Guía de recomendaciones para compras seguras por Internet

primero la gente

Secretaría de Innovación Tecnológica del Sector Público

Jefatura de Gabinete de Ministros Argentina

Guía de recomendaciones para compras seguras por Internet

La creación de la Web en 1990 y la apertura pública de Internet en 1995 por parte del gobierno de los Estados Unidos dio inicio a la etapa de la Internet comercial, donde el sector privado -bancos y empresas- comienzan a invertir en el desarrollo de plataformas tecnológicas para el desarrollo de la modalidad de negocios del siglo XXI: el comercio electrónico. Con el objetivo de poder realizar transacciones monetarias en línea, comenzaron a aparecer sitios de compraventa de productos y servicios, sistemas de pago electrónico y la banca por internet, lo que dio origen a una economía digital.

Pese a los beneficios que ofrece esta práctica por la variedad de la oferta, comodidad de uso y fácil acceso a un amplio catálogo de productos y servicios, aún existen usuarios en la red recelosos de volcar en determinados sitios datos filiatorios -dirección, teléfono, etc.- o de tarjeta de crédito y/o cuenta bancaria. Asimismo existe desconfianza acerca de si el sitio donde se va a realizar la operación es seguro y dice ser quien es.

Para ello, existen una serie de recomendaciones que un usuario tiene que tener en cuenta a la hora de realizar una compra por Internet.

Básicamente existen tres niveles de seguridad:

1. **La seguridad del dispositivo – computadora, tablet o celular - desde donde se va a realizar la compra.**
2. **La seguridad que ofrece el sitio web donde se va a realizar la transacción.**
3. **La reputación de la empresa que se encuentra detrás de la tienda en línea.**

En cuanto a la **seguridad del dispositivo**, lo primero que se recomienda realizar es la operación con un dispositivo personal y con una conexión a Internet propia. No se recomienda hacer una operación financiera desde lugares públicos utilizando redes abiertas, tampoco en dispositivos de terceros donde no sabemos qué tipo de programa o aplicación puede haber instalado en la misma. Por ejemplo puede haber o software espía que se encargue de registrar todo lo que tecleamos mecánicamente en el dispositivo –llamado keylogger- y así registrar nuestros datos personales y financieros para posteriormente “robarnos” nuestra identidad en otros sitios web.

Otra cuestión a considerar es tener el sistema operativo actualizado. Esto para evitar lo que se denomina agujeros de seguridad, tanto en una computadora o tablet como en el celular. Si es Windows -el sistema operativo más utilizado- se actualiza automáticamente. También tener el firewall o cortafuegos activado -que viene incorporado al mismo- y es el que regula la información que entra y sale de la computadora. Tenemos que garantizarnos que se encuentre activado al momento de realizar la compra, ya que nos va a advertir si ingresamos a un sitio que no es seguro alertándonos como "sospechoso" por no cumplir con los estándares de seguridad adecuados y recomendándonos no ingresar a los mismos.

Lo segundo es tener el **antivirus actualizado**, con la base de datos de peligros y amenazas al día. Si bien generalmente estos programas se actualizan automáticamente, resulta adecuado asegurarse con una actualización manual para evitar el ingreso de software malicioso -virus o troyanos- encargados de recopilar números de tarjeta de crédito, datos de identificación personal etc, tanto así como de software espía. Una vez verificado esto, realizar un escaneo del equipo con el antivirus antes de realizar la compra del producto.

En cuanto a la **seguridad del sitio web** donde vamos a realizar la compra, tenemos dos formas de acceder: realizando una búsqueda por producto en el que estamos interesados o ingresando directamente a una tienda específica para navegar y elegirlo. Existen dos tipos de negocios para realizar compras en línea, las tiendas on line, que son de un negocio o una marca específica o los llamados sitios de subastas, que son empresas que brindan el espacio para que usuarios y otros negocios compren y vendan productos y servicios.

Lo primero que se debe asegurar es que la dirección web sea la correcta a la hora de ingresar. Hay muchas páginas falsas con direcciones muy similares a las originales que van a tratar de obtener nuestros datos personales para el robo de identidad, para realizar una operación financiera o cometer otros delitos a nuestro nombre.

La segunda cuestión es verificar que sea en un sitio seguro. Esto se idéntica -dependiendo del navegador que utilicemos- con un candadito en la barra de direcciones o en la barra de estatus. Si el mismo está cerrado significa que el navegador lo identifica como sitio seguro. Si está abierto esto indica que el certificado que presenta el sitio no es reconocido.

Los certificados de seguridad, además de indicar que los datos que se carguen en el sitio van a estar protegidos, indican que existe una autoridad de certificación reconocida que garantiza que el sitio es propiedad de la empresa u organización que dice ser. Los navegadores confían en que las autoridades de certificación -que pueden ser empresas u organizaciones prestigiosas- identifican el sitio como seguro.

Lo segundo que tenemos que ver es que la información que vamos a cargar en el sitio -número de tarjeta de crédito, número de cuenta bancaria, etc.- esté codificada, cifrada, lo que en términos de seguridad informática significa encriptada. De esta manera, la información que volquemos en el sitio sólo podrá ser leída por la persona que tiene "la llave" para leerla, en este caso la tienda. Esto se utiliza por si -en algún punto de la red- un hacker intercepta la información desde que viaja del cliente hasta el servidor que aloja el sitio no pueda acceder a esa información privada. Para identificar si un sitio protege la información que se transmite, al momento de realizar la operación financiera –no necesariamente cuando se ingresa al sitio- debe aparecer en la barra de direcciones del navegador el encabezado https, no http. Esto significa el protocolo de transferencia de hipertexto es **SEGURO**.

La mayoría de las tiendas en línea solicitan a los compradores suscribirse al sitio web mediante el uso de un usuario y contraseña. Estos sistemas requieren una dirección de mail, para lo que se recomienda abrir una gratuita para operar en estos sitios. También se pueden utilizar contraseñas largas, alfanuméricas, en las que es importante no utilizar las mismas que usamos en casillas de mails o redes sociales. Algunos sitios web solicitan otra información tales como nombre y apellido, dirección postal para la entrega a domicilio de un producto y datos de tarjeta o cuenta bancaria al momento de realizar la operación. Si solicitan otros datos como preferencias o hobbies, señalando algunos de ellos de una lista hay que tener en consideración que esto es para formar parte de bases de datos para luego enviar publicidad a medida del usuario a través de correos no deseados o spam.

En términos financieros, se recomienda utilizar la tarjeta de crédito como método de pago más seguro. En muchos sitios de subastas, los usuarios pactan en forma de pago y el envío de un producto, esto no se recomienda –salvo que sea de mucha confianza el vendedor- no realizarlo mediante cheque o transferencia de dinero a una cuenta bancaria.

Muchos sitios de subastas no se hacen responsable de este tipo de cuestiones entre usuarios. Ellos dicen que solo brindan una plataforma tecnológica para la compraventa de productos, que son simplemente un intermediario. Aunque un fallo de la Corte Suprema de Justicia del año 2013 asigna responsabilidad solidaria a los sitios de subastas o venta de terceros en Argentina a partir de la publicación de un producto falso por parte de un usuario. En este sentido, al existir interés económico por parte de la empresa en la venta de ese producto, tiene una participación en la operación.

En cuanto a la reputación de la empresa con la que estamos operando -en caso de que no sea muy conocida- googlear, entrar a foros y leer comentarios sobre experiencias de usuarios, si salió alguna noticia reflejada en la web en relación al sitio web, buscar referencias para saber con quién se va a tratar, fundamentalmente si el negocio solo tiene presencia virtual. Si el comercio tiene presencia física y tiene venta online, averiguar la dirección y el teléfono de contrato, si tiene un centro de reclamos, etc.

Es importante -en la medida de lo posible- leer los términos y condiciones de uso para conocer cuál es la política de devoluciones y reembolsos de la empresa y el sistema de envíos de productos que utiliza, viendo qué responsabilidades tiene el sitio por si llega deteriorado o no llega a destino. Esto fundamentalmente para las tiendas en línea. En cuanto a los sitios de subastas, conocer qué nivel de responsabilidad tiene la empresa frente a la posibilidad de

fraude por parte del vendedor de un producto, un tercero y cuáles son los canales de denuncia frente a estafas.
También leer la política de privacidad de datos, es decir, para saber que va a hacer la empresa con nuestra información. Esto es relevante en tanto algunas empresas especifican en algunas cláusulas que el sitio es propietario de algunos datos que vuelca el usuario para usos comerciales. Esto implica que puedan vender a terceras empresas para usos de marketing y publicidad.

Por último, cuando terminemos de realizar compras por Internet, se aconseja eliminar los archivos basura que se instalan automáticamente en nuestra computadora cada vez que navegamos por la web. Hay programas gratuitos muy buenos que se pueden descargar de Internet para esto. Esto es importante para eliminar las cookies, unos pequeños archivos que se instalan de los sitios web automáticamente en nuestro disco rígido para identificarnos como usuarios del mismo y establecer nuestras preferencias dentro de éste. Una de las funciones que tiene es recordar nuestro nombre de usuario para que no tengamos que volver a cargarlo cuando volvamos a ingresar, por ejemplo, pero estos archivos son utilizados por muchos sitios para reportar también en forma automática nuestros hábitos de navegación y enviar publicidad a medida, en esos mismos sitios web o mediante el envío de correos no deseados con publicidad.