LEGÁLITAS

La otra cara del Black Friday: estafas y delitos online

- **Las prácticas más repetidas son el timo en la compra o venta de objetos de segunda mano que nunca llegan, la creación de tiendas online falsas mediante plataformas digitales seguras o el ofrecimiento de cupones de descuento falsos que suelen contener malwares**

- **Se deberá sospechar de aquellos mensajes, enlaces o avisos recibidos en cualquier dispositivo electrónico o por email donde se pida información personal sin haber realizado nada que requiera dar dicha información**

Madrid, 17 de noviembre de 2022.- Numerosos son los usuarios que aprovechan los descuentos del Black Friday para adquirir determinados productos o incluso realizar las compras navideñas. Sin embargo, esta época puede ser igualmente utilizada por ciberdelincuentes para cometer sus fechorías y hacer que los consumidores “piquen” en ofertas que solo conducen al robo de datos o, en el peor de los casos, al acceso a cuentas bancarias.

Desde Legálitas hacemos un repaso de los riesgos de hacer compras online, independientemente de si es Black Friday o no, de las ciberestafas más comunes o de los procedimientos a seguir en caso de ser víctima de este tipo de prácticas.

Riesgos de hacer compras online

Los principales riesgos al realizar compras online se pueden dividir en dos tipos: por un lado, los **incumplimientos por parte del vendedor** (no entrega el producto, el artículo que llega no es lo que se ha comprado, comunicación de falta de stock tras la compra del producto o la no devolución del importe tras haber desistido de la operación, entre otros) y, por otro lado, la posibilidad de ser **víctimas de estafas**

debido a la compra a través de una web pirata o la suplantación de identidad para realizar compras no autorizadas.

Datos legales al realizar una compra a través de Internet

Siempre que se esté navegando por una página web segura, lo legal y normal es que se pidan **datos de carácter personal** como puede ser el nombre y apellidos, DNI o la dirección postal en orden al envío de la mercancía. En cuanto a los **medios de pago** y en atención a las distintas formas de pago que puede ofrecer el vendedor, lo más habitual será el número de tarjeta de crédito o débito, su fecha de caducidad y el Código de Valor de Validación (CVV). No obstante, al realizar el pago la entidad emisora de la tarjeta deberá enviar un mensaje para proceder a confirmar la operación de acuerdo con las disposiciones normativas actualmente vigentes.

Por lo general, se debe sospechar de mensajes, enlaces o avisos de cualquier tipo que se puedan recibir en los distintos dispositivos electrónicos o por email donde se pida información personal sin haber realizado nada que requiera dar dicha información. Esto se debe a que, detrás de ello, se puede esconder una estafa o fraude.

Plataforma de pago segura: qué debe contener

Las plataformas de pago seguras se caracterizan por pedir una **doble autentificación** en lo que a la confirmación del pago se refiere. Por su parte, la entidad bancaria pedirá al usuario la confirmación mediante algún tipo de código o clave que solo él puede conocer.

Estafas más comunes en las compras online

Algunas de las prácticas que se repiten con mayor frecuencia son, entre otras, el timo en la compraventa de objetos de segunda mano que nunca llegan, la creación de tiendas online falsas mediante plataformas digitales seguras, el ofrecimiento de cupones de descuento que suelen contener malwares o inversiones en criptomonedas que en realidad son estafas piramidales en las que, para recuperar el dinero invertido, la víctima debe realizar cada vez más aportaciones.

Pero, sin duda, hay que considerar como las más comunes el phishing o el smishing. El **phishing** consiste en la recepción de correos electrónicos de entidades bancarias o instituciones supuestamente legítimas en los que se solicitan datos personales, claves y contraseñas de acceso a cuentas bancarias electrónicas. Todo ello con el fin de conseguir la mayor información posible para utilizarla a posteriori de manera fraudulenta. Y el **smishing** se caracteriza por el envío de un mensaje o SMS por parte de una entidad fiable para robar información o realizar cargos al número de cuenta del usuario.

Cómo distinguir una publicidad “real” de phishing

La publicidad recibida, en ocasiones, no es de quien aparenta ser, sino que se trata de una suplantación de una marca conocida ofreciendo, generalmente, **ofertas muy tentadoras** y dando poco tiempo para acceder a ellas. El Black Friday es una ocasión perfecta con la que los ciberdelincuentes tratan de conseguir que se les facilite información personal o financiera y todas las contraseñas.

Como consejo general, se deberá desconfiar de las promociones que parezcan demasiado buenas para ser verdad y, sobre todo, cuando presionan para que la compra sea inmediata. Por otro lado, es importante **fijarse en el remitente** ya que, aunque la dirección de email o enlace al que se deriva sea muy parecido al de una empresa o marca de confianza, hay una serie de aspectos que delatan su falsedad como la extensión o dominio. Lo mismo ocurre con los mensajes de texto que incitan a clicar en un vínculo para realizar una compra o introducir datos en un formulario.

En estos casos, es importante verificar cuidadosamente que dicho vínculo pertenece realmente a la empresa que dice enviarlo y visitar su página web oficial a través del navegador que se usa normalmente. Siguiendo estos pasos se evitarán los objetivos de estas acciones: generar una falsa sensación de seguridad y tener acceso a las cuentas bancarias, correo electrónico o descargar archivos maliciosos en los ordenadores o dispositivos.

Qué hacer en caso de ser víctima de una estafa online

Legálitas recomienda, en primer lugar, **hacer acopio de pruebas de cargo** como, por ejemplo, capturas de pantalla en las que se vea todo lo ocurrido: desde el anuncio publicado en algún portal o página web, hasta los mensajes intercambiados con el presunto estafador. Asimismo, es muy importante solicitar datos a la entidad bancaria sobre la cuenta de destino a la que se le envió el dinero en el caso haber realizado alguna transferencia o pago por Bizum. Cuanta más información se aporte junto a la denuncia de los hechos, mayores serán las posibilidades de demostrar la comisión del delito de fraude, así como averiguar la identidad del culpable.

Una vez reunidas todas las pruebas, se deberá acudir a la comisaría de Policía Nacional oportuna, a la Guardia Civil o al Juzgado de Instrucción de Guardia, e interponer la correspondiente denuncia para que, de esta forma, se inicie una investigación policial. Una vez localizado y detenido el culpable será el juez de instrucción competente quien determine si se está ante un **delito de estafa leve, menos grave o grave**. Entendiendo por leve aquel delito en el que el importe defraudado no supere los cuatrocientos euros; y por delito menos grave o grave aquel en el que se supere dicho límite. En cualquier caso, la víctima tiene derecho a reclamar la devolución del importe total y todos los daños y perjuicios sufridos.

Consejos o recomendaciones para evitar fraudes o timos en la red

LEGÁLITAS

Al navegar por Internet es importante tener en consideración las siguientes cuestiones:

1. Evitar todo **enlace sospechoso** que provenga de una dirección desconocida.
2. Obviar el **acceso a sitios web de dudosa reputación** que se promocionen con ofrecimientos gratuitos, descuentos en la compra de determinados productos, etc., así como ingresar cualquier tipo de información personal en páginas web con estas características.
3. Usar **tecnologías de seguridad** (antivirus, firewall o antispam) y mantener actualizado tanto el sistema operativo como las aplicaciones web para así disponer de los últimos parches de seguridad.
4. Descargar programas y aplicaciones desde **sitios web oficiales**.
5. Aceptar únicamente **contactos conocidos** en la interacción en redes sociales y sistemas de mensajería instantánea.
6. No ejecutar **archivos sospechosos** de cuya procedencia no se esté completamente seguro.
7. Utilizar **contraseñas fuertes** que integren números y caracteres y que no resulten fácilmente deducibles.
8. Desconfiar de **precios sorprendentemente bajos** en comparación con la media del mercado.

Para más información, contactar con David Jiménez, director de Comunicación.
Mail: comunicacion@legalitas.es | T. 91 771 26 16
Avenida de Leopoldo Calvo-Sotelo Bustelo, 6 - 1º. 28224 Pozuelo de Alarcón (Madrid)