Foto: Maggy Producciones

Según la Policía Nacional del Perú, los fraudes por Internet han aumentado en más de 80% en los últimos años. Es importante saber realizar transacciones on-line de un modo seguro.

Cómo prevenir los **delitos informáticos** a través de **Internet**

A medida que avanza la tecnología y se impulsan las operaciones electrónicas, más personas realizan sus transacciones bancarias a través de Internet, pues permiten un ahorro en costos bancarios, pero por sobre todas las cosas, un gran ahorro en tiempo. Sin embargo, los delitos informáticos también se hacen más sofisticados y aparecen nuevas formas de fraudes por Internet.

Según estimaciones de la Policía Nacional del Perú, desde el 2006, este tipo de fraudes ha sufrido un aumento superior al 80%. En dicho año, la Policía investigó 276 casos. En el 2009, la cifra sobrepasó los 500 casos. Esto se debe a lo complicado que resulta hallar a los responsables y a lo "fácil" que resulta la ejecución de estos delitos, explica la División de Investigación de Delitos de Alta Tecnología (Divindat) de la PNP.

Hace cinco años, la forma más conocida de cometer delitos financieros por Internet era el "phishing"; luego, apareció el "pharming" (o troyano); y después, el "man in the browser".

El "phishing" consiste en el envío de correos electrónicos que, aparentando provenir de la entidad bancaria, llevan a páginas Web falsificadas desde donde roban los datos confidenciales y claves bancarias a los incautos usuarios.

Los troyanos son programas maliciosos que se instalan en el computador sin consentimiento alguno; por ejemplo, cuando se cargan juegos o videos gratis de

Internet, y que pueden desde capturar datos personales y financieros hasta ver en tiempo real lo que las personas digitan o hacen en su computador.

El "man in the browser" es parecido al "pharming" y falsifica los sitios de los bancos sin que el usuario lo pueda detectar.

En la Encuesta Mundial sobre Seguridad del Consumidor en Línea 2010, (2010 Global Online Consumer Security Survey), realizada por RSA, la división de seguridad de EMC, hubo más de 950 encuestados de América Latina y participaron en el sondeo, en representación de Brasil, Chile, Colombia, México y Perú. Todos los encuestados eran usuarios en línea activos y, durante el mes previo a la encuesta, el 92% realizó una transacción bancaria en línea y el 80% realizó una compra en línea.

En la región, el 31% asegura haber sido víctima de un ataque de phishing y, de todos los consumidores de los países de América Latina, Brasil informó el porcentaje más alto (41%), seguido por Perú (31%), México (30%), Chile (29%) y, finalmente, Colombia (24%).

SANCIONES

La preocupación de la proliferación de nuevas modalidades de delitos, como la violación de correos electrónicos, tarjetas de crédito, entre otros, llegó al Congreso, y hace algunos meses la bancada de Unidad Nacional (UN) presentó un proyecto de ley que tipifica estos delitos y establece sobre ellos penas de cárcel.

El proyecto surgió de la necesidad de ampliar la tipificación de los delitos informáticos que se encuentran fijados en el Código Penal. La iniciativa establece una prisión efectiva de ocho años para aquella persona que utiliza, sin autorización, un medio electrónico de pago ajeno para obtener indebidamente cualquier efecto, bien o servicio. Mientras que será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años, el que sin autorización cree, capture, grabe, copie, altere, duplique o elimine por cualquier medio la data o información contenida en un medio electrónico de pago.

La mayoría de los expertos en el tema considera positivo el hecho de tipificar los delitos que aún no son establecidos en el Código Penal, pero dudan de que el Poder Judicial tenga la capacidad para atender la carga procesal en esos temas.

Es más, algunos refieren que, con la actual legislación, no se conoce si alguna persona se encuentra purgando condena por delitos informáticos, lo que refleja la dificultad para aplicar la ley.

¿QUÉ HACER?

Ante el avance de los fraudes, la seguridad de las operaciones es una constante preocupación de las entidades financieras y muchas vienen realizando campañas para enseñarles a sus clientes a hacer transacciones on-line de un modo seguro.

Para combatir los fraudes tipo "phishing", los expertos recomiendan que si uno quiere ingresar a la sucursal virtual de una entidad financiera lo haga digitando la dirección de dicha entidad directamente en su navegador y nunca a través de enlaces o links. Además, puede revisar la autenticidad de los sitios financieros verificando su certificado digital (haga clic en el candado que aparece en la página) para no ser engañados por páginas Web que se crean con el fin de robar datos.

Para contrarrestar a los troyanos, la recomendación es instalar y mantener actualizado su equipo con un antivirus que lo proteja del espionaje y robo de información, así como mantener su navegador actualizado con todos los parches del sistema operativo para evitar accesos externos no autorizados en su equipo.

Finalmente, es importante tener presente que, al momento de digitar claves en Internet, se debe hacer con precaución y sin que otras personas la vean, así como se recomienda cerrar el navegador al finalizar las operaciones. Es muy importante no realizar transacciones bancarias desde lugares públicos o a través de redes inalámbricas desconocidas.