considerablemente** durante estos días, lo que eleva también la atención y el tráfico de usuarios. Y en ese escenario**, las posibilidades de encontrarse con intentos de estafa también crecen**, especialmente a través de enlaces, anuncios o mensajes que buscan aprovechar la rapidez con que muchas personas toman decisiones de compra.

Por eso, es clave considerar ciertas **precauciones básicas antes de revisar cualquier promoción**. Para ello, el experto en Ciberseguridad y académico de la Universidad de los Andes (Uandes), **Claudio Álvarez**, entrega recomendaciones para evitar caer en estafas durante el Black Friday. Estas son:

- "**Acceder siempre desde los portales oficiales del evento**, publicados por la Cámara de Comercio de Santiago. Evitar enlaces recibidos por WhatsApp, SMS, correos o redes sociales, especialmente si conducen a dominios desconocidos o con faltas ortográficas.
- **Revisar que la URL del comercio sea la auténtica**: dominio correcto, HTTPS activado, candado de seguridad, y certificados que calcen con la marca. Muchos sitios fraudulentos usan variaciones mínimas del nombre.
- **Nunca entregar datos bancarios, claves o coordenadas en páginas que no sean el sitio del banco**. Los comercios reales solo redirigen a WebPay u otras pasarelas oficiales; ninguno debe pedir claves personales del banco.
- **Desconfiar de ofertas 'demasiado buenas para ser verdad'**. En estos eventos aparecen descuentos altos, pero muy pocas veces bajan de forma extrema. Por ejemplo: 80% o 90% en productos caros.
- **Verificar que exista un servicio de atención al cliente legítimo, con teléfono, RUT y dirección comercial verificable**. Las tiendas reales tienen presencia pública, redes sociales activas y reclamos respondidos.
- **Revisar si el comercio está inscrito en el listado oficial del evento**. Si no aparece ahí, se debe asumir como riesgo elevado.
- **Evitar pagar por transferencias directas a cuentas personales**. Preferir WebPay, tarjetas de crédito o débito, o billeteras digitales reconocidas, pues permiten reversos y reclamos formales.
- **Mantener actualizado el navegador, el sistema operativo y los sistemas de**

protección. Muchos fraudes se aprovechan de vulnerabilidades de software desactualizado.

Buscar señales de *red flags*: faltas ortográficas en el sitio, imágenes pixeladas, políticas de devolución confusas, precios sin coincidencia con el resto del mercado, o presión excesiva del tipo ‘últimas unidades’ o ‘solo queda uno’”.

y tú, ¿qué opinas?