Protección de datos y compras a través de internet

Recomendaciones de seguridad para las comprar a través de internet y descripción de los principales aspectos relacionados con el tratamiento de los datos personales en el uso de internet.

Dado que el Consejo para la Transparencia, a partir de la modernización de la ley de protección de datos personales se transformará en el órgano garante del cumplimiento de la normativa, se entregan una serie de recomendaciones que apuntan a salvaguardar la seguridad y control de los datos que los usuarios entregarán vía canales de venta electrónicos, con el fin de evitar que sean utilizados sin autorización o con finalidades distintas para los que la información fue otorgada, o ser víctimas de delitos informáticos

1. **Cada vez que le soliciten registrar sus datos en una tienda online o un proceso de compra, revise la política de privacidad de dicho sitio web.** Esto le permitirá conocer en qué consiste la autorización que está otorgando para el tratamiento de su información personal, lo que comprende la forma cómo sus datos serán almacenados, gestionados y, eventualmente, transmitidos o cedidos a terceros.

2. **Ingrese sólo a sitios web que permitan identificar claramente la tienda de comercio electrónico de que se trate, y que empleen protocolos de seguridad "https".** Esta sigla se refiere al "protocolo seguro de transferencia de hipertexto", que constituye una manera más segura de acceder a los contenidos de Internet, ya que cualquier dato o información que sea introducido al sitio web será cifrado, restringiendo de esta forma la posibilidad de que pueda ser interceptado por terceros no autorizados.

3. **En el caso de las "apps para compras online" o tiendas online que disponen de aplicaciones descargables en teléfonos inteligentes o tablets, los usuarios dueños de los dispositivos deben asegurarse de emplear la aplicación oficial del respectivo proveedor y además de proteger el acceso a ellas.** Esta acción apunta a evitar que personas sin su autorización puedan usarlas y efectuar compras en su nombre. Una recomendación que puede resultar crítica, dado que los usuarios de dispositivos móviles mantienen, por lo general, configuradas estas apps con sus datos personales y bancarios. Con este antecedente en cuenta es recomendable el empleo de medidas de seguridad especiales como son las "app lockers".

4. **Prefiera las tiendas online que empleen mecanismos de seguridad de "doble verificación",** esto es, que soliciten al momento de ingresar al sitio web o durante el proceso de compra, además de la contraseña, un código adicional. Lo anterior vuelve más complejo que un usuario no autorizado pueda acceder a la cuenta y/o concretar una transacción. Este código generalmente es enviado a un canal al que sólo tiene acceso el titular de la cuenta, a través de mensajería SMS, llamadas telefónicas o una llave de seguridad.

5. **Prefiera equipos con medidas de protección adecuadas y cuyos sistemas operativos cuenten con las últimas actualizaciones, evitando ingreso a sitios web mediante redes de Internet públicas sujetas a mayores riesgos y amenazas de seguridad.** Asegúrese de que el computador, teléfono inteligente o Tablet mediante el cual visitará las páginas de las tiendas o comercios tengan antivirus, firewall y antispyware. De esta forma se garantiza la incorporación de las más recientes medidas de seguridad desarrolladas por el proveedor del software, junto con corregir fallos técnicos y otras vulnerabilidades.

6. **Digite directamente su dirección o URL en el navegador de Internet.** Esto cobra especial relevancia en aquellos casos en que quiera acceder a páginas web que requieren el registro de sus datos personales. Se sugiere evitar el ingreso a los sitios de interés a través de hipervínculos contenidos en otras páginas web o en correos electrónicos. De esta forma puede prevenir el acceso a portales falsos que simulan ser las páginas oficiales de empresas, bancos o medios de pago digitales.

7. **Utilice contraseñas complejas y únicas para cada tienda online donde mantenga una cuenta de usuario, especialmente respecto de servicios más sensibles, como los bancarios o de medios de pago.** De esta forma, sus claves serán menos vulnerables a eventuales intentos de hacking o cracking. Se recomienda la utilización de gestores de contraseñas, que permiten la generación automática de claves complejas para acceder a distintos recursos.

8. **En caso de registrarse en un sitio web o de comunicar en una determinada transacción información sobre sus cuentas bancarias o tarjetas de crédito, tenga la precaución de revisar con regularidad los estados de cuenta de sus tarjetas en días posteriores,** con el objeto de detectar cargos sospechosos o no autorizados, que podrían estar vinculados a la utilización fraudulenta de la numeración de una tarjeta de crédito válida.

9. **Cookies.** Por intermedio de los cookies de Internet, todo el historial de navegación va quedando registrado y guardado en la red. Las páginas web y las aplicaciones usan esta información, lo que posteriormente permite, entre otras cosas, efectuar publicidad dirigida directamente al usuario, en base a los sitios electrónicos que han sido visitados con más frecuencia.

   En muchas de los sitios de internet a los que se accede por primera vez, despliegan un mensaje de autorización de cookies. Esta es una exigencia para aquellos sitios que se alojen en Europa por las estrictas reglas de protección de datos personales. Sin embargo, no es una obligación general aplicable a todos los países.

   Al aceptar o autorizar el uso de cookies, estamos permitiendo que la información de navegación pueda ser empleada para poder hacer tratamientos de datos como perfiles de usuarios y publicidad personalizada.

Una forma de evitarlo es a través de la navegación anónima que algunos softwares admiten. Si bien esto puede resultar complejo de evitarse, es conveniente tomar conciencia de toda la información personal que se está entregando al navegar por Internet, aunque de manera expresa no proporcionemos ningún dato.