ANÁLISIS

La seguridad y la tecnología (I)

ANDRÉS JULIÁN GÓMEZ MONTES
CONSULTOR EN INNOVACIÓN Y ESTRATEGIAS EMPRESARIALES

Hace unos días fui invitado a un foro sobre el futuro de Ibagué como ciudad-región, en mi calidad de vicepresidente de la comisión de educación y capacitación de la *Cámara Colombiana de Comercio Electrónico*. En este tipo de eventos, a los cuáles asisto permanentemente, siempre se repiten algunas preguntas y esta no fue la excepción. Al finalizar mi intervención se me acercó un empresario a preguntarme cómo "combatir" los fraudes y percepciones de inseguridad en las compras en línea.

La respuesta a esta pregunta, que compartiré más adelante, me hizo pensar de la importancia de la seguridad cuando estamos hablando de la tecnología, de las percepciones que tenemos los usuarios, y en particular los empresarios, y lo que debemos hacer frente a esta.

Para empezar quiero dejarlo muy claro: la seguridad es un tema vital en el ambiente de las tecnologías. Sin embargo, muchas requieren cierto apoyo de los usuarios, cosa que no siempre hacemos.

En un artículo anterior hablé de los altos costos que puede tener perder información de nuestra empresa, por ejemplo, cuando perdemos un computador o se daña un disco duro. De la misma forma, con lo "hiperconectados" que estamos actualmente en internet, son muchos los riesgos y la información que tenemos almacenada en nuestros equipos o que enviamos a través de internet, puede ser comprometida en cualquier momento. Esto no es para ser alarmista, pero si para tomar medidas preventivas.

Retomando la pregunta del empresario que se me acercó en Ibagué, le compartí un dato que manejan las franquicias de tarjetas créditos. Ellos dicen que es mucha más alta la tasa de fraude con tarjetas crédito que se hacen con clonaciones o robo de información, cuándo se paga la cuenta en un restaurante o tienda física, que a través de una compra en internet. Es decir, al darle nuestra tarjeta para un pago a un mesero o empleado de la tienda, estos pueden robar la información de la misma y así es cómo se cometen los principales fraudes. El problema es que esta información robada en el mundo físico, usualmente acaba siendo usada en portales de internet.

A pesar de lo anterior, es importante tomar ciertas medidas de precaución. Por ejemplo, cuando se compre a través de internet, nunca lo haga en un computador que no sea de su propiedad y mucho menos en uno público, como el de un café internet o una biblioteca. Adicionalmente y en lo posible, tenga instalado algún programa antivirus y/o antiespia (antispyware).

Si usted es un ejecutivo que se mueve mucho y se conecta a redes wifi de internet públicos, tome en cuenta lo siguiente. Para empezar, en lo posible utilice páginas web con certificados SSL (cuando sale el candado cerrado en el navegador y la dirección empieza por https). Si utiliza un lector de correo electrónico para consultar su correo, verifique si su proveedor tiene instalado un certificado de seguridad.

LA SEGURIDAD ES UN TEMA VITAL EN EL AMBIENTE DE LAS TECNOLOGÍAS, PERO MUCHAS REQUIEREN APOYO DE LOS USUARIOS

Por ejemplo, si usted usa los servicios corporativos o personales de Google, es decir Google Apps o Gmail, estos servicios están activados y podrá usarlos sin costo adicional. La ventaja de usar estos certificados de seguridad, tanto para páginas web como para correo electrónico, es que la información viaja cifrada y si alguien está "escuchando" será muy difícil, casi imposible, que descifre la información que usted está enviando.

Otra recomendación que hago a quienes viajan permanentemente y se conectan a estas redes públicas, es usar un servicio cifrado de lo que se conoce como VPN, por sus siglas en inglés (en español es red virtual privada). Algunas empresas ofrecen a sus empleados acceso a estas redes, que además funcionan desde cualquier lugar del mundo, como si estuvieran en su oficina, pudiendo acceder a servidores locales y otros. Una ventaja adicional es que en una red pública con un VPN la información se cifra y nuevamente será muy difícil para un tercero descifrarla.

Hay varios servicios de VPN y yo recomiendo Hotspod Shield, que tiene una versión gratuita, otra paga que no es costosa y funciona con los principales sistemas operativos, incluyendo iOS de Apple y Android.