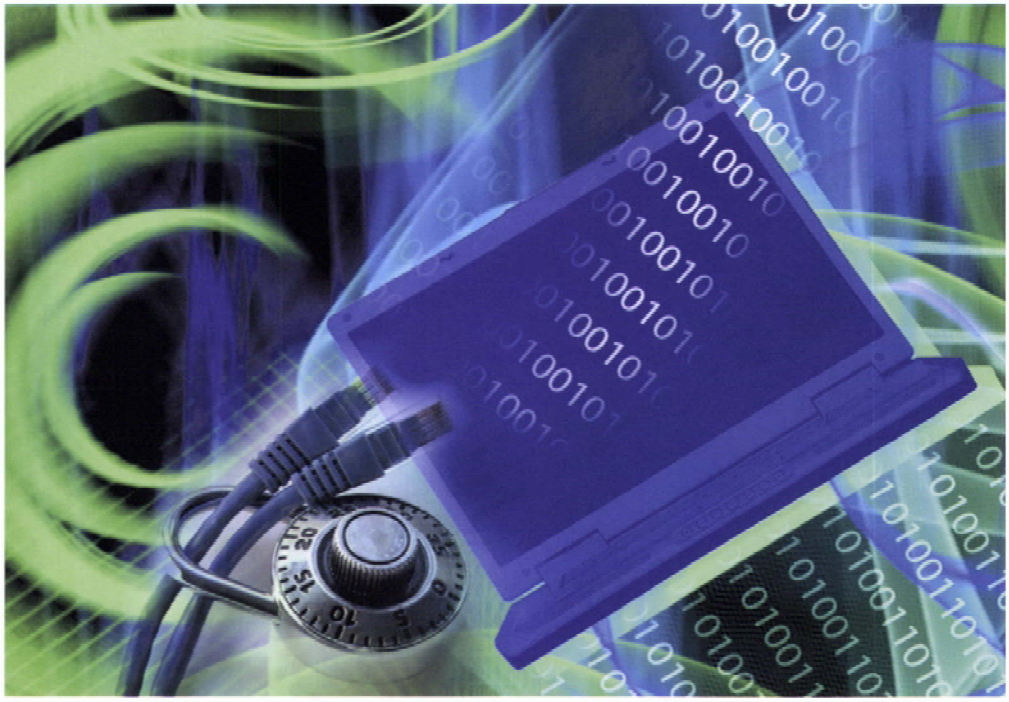
Seguridad informática en Chile:

Cómo Frenamos los Peligros en Internet

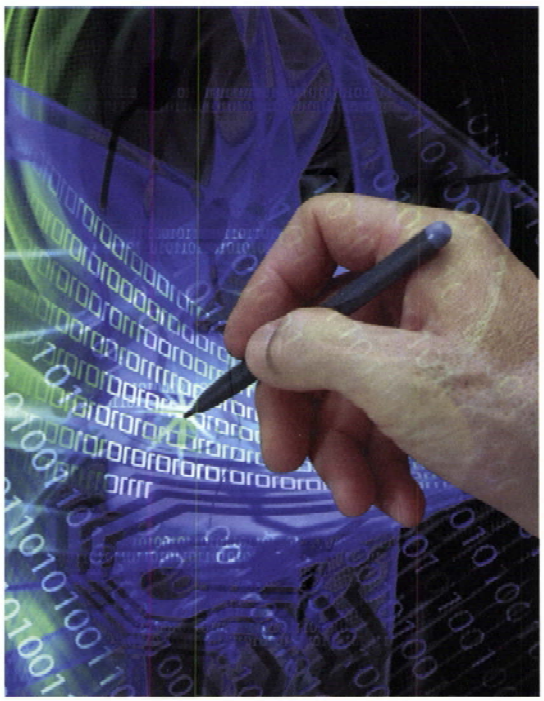
La normativa que obligó a los bancos a entregar una segunda clave a sus clientes para hacer transferencias electrónicas trajo a discusión el grado de seguridad con que hoy los chilenos navegamos en Internet. Y aunque estamos lejos de dar solución total al problema, existen herramientas y conocimientos para minimizar los riesgos. La FCFM ya camina en esa dirección.



El 7 de agosto de 2007 a través de la circular Nº 3.400, la Superintendencia de Bancos e Instituciones Financieras (SBIF) estableció que desde el 1 de enero de 2008 (plazo prorrogado en un mes) las doce instituciones bancarias del país deben contar con dos factores de autentificación distintos para la realización de transacciones a través de Internet, debiendo ser uno de ellos de generación o asignación dinámica.

Se exigió así que los bancos entregaran gratuitamente a sus clientes un dispositivo que otorgue una segunda clave, pudiendo ser una tarjeta de coordenadas con dos tipos de ejes, de números y letras que al combinarse dan una clave; un pequeño dispositivo digital (Token) que al momento de hacer la transferencia provea una clave al cliente; o un SMS (Short Message Service) que arroja la segunda clave a través del celular.

Lo que hay detrás de esta medida es una creciente preocupación en todo el mundo por la seguridad en las redes, ya que la frecuencia creciente de fraudes a través de la red y la utilización maliciosa de los datos captados por hackers pone de manifiesto la inseguridad con que hoy navegamos en Internet. Según un estudio reciente de la empresa Symantec, creadora de Norton Antivirus, el número de virus informáticos, "gusanos" y "troyanos" actualmente en circulación ha superado la cifra del millón. Y agrega



que la tercera parte de las amenazas actualmente en circulación fueron creadas en 2007.

CONTRASEÑAS FIJAS = TECNOLOGÍA OBSOLETA

El académico del Departamento de Ciencias de la Computación (DCC) de la FCFM - U. de Chile y experto en seguridad informática, Alejandro Hevia, explica que en el caso de los bancos es necesario analizar tres aspectos en la seguridad: el primero que el servidor del banco sea seguro, aspecto que en general en Chile está bien desarrollado. El segundo componente es que el canal de comunicación esté protegido (típicamente usando un mecanismo denominado SSL), la forma más sencilla de comprobarlo es a través del "candado" que aparece en la parte inferior de la pantalla que certifica ese nivel de seguridad. Y el tercero es la seguridad del computador de quien realiza la transacción, que es el punto más crítico. "A los bancos se les obligó a ayudar en la prevención de este último componente porque usualmente no es suficientemente buena" dice Hevia, y agrega: "si como usuario de Internet no soy cuidadoso con los programas e instalo juegos de dudosa procedencia o bajo programas a través de sistemas Peer to Peer (P2P), es altamente probable que a la vez descargue programas maliciosos o *malware*, que no son evidentes cuando los instalas porque no muestran ningún indicio de que los estás descargando. Pero éstos rápidamente toman el control del computador y te espían pudiendo conocer, por ejemplo, la contraseña que usas para conectarte al sitio Web del banco".

Precisamente para evitar que programas maliciosos graben las contraseñas y se utilicen para robar dinero de las cuentas, los bancos decidieron incorporar la autentificación de dos factores, lo que significa que para conectarse al banco el cliente hoy tiene que demostrar que sabe algo y que tiene algo. "Lo que se quiere prevenir es que si un *malware* ve mi contraseña personal y se la envía a un *hacker* malicioso, éste, al no tener el dispositivo que entrega la segunda contraseña, puede ver la cantidad de dinero que tengo pero no puede hacer transferencias. Este tipo de dispositivos te generan contraseñas que van cambiando, y por mucho que alguien las monitoree no debiera ser capaz de adivinar la próxima contraseña válida", explica el académico.

Como usuarios, mantener la "higiene computacional" es fundamental para evitar el ataque de malware, para lo cual Alejandro Hevia dice que los pasos a seguir son:

1. Tener las actualizaciones al día.
2. Tener antivirus, antispyware y cortafuego.
3. Siempre instalar software que provengan sólo de fuentes confiables.

Aunque Hevia aclara que estos dispositivos son efectivos, no significa que sean infalibles, "pero sí representan un paso adelante al evitar que una contraseña fija sea todo lo que determina si muevo dinero de mi banco, agregando un nivel extra de protección. La utilización de contraseñas fijas es tecnología obsoleta y basar la seguridad sólo en una tecnología obsoleta resulta peligroso".

A juicio del profesor, estos dispositivos debieran servir al cliente por largo tiempo: "Por ejemplo, el Token no tiene una limitación a priori porque la matemática utilizada no se tornará insegura dentro de un tiempo, por lo que debieras pedir uno de éstos una sola vez. Y aunque no son infalibles, hoy el costo de abrirlos y leer la información es muy alto y requiere de conocimientos muy especializados".

Quizás la única posibilidad de ataque, según Alejandro Hevia, sea a través de una variante del método conocido como *phishing*, cuya

estrategia más común es enviar un email en que convencen al usuario de conectarse a un sitio Web que en apariencia es exactamente igual al original, pero la URL es distinta. "Los nuevos dispositivos están hechos para prevenir que ese sitio falso guarde la contraseña, porque al ser dinámica no le va a servir para una próxima vez. ¿Dónde está el problema? En que si bien no le sirve para una próxima vez, sí le sirve para esa vez, lo que significa que si ese *hacker* malicioso se conecta al sitio Web al mismo tiempo que yo me estoy conectando, lo que puede hacer es ubicarse en 'el medio'. Entonces él me pregunta a mí cuál es la contraseña, él se la envía al banco y a su vez el banco cree que está hablando conmigo, pero en realidad está hablando con el hacker", explica el académico.

LA HIGIENE COMPUTACIONAL ES LA CLAVE

¿Y qué pasa con las compras en línea? Alejandro Hevia expresa que hoy es muy fácil clonar las tarjetas por Internet porque sólo se necesita el número y los datos de la persona, que pueden ser obtenidos fácilmente por los programas maliciosos. "Para evitar esto, las tarjetas de crédito y débito en algunos países de Europa tienen un chip que almacena la información de forma muy protegida que no revela el número tan fácilmente", y explica que la ventaja de estas tarjetas es que no son clonables, "porque el chip ocupa protocolos para encapsular los datos que sólo los puede leer el banco".

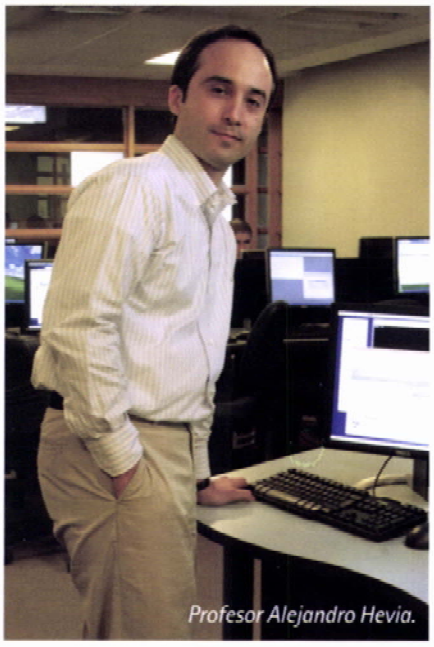
A juicio del académico las tarjetas nacionales usan una tecnología de cinta magnética que "está obsoleta y es tremendamente insegura, ya que es muy fácil de copiar y las máquinas que permiten clonarlas son muy baratas", por lo que la tendencia debiera ser que los bancos nacionales adopten la tarjeta con chip, porque "se están dando

Las tarjetas de crédito con chip son más seguras que las tradicionales de banda magnética.

cuenta de que la tecnología está llegando a un punto en que ya no es tan conveniente mantenerse en el *statu quo*".

En este sentido, Hevia destaca que el aumento en las medidas de seguridad les está haciendo más difícil el trabajo a los *hackers* maliciosos, a quienes ya no les basta con recopilar datos y después usarlos. "Pero por otro lado –argumenta- cuando le prometes a la gente mayor seguridad, ellos bajan las defensas. Y si les llega un e-mail de *phishing* no le dan mayor importancia porque creen que con tener un Token basta". En este sentido, la "higiene computacional" se torna un factor esencial para evitar ataques. Es decir, que el usuario mantenga buenas prácticas, siendo una de ellas obtener programas de fuentes confiables, explica el profesor. "Si instalas un programa pirata puede que venga alterado por un *hacker* y una vez que instalas algo en tu computador ya no hay mecanismo para que se vuelva confiable. Y ahí está la importancia de tener licencias legales". Al respecto, cuenta que existen alternativas para utilizar sistemas operativos seguros, como Linux, que incluso se pueden descargar gratuitamente desde Internet. "Lamentablemente mucha gente se despreocupa y le da lo mismo si hay un *software* malicioso corriendo. Pero cuando accidentalmente instalo algo estoy

> Hoy es muy fácil clonar las tarjetas por Internet porque sólo se necesita el número y los datos de la persona, que pueden ser obtenidos fácilmente por los programas maliciosos.


Profesor Alejandro Hevia.

abriendo las puertas para que un *hacker* malicioso pueda tomar completo control de mi computador remotamente, pudiendo no sólo ver lo que escribo, sino también puede guardar cosas en mi computador, por ejemplo, pornografía infantil y desde ahí comenzar a distribuirla. Entonces abrir la puerta para que otro controle mi equipo me hace susceptible de responsabilidades que no me competen", explica el académico del DCC.

RESPUESTAS DESDE LA FACULTAD: CLCERT

La seguridad informática comprende muchos más aspectos que el bancario. Y para abordarlos en su conjunto, una de las

PRIMER CONCURSO DE HACKEO ÉTICO

Con el objetivo de crear conciencia sobre la seguridad informática y evaluar el nivel técnico de los expertos en seguridad de nuestro país el CLCERT, con el auspicio de Microsoft organizó una iniciativa única en Chile: el "Ethical Hacking Challenge", concurso que consiste en encontrar las fallas de seguridad en la configuración y operación de una máquina específica.

El servidor "Challenge" ejecuta el sistema operativo Microsoft Windows Server 2003 R2™ que utilizó Microsoft Internet Information Server 6™ como software de servicios Web. Este servidor tiene tres vulnerabilidades plantadas en forma intencional, cada una con un grado de dificultad mayor. Los participantes, estudiantes o profesionales del área de seguridad informática, que primero logren ingresar exitosamente al servidor a través de alguna de las vulnerabilidades plantadas u otras nuevas, ganarán el concurso que se inició el 21 de abril y se extenderá por varios meses. El objetivo del concurso es crear conciencia sobre la seguridad informática y evaluar el nivel técnico de los expertos en esta área en el país.

importantes iniciativas al interior de nuestra Facultad es el CLCERT –Grupo Chileno de Respuesta a Incidentes de Seguridad Computacional– compuesto por investigadores de nuestra Facultad. Su misión es monitorear y analizar los problemas de seguridad de los sistemas computacionales en Chile y reducir la cantidad de incidentes de seguridad perpetrados desde y hacia éstos. Asimismo, el CLCERT constituye un punto nacional de encuentro, contacto y coordinación entre instituciones y personas relacionadas del medio local.

Junto con realizar un trabajo investigativo que permita alertar y educar a la comunidad sobre las principales amenazas, el CLCERT también realiza trabajos colaborativos con empresas y el gobierno, siendo uno de sus principales intereses atacar problemas macro, de "importancia nacional" según define el profesor Alejandro Hevia, quien también es director de este Grupo.

Si bien el CLCERT está abierto a trabajar con el gobierno y con empresas, su principal objetivo es atacar problemas más grandes que los usualmente abordados por una sola empresa. Entre los temas de interés para el CLCERT se encuentran resolver la implementación segura de las facturas electrónicas y de la votación electrónica, asegurar las redes chilenas, establecer un sistema de manejo de datos personales o, por ejemplo, ver cómo transformar todos los documentos del poder judicial a formato electrónico, garantizando que éstos no sean modificados por los usuarios si son leídos en Internet. Son problemas conceptualmente difíciles; que no son fáciles de resolver por una sola empresa que trabaje en seguridad. Su solución, que requiere de conocimientos altamente especializados, involucra a entidades de gobierno, empresas y ciudadanos en general. "Nos interesa investigar estos problemas y creemos tener el conocimiento técnico para dar soluciones a los desafíos que involucran", dice el académico y agrega: "contamos con un grupo consolidado, que cumple un rol significativo en docencia e investigación sobre estos temas en Chile".

Sin embargo, al interior del grupo existe claridad respecto de que hay dificultades más urgentes cuya resolución permitirá abordar mejor otros problemas de mayor importancia nacional. "Quizás hoy lo más urgente sea resolver el tema de los programas espías, que está muy extendido. Creemos que el país debe atacar lo básico, la amenaza del *malware* que está afectando a todas las instituciones, por lo tanto tenemos que coordinar a la gente para que se preocupe, que el gobierno y las empresas se preocupen y educar a los ciudadanos en el buen uso del *software*. El problema del *malware* es esencialmente de educación, porque existen técnicas y herramientas para aminorarlo. Una vez controlado este problema podemos empezar a hablar cómo resolver la transformación de los archivos del poder judicial, la votación electrónica u otros problemas del país", explica Hevia.

SOFTWARE MÁS SEGURO

El segundo desafío, muy relacionado con el anterior, es el de autentificación en Internet, "que sepa con quién estoy hablando" señala Hevia. Y agrega "en este momento no hay ningún mecanismo fácil para demostrar que yo soy yo en Internet y esa es una de las razones de muchos de los problemas de seguridad en la red".

Finalmente, un tercer gran desafío es desarrollar *software* seguro: "Lamentablemente, el *software* es con frecuencia inseguro, tiene errores introducidos involuntariamente. Hacer programas es muy complejo y estas equivocaciones son utilizadas por *hackers* para hacer daño. Es un gran desafío, sobre todo para nosotros como Universidad, enseñarles a los estudiantes a hacer programas seguros. Existen herramientas que nos ayudan a hacer programas con menos errores, pero ninguno es la panacea. Si se resuelve este desafío, el *malware* va a disminuir pues no va a tener cómo entrar fácilmente a mi computador. Y también se podrán resolver de mejor forma temas como la autentificación, anonimato, privacidad y responsabilidad en Internet", concluye Hevia.

Texto: Ana Gabriela Martínez A.