

CONSEJOS PARA COMPRAS SEGURAS EN LÍNEA

Autor: Andy Darlymple
Consultor de gestión, administración de información
de riesgos, sistemas de seguridad global (GSS).
Boletín Commercial Crime Internacional
ed. Andy Holder, February 2009
volume 26, No 8, pag 10-11.

La demanda en línea al por menor sigue siendo fuerte y se prevé que crezca en 2009, ya que las condiciones económicas siguen siendo estrechas y la competencia entre los minoristas para nuestra Web en línea es intensa.

La contracción del crédito, sin embargo, también ha tenido el efecto de traer más estafadores en el Internet. Mientras los estafadores se vuelven más sofisticados y se convierten en personas más desesperadas para encontrar la manera de hacer dinero durante la recesión, quien realice compras en línea tiene que vigilar más y desconfiar de las trampas que hay.

Aquí están algunas de las medidas básicas de seguridad de Internet y las "reglas" a las que la industria de Tecnologías de la Información se adhiere, para asegurarse de que las tiendas en línea son seguras y evitar a muchos estafadores, explotadores y oportunistas que están dispuestos a asaltar.

Regla uno: La mayoría de los programas maliciosos son conocidos por explotar los problemas con el software y sistemas operativos. Por esta razón, es muy importante mantener su producto antivirus actualizado con los últimos archivos de firmas (en general ocurre automáticamente, con la mayoría de los productos anti-virus) y sistemas operativos de actualizaciones de Microsoft. Esto reduce la probabilidad de que un código malicioso o clave de registro de software se ejecute en su PC sin su conocimiento, a través de la transmisión de sus datos a los defraudadores por medio de Internet.

Regla dos: nunca este en línea sin asegurarse de que ha activado el firewall personal. Este firewall personal añade una capa de protección a la PC por mantener conexiones desconocidas. La seguridad personal incluido en Windows XP y Vista generalmente se considera insuficiente. Puede controlar los datos procedentes de la PC y filtro de entrada, sin embargo no pueden controlar adecuadamente conexiones salientes, por ejemplo si su PC está infectada por algún programa malicioso, puede ser el

envío de spam o de otros datos en Internet sin su conocimiento, mediante la adición de un Firewall personal usted puede controlar y detener conexiones salientes no deseadas. Hay una serie de firewalls personales en el mercado, tanto gratuitos como de pago, algunos vendedores de anti-virus incluyen firewalls personales como parte de sus productos.

Regla tres: Nunca seleccione la opción "recordar mi contraseña" al registrarse en línea, como las contraseñas se almacenan en la PC, en los formatos de texto, son la primera cosa que un estafador tiene como objetivo. Algunos de los programas maliciosos han sido diseñados y escritos para buscar en tu PC estas contraseñas. Además de esto, si usted utiliza un equipo portátil que se pierde o es robado, la contraseña se va con él.

Regla cuatro: Asegúrese de que sus tarjetas de crédito estén registradas con su tarjeta de proveedores de servicios de seguridad en línea, tales como "Verified de Visa" y "MasterCard SecureCode".

Regla cinco: utilice una sola tarjeta para compras en línea, manteniendo un límite en la tarjeta lo más bajo posible, o incluso usando un complemento para su tarjeta de compra en línea.

Regla seis: asegúrese de usar una tarjeta de crédito y no una tarjeta de débito. El banco le ofrece garantías de seguridad con una tarjeta de crédito que no se dan con una tarjeta de débito. A fin de no tener la tentación de tomar su nueva y brillante tarjeta de platino en un frenesí de compras en línea.

Regla siete: asegúrese de comprobar sus declaraciones regularmente, y si hay cualquier actividad irregular, informe de inmediato.

Regla ocho: siempre busque el título de candado en la esquina inferior derecha del navegador (cuando se usa Internet Explorer) antes de entrar en los detalles de su tarjeta. Recientemente se ha añadido la barra de la pantalla verde para mostrar un sitio Web con un certificado de validación ampliada, esto significa que la clave de inscripción se ha hecho fuerte y tiene el sitio de validación externa.

Regla nueve: haga un hábito del control de la política de privacidad de los sitios para obtener más detalles de cómo su información personal será utilizada y sólo proporcione el mínimo de información personal, especialmente en los formularios en línea.

Regla diez: Nunca compre en sitios a los que llegue por hacer clic en enlaces que están en correos electrónicos de marketing no solicitados (SPAM).

Regla once: Es importante recordar que tú puedes estar haciendo las cosas bien pero el proveedor quizás haga algo mal. Un proveedor puede hacer el almacenamiento de todos los datos de su tarjeta de crédito en un único servidor. Esto crea un sólo gran objetivo de un pirata informático. Si el sitio Web de los vendedores es violado sus datos puede verse comprometidos. La industria de las tarjetas de pago ha presentado recientemente sus propias normas de seguridad de datos para tratar de proteger los datos en reposo, sin embargo, las normas no se aplican plenamente y este riesgo es para todas las transacciones con tarjeta de crédito, no sólo a través de Internet.

Regla doce: finalmente, no basándonos en testimonios de clientes anteriores, en las organizaciones de marketing y no necesariamente en hechos; la regla de oro del comercio sigue siendo la misma que alguna vez fue... si la oferta parece demasiado buena para ser verdad, ¡probablemente lo es!