DELITOS INFORMÁTICOS: EL ROBO DE INFORMACIÓN PARA ACCESO A PÁGINAS WEB DE LOS BANCOS

Ing. Luis Cruz Tregear
Docente de la Facultad de Ingeniería, Nutrición y Administración de la UNIFÉ
Funcionario del Programa Integral de Seguridad Bancaria de la ASBANC

Resumen

Con el avance de la tecnología, vienen las ventajas de servicio para los usuarios del sistema financiero, pero también llegaron los delitos informáticos, los cuales son clasificados como delitos no violentos y pueden afectar a los clientes del sistema financiero que no tienen el adecuado conocimiento en el uso de las herramientas tecnológicas, y/o de las medidas de seguridad que deben adoptar para usarlas y que son el complemento necesario para las medidas que las entidades del sistema financiero peruano han implementado en bien de sus clientes. La seguridad es una tarea de dos: El que brinda el servicio y el que lo utiliza. Ambos son parte de una cadena de valor del servicio y cada uno tiene su tarea; el detalle es cuan comprometidos están ambos en disfrutar los beneficios con seguridad, tranquilidad y confianza. Por ello, mi aporte con este artículo es contribuir a incrementar la cultura de seguridad en los clientes y usuarios del sistema financiero peruano.

Hoy en día las modalidades delictivas no están exentas del uso de la tecnología, los delincuentes informáticos han descubierto la forma de obtener la información del usuario y clave secretas de los clientes, utilizando troyanos y gusanos que en forma de virus se almacenan en los computadores de los clientes. ¿Cómo funciona esto?, se los explico a continuación.

Muchos usuarios tiene activo su servicio de acceso por Internet a las páginas web de los bancos donde al ingresar un usuario y clave personales, pueden tener acceso a los servicios que el banco les ofrece, como son pago de recibos de luz, agua, teléfonos, transferencias electrónicas entre sus cuentas y a cuentas de terceros del mismo banco e inclusive usando un código de cuenta interbancario, se puede transferir dinero de su cuenta a otra cuenta en otro banco.

Los delincuentes envían mensaje de correo electrónico con avisos que supuestamente son generados por las entidades bancarias que indican a los clientes que ingresen a un enlace que está listo en el mismo correo y que los debe llevar a la página web de su banco, para solicitarles una actualización de datos. Lo que realmente hace este enlace es llevarlos a otra página web similar a la original del banco, es decir una página "clonada" y pedirles esa información personal de usuario y clave, luego está página clonada les indica a manera de disculpa que no ha podido acceder al servidor del banco por un problema técnico pero que usted puede intentarlo más tarde. Lo que realmente pasó es que esa información se registró en esa web fraudulenta y el delincuente informático usará esa información para acceder a la página web real del banco y transferir su dinero a otras cuentas y robárselo.

En ese sentido, los bancos han tomado medidas de seguridad y han implementado medios para hacer que las claves sean dinámicas, como por ejemplo, la famosa clave digital del BCP, o la Tarjeta de Coordenadas del BBVA o la clave dinámica token del ScotiaBank y, recientemente, la clave digital vía SMS del Interbank. Todas estas formas

de proteger la clave de los clientes hacen que ésta se cambie dinámicamente en períodos muy cortos de tiempo, aproximadamente cada minuto. Lo que hace que por más que un delincuente pudiera obtener tu clave, ésta ya no vale al minuto siguiente.

Esta nueva tecnología es muy segura, pero nada es completo si el cliente del sistema financiero y bancario, no ayuda con sus medidas de precaución, dado que el cliente es la otra pieza fundamental para promover estas tecnologías y uso masivo de los servicios financieros. Por ejemplo, los clientes no deben usar cabinas públicas para sus transacciones bancarias por Internet, tampoco deben usar cualquier computadora para este mismo fin. Deben utilizar una computadora de su propiedad, segura que solo usted o personas muy restringidas tengan acceso a ella y tener instalado software antivirus, anti-espías, y adecuadamente licenciado con el software de sistema operativo, por su puesto con todos sus parches que el fabricante recomienda.

También la Policía Nacional del Perú, por intermedio de su división de delitos de alta tecnología (DIVINDAT), está permanentemente colaborando en detectar y capturar a los delincuentes informáticos que siguen intentando apoderarse de esta información sensible de los clientes del sistema financiero.

Por ejemplo, recientemente un joven estudiante de computación no solo realizó transferencias de fondos, también hizo recargas virtuales y fue atrapado por la PNP en San Miguel. Esta información salió publicada en el diario La Republica del 17 de Junio del 2010. El hecho ocurrió en circunstancias que los agentes de la Dirincri lo sorprendieron en la cafetería 'Starbucks', del centro comercial San Miguel, cuando acababa de conectar su laptop a la red Wifi del referido local, y tenía en su poder una lista de claves y números de tarjetas de crédito.

La seguridad informática es un tema muy amplio y este tema es uno de los tantos del que podemos comentar en otras publicaciones.