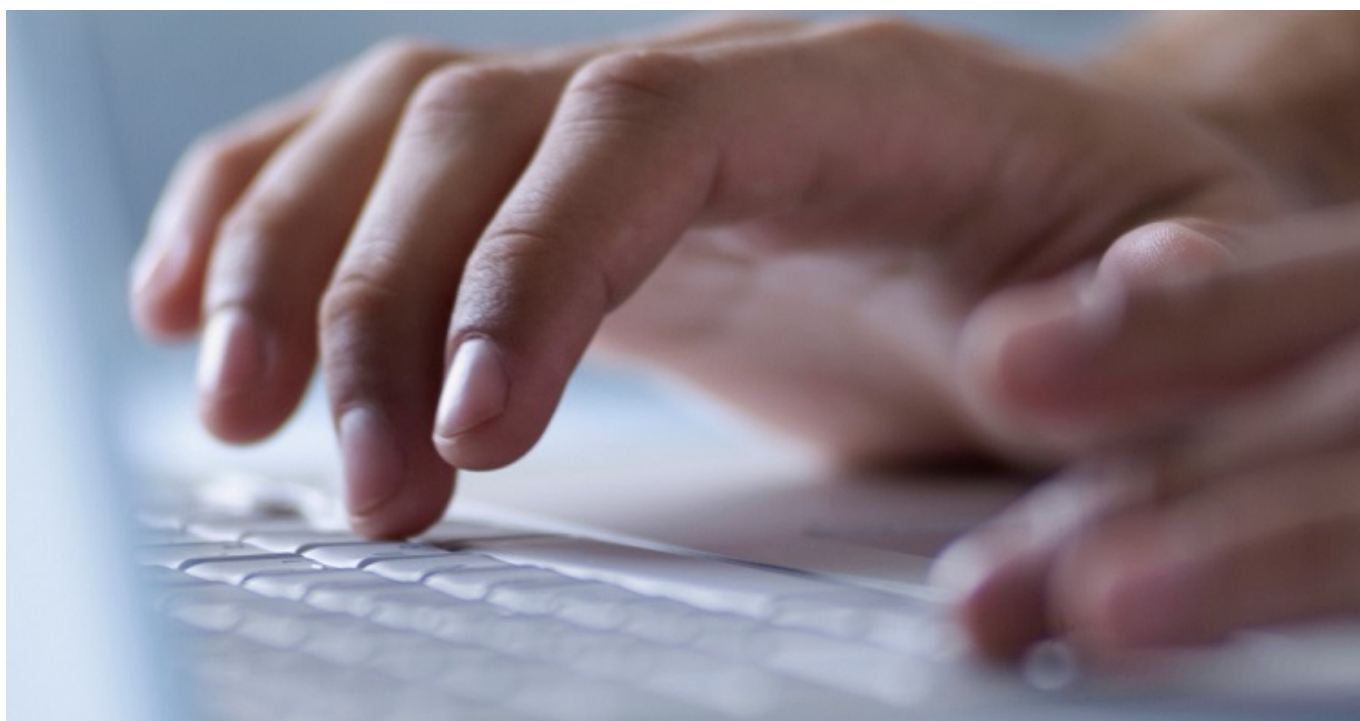


Aunque se extiende durante tres días, entre las 0 horas del lunes 04 de octubre hasta el miércoles 06 del mismo mes, uno de los eventos de ofertas digitales más importantes del comercio chileno lleva por nombre **CyberMonday**.

Iniciativa de la **Cámara de Comercio de Santiago (CCS)**, la jornada de compra online -que lleva más de diez versiones- cuenta en esta oportunidad con la participación de más de 700 marcas. La CCS destaca que las plataformas digitales de cada una de ellas tienen un **“Sello de Confianza”** que otorga «garantías en el proceso”.



El Comité de Comercio Electrónico de la CCS, instancia que coordina la jornada, destaca la existencia del Código de Buenas Prácticas para el Comercio Electrónico, bajo el cual las empresas que participan del evento son orientadas a atender a los clientes.

A ello, se suma el sistema “Resolución en Línea” que encauza reclamos al Centro de Arbitraje y Mediación de la CCS. La modalidad estuvo en fase de marcha blanca en la versión 2020 y en la actual ya está incorporada como práctica para los participantes oficiales. El objetivo de la mediación es actuar como un tercero que facilite la comunicación con la tienda, buscando alternativas de solución efectivas mediante un acuerdo.

En todo caso, los consumidores deben actuar con mucha prevención porque puede darse el hecho de que marcas participantes en Cyber Monday enfrenten paralelamente recursos interpuestos por el [Servicio Nacional del Consumidor \(Sernac\)](#) debido a incumplimientos a los términos de compra y venta en eventos digitales anteriores o por no ajustarse a Ley del Consumidor.

En ese sentido, no entregar información requerida por el Sernac y no comprobar que las ofertas promocionadas son mejores que tres meses antes del evento (según el compromiso que las empresas participantes asumen), son las principales razones por las que el servicio público genera denuncias que se incrementan cada año.



### **Confianza Cero**

Casi el 80% de las personas que compran productos o servicios en Chile se autocalifican como «compradores digitales», según indica un estudio de la CCS. Ante eso, hay que tener en cuenta que, de acuerdo a los datos del laboratorio estadounidense de análisis e inteligencia FortiGuard Labs, ya se registran más de dos mil millones de intentos de ciberataques durante el primer semestre del 2021 en

Chile.

Por su parte, el Panorama de Amenazas en América Latina 2021 de Kaspersky -empresa de ciberseguridad rusa- señala que los ciberataques en nuestro país aumentan en un 20% durante los primeros ocho meses de 2021, comparado con igual período anterior.

Y es que el contexto digital para las compras implica hoy riesgos que deben considerarse a la hora de cualquier gestión o transacción. En ese sentido, dos son las amenazas más recurrentes: el Phishing y el Scam.

El Phishing es un correo electrónico o mensaje al celular que da cuenta de promociones aparentemente muy buenas o comparte datos “urgentes” que deben ser aprovechados “rápidamente” con el objetivo de que se entregue información confidencial (como contraseñas) o llevar a la persona a una web maliciosa e instalarte un malware (virus). Todas estas modalidades pueden llegar por SMS (smishing) o llamadas telefónicas (vishing).

El Scam, en tanto, es una estafa en la que se engaña a un(a) usuari@ para que haga un pago o transferencia. Hay muchos tipos, siendo el más común el de suplantación de identidad; ahí el ciberdelincuente crea sitios web o cuentas de redes sociales falsas con ofertas y productos ficticios, de manera de acceder a datos bancarios.

Se trata de un método que ha evolucionado mucho, porque actualmente clona sitios web y también redes sociales a través de las cuales concreta publicidad engañosa y fraudes.

FortiGuard Labs precisa que muchos ejemplos de Scam hasta pagan por marketing y posicionamiento SEO de Google, para que el sitio malicioso aparezca en primer lugar en las búsquedas. También crea aplicaciones falsas que suben a Apple Store o Google Play.

Así, con toda esta información, el primer consejo general clave es revisar siempre con calma tanto los sitios web que ofrecen productos como las informaciones que llegan al correo electrónico, whatsapp o cualquier red social.

Debe validarse que los correos provengan de personas conocidas (aunque no sean cercanas) o del dominio web oficial de la tienda o empresa; que la oferta sea lógica y que lo solicitado para cualquier transacción de dinero realmente sea algo que se requiera.

Un aspecto útil es que antes de dar el click, pasar el mouse por encima del link y revisar que lleve a un

sitio oficial y cifrado con https.

La base es actuar con un eficaz grado de desconfianza y sentido común: no es normal ni lógico que se pidan contraseñas, números de tarjetas de crédito o códigos de seguridad; tampoco es seria -en un contexto general- una oferta que implique el 99% de descuento, ni menos computadores a un dólar.

Los expertos dicen que es necesario aplicar un total modelo «zero trust» (“confianza cero”).

### **Aspectos clave**

Para que los consumidores pongan atención en las operaciones que van a hacer a través de los diversos sitios web participantes, ocho son los principales aspectos que se deben considerar:

- 1. Las ofertas deben ser verdaderas**, es decir, explicar claramente el porcentaje de descuento del producto para el CyberDay respecto del valor normal.
- 2. Medios de pago:** las empresas deben informar los medios de pago aceptados, y las condiciones, plazos, costos y cobertura geográfica de despacho de los productos.
- 3. Información clara y oportuna sobre los datos de contactos de las empresas.**
- 4. Precio:** es importante que las empresas informen el precio final del producto en pesos (que incluyan las tasas e impuestos), y que éste sea respetado.



**5. Información sobre el stock de productos sujetos a la oferta:** los consumidores tienen derecho a conocer el número de unidades de cada producto que se encuentran disponibles para ser adquiridos.

**6. Información clara y oportuna sobre los descuentos:** se deben señalar los **porcentajes de descuentos** que se ofrecerán y sobre qué productos se aplicarán.

**8. Exclusiones o limitaciones:** se debe informar a los consumidores acerca de determinadas marcas de productos que pudiesen estar excluidas de las ofertas, como también si es que existe alguna limitación en la cantidad de productos que puede adquirir un consumidor.