Diario Maule Hoy
Uniendo la Región

Fecha: 31/05/2025 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $0 Tirada: 0 Frecuencia: DIARIO
Vpe pág: $0 Difusión: 0
Vpe portada: $0 Ocupación: 55,76%

No todo lo que brilla es cyber:

Sernac entrega recomendaciones para evitar estafas durante este evento

Existen distintos tipos de fraudes que incluyen desde robo de datos personales, hasta instalación de virus maliciosos en los dispositivos.

Quedan pocos días para que se desarrolle uno de los eventos digitales de ofertas más esperados por las y los consumidores, sobre todo para adquirir esos productos de más elevado precio.

Desde el 2 al 4 de junio se realizará el **CyberDay 2025**, que contará con la participación de casi 700 marcas, lo que generará un alto volumen de transacciones y un intenso tráfico en línea.

Por esta razón, es fundamental que las y los consumidores extremen las precauciones para evitar caer en delitos informáticos y diversos tipos de fraude, ya que los delincuentes se aprovechan de la confianza en grandes marcas, la urgencia para conseguir una oferta y la dificultad para detectar falsificaciones.

TIPOS DE FRAUDE

1. Phishing / Smishing

Fraudes por correo, SMS o WhatsApp que simulan ser bancos, tiendas o incluso el propio evento CyberDay. Buscan engañar al usuario para que entregue datos sensibles, como claves, contraseñas o datos de tarjetas. Estos mensajes suelen ofrecer promociones atractivas e incluyen enlaces maliciosos que redirigen a páginas falsas que imitan sitios oficiales.

Una vez que la persona ingresa sus datos, los delincuentes los capturan para robar fondos, realizar compras o suplantar identidad.

2. Sitios web clonados («Spoofed Sites»)

Páginas espejos o falsas que imitan a tiendas reales usando dominios parecidos. Replican el diseño, logotipos y hasta los banners del Cyber para parecer legítimos. Cualquier pago o dato entregado va directo a los estafadores.

3. Ofertas fantasmas en redes sociales / Marketplaces

Publicaciones falsas difundidas en redes sociales o marketplaces no regulados que anuncian productos muy baratos que no existen o nunca serán entregados. Los estafadores desvían al comprador a WhatsApp o mensajes privados, donde solicitan pagos por transferencia sin ninguna protección. Para aumentar la credibilidad, a veces simulan envíos mediante falsos couriers, incluso entregando números de seguimiento fraudulentos

4. Card-not-present & «Carding»

Uso fraudulento de tarjetas en línea o teléfono, sin tenerlas físicamente. Esto es especialmente riesgoso, ya que no se verifica la identidad del titular. Los delincuentes prueban tarjetas robadas para hacer compras pequeñas, validar su funcionamiento y luego cometer fraudes mayores o vender los datos en mercados ilegales, lo que se conoce como «carding». Durante el Cyber estos delitos aumentan, ya que los estafadores aprovechan tiendas con baja seguridad o crean sitios falsos para realizar cargos fraudulentos.

5. Enlaces de seguimiento / delivery falsos

Mensajes que simulan seguimiento de envíos, que aparentan provenir de empresas de logística tras una compra (real o simulada). El consumidor recibe un correo, SMS o Whatsapp con un enlace malicioso, donde le piden datos bancarios, instalan virus o solicitan pagos falsos. Apuntan a robar claves, códigos de autenticación y controlar el dispositivo.

6. Publicidad engañosa y «ofertas que no eran tales»

Empresas que simulan descuentos inflando precios días antes del evento o que cancelan compras, alegando falta de stock. También se da esta práctica cuando envían productos que no coinciden con lo ofrecido o simplemente no se entrega, vulnerando los derechos del consumidor.

7. Quishing (QR Phishing)

Fraudes mediante códigos QR que redirige a sitios fraudulentos. Se presentan como cupones, promociones o seguimientos y los difunden a través de afiches, volantes, RRSS o correos. Al escanearlos, se accede a páginas falsas que pueden robar datos o instalar virus maliciosos, sin que el usuario vea la URL real.

8. Aplicaciones falsas

Aplicaciones falsas con programas maliciosos que imitan a las originales de bancos, tiendas o empresas de delivery para robar información personal. Se instalan desde links engañosos o tiendas no seguras, y piden permisos excesivos para robar datos personales, bancarios o infectar el celular con malwares que operan en segundo plano.

RECOMENDACIONES

Una vez conocido los principales tipos de fraude, es importante que cada consumidor pueda tomar todas las precauciones posibles.

En primer lugar, es importante **verificar el sitio web** donde se está realizando la compra. Para este evento digital, todas las marcas estarán disponibles en **Cyber.cl. Se deben evitar utilizar enlaces recibidos a través de SMS, Whatsapp, correos electrónicos o redes sociales.**

En cuanto a la seguridad en los pagos, se recomienda usar tarjetas de crédito, tarjetas virtuales o plataformas reconocidas como WebPay, PayPal o MercadoPago, que ofrecen mayor protección ante fraudes. También es esencial activar la autenticación en dos pasos (2FA), no compartir datos bancarios por canales informales y revisar con frecuencia los movimientos de cuenta. Se desaconseja realizar transferencias directas a cuentas personales, ya que estas no cuentan con mecanismos de devolución en caso de estafa.

Se debe planificar el presupuesto antes del evento y evitar compras impulsivas. Es importante que cada consumidor lea los términos y condiciones

En caso de sospechas o fraudes, se debe contactar inmediatamente al banco y bloquear la tarjeta, cambiar contraseñas de los servicios afectados y realizar las denuncias correspondientes, ya sea a la PDI, al Ministerio Público o al SERNAC, a través de sus canales: SERNAC.cl, call center gratuito 800 700 100 u oficinas ubicadas en cada región.