Medidas de seguridad

a la hora realizar compras online

acens .com
the hosting company

Calle San Rafael, 14
28108 Alcobendas (Madrid)
902 90 10 20
www.acens.com

En los tiempos que nos movemos, las compras online han adquirido un peso muy importante en la sociedad. Hoy en día muchos usuarios se decantan por adquirir ciertos productos por medio de Internet en vez de acudir a una tienda física. Este aumento de las compras online es debido en parte a la comodidad de poder adquirir cualquier producto desde cualquier sitio sin desplazarse, además de que por lo general los precios de los productos que encontramos por la red suelen ser menores que los de cualquier establecimiento.

Pero este aumento de las ventas online también ha llevado consigo un aumento de la ciberdelincuencia, ya que nos podemos encontrar muchas aplicaciones que utilizan las ventas virtuales para estafar a los consumidores.

A lo largo de este White Paper iremos viendo las principales medidas de seguridad que deben tener presente los usuarios a la hora de realizar sus compras por la red.

Verificar que se utiliza el protocolo HTTPS

Una de las principales medidas que debemos tener presente a la hora de realizar las compras virtuales, es verificar que la página donde estamos realizando la compra esté utilizando el protocolo HTTPS.

Normalmente las páginas webs utilizan el protocolo HTTP (sin la 'S' final), donde la información que se maneja no va encriptada. Pero en las tiendas online se maneja información privada del usuario, como puede ser sus datos bancarios o sus datos personales, por lo que es imprescindible que la información se encripte para mayor seguridad.

El protocolo HTTPS cifra la información que se envía por la aplicación mediante un certificado de seguridad que hay instalado a nivel del dominio. Con esto el usuario se asegura de que la información que mande no pueda ser legible para ningún hacker, a no ser que consiga la clave de desencriptación (algo muy difícil de conseguir).

En las páginas que utilizan el protocolo HTTPS normalmente aparece el icono de un candado en el navegador. Este icono nos está indicando que el sitio es fiable y que los datos están encriptados. Pinchando en el candado obtienes el informe de seguridad de esa página. Hay casos en que la página está cifrada pero no aparece el candado, y algunas páginas ponen el candado y realmente no estén encriptadas. Lo mejor es

que mires en las opciones de seguridad de tu navegador para obtener la información de seguridad real de la página, cosa que también puedes conseguir si pinchas en el icono que aparece a la izquierda de donde escribes las direcciones web en tu navegador.

Mantener actualizado nuestro equipo

Cuando hablamos de actualizar el equipo no sólo hay que centrarse en el sistema operativo que utilicemos, sino en cualquier otro software que tengamos instalado, como pueden ser antivirus, antispam, Java...

Manteniendo aplicaciones desactualizadas, estamos dejando puertas abiertas para que los hackers puedan entrar en nuestros equipos, de ahí la importancia de actualizar siempre que salga una nueva versión.

Evitar realizar compras desde conexiones no seguras

En la sociedad en la que nos movemos es normal que en sitios como pueden ser bares, hoteles o centros públicos, uno se pueda conectar a la red desde sus dispositivos. Muchos pueden aprovechar para realizar alguna compra que necesite, pero esto puede ser un gran riesgo.

Por lo general este tipo de conexiones están abiertas, sin ningún sistema de encriptación, con lo que

cualquier hacker puede estar conectado y atacar a cualquier dispositivo que se conecte desde esa red, y así poder robarle su información.

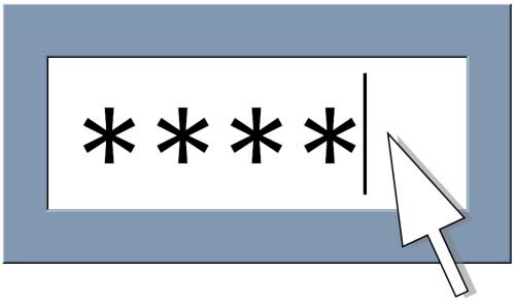
Si te conectas desde uno de estos sitios, es muy recomendable que tengas un software de seguridad capaz de analizar en tiempo real cualquier tipo de amenaza.

Leer la política de privacidad de la web

¿Cuántas veces hemos entrado en un sitio donde se nos indica que leamos su política de privacidad y automáticamente lo hemos descartado? Éste es un gran error que muchos usuarios cometemos, ya que ahí es donde se nos tiene que indicar de forma clara del uso que darán a nuestros datos.

Si al leerla observamos que no dice con claridad el uso que harán con los datos personales que introduzcamos (datos personales, número de tarjeta de crédito...) debemos optar por abandonar ese sitio, ya que no nos aseguran un uso adecuado de nuestros datos.

Uso de contraseñas seguras



La mayoría de las tiendas online piden que el usuario se registre previamente introduciendo sus datos personales y una contraseña. A la hora de poner la contraseña tenemos que tener muy claro que ésta no debe ser algo lógico ni fácil de descubrir por otro usuario.

Para crear nuestra contraseña debemos utilizar letras, números y cualquier otro símbolo como pueden ser exclamaciones, interrogaciones.... Con esto estamos aumentando la complejidad de esta clave, evitando que algún usuario se pueda hacer con ella.

También es recomendable que esta clave no sea igual a las claves que utilicemos en otros sitios, y sobre todo que no sean las mismas que utilicemos en servicios de banca online.

En referencia a las contraseñas, es muy aconsejable que no usemos la opción de recordar contraseña en los sitios donde nos demos de alta, ya que si lo marcamos cualquiera que entre al equipo podrá entrar en esas aplicaciones donde estamos registrados.

Limitar el importe de la tarjeta de crédito

Una buena práctica para evitar posibles fraudes por medio de la tarjeta de crédito es que tengamos en ésta un límite bajo de dinero a gastar cada día. Este importe puede ser limitado por la entidad bancaria; de esta

forma si consumimos este límite no se podrá utilizar más la tarjeta durante ese día. Así, en caso de pérdida el dinero que puede ser sustraído será el límite que tengamos asignado a la tarjeta.

Otra opción a la hora de comprar por la red mediante tarjeta bancaria es hacer uso de tarjetas virtuales que los bancos te permiten crear. Este tipo de sistema consiste en crear un número de tarjeta virtual, a la que le asignaremos una cantidad de dinero para realizar la compra.

A la hora de introducir el número de la tarjeta donde se hará el cargo, en vez de introducir nuestro número de tarjeta física introduciremos nuestro número de tarjeta virtual, y en caso de que alguien pueda conseguir este número de tarjeta, no podrán hacer nada.

Guardar una copia de la transacción realizada

Cuando uno realiza una transacción online debemos guardar una copia de cualquier información que nos dé la aplicación. Normalmente, tras la compra la aplicación suele enviar un correo con los datos del pedido, a la vez que también los suele mostrar en pantalla.

En caso de problemas, esta copia del pedido nos puede ayudar en las reclamaciones que hagamos sobre el negocio.

Haga uso de su instinto

Este punto lo hemos dejado para el final, pero no por ello es el menos importante. A la hora de realizar cualquier compra por la red debemos hacer uso de nuestra intuición al igual que hacemos en la vida cotidiana.

Debemos tener claro que si la oferta que encontremos es demasiada buena para ser cierta, lo más seguro es que se trate de algún tipo de fraude.

En caso de sospechar que hemos sido víctima de algún tipo de fraude en línea, debemos informar de forma inmediata a nuestra entidad bancaria, para que actúe de la forma oportuna ante esta situación.