

Páginas web falsas permiten obtener contraseñas para extraer fondos

"PHARMING": LA NUEVA ESTAFA QUE AMENAZA LAS TRANSACCIONES BANCARIAS A TRAVÉS DE INTERNET

Estafadores "2.0" traspasan fondos bancarios clonando páginas, lo que resulta en un mecanismo más sofisticado y difícil de detectar.

Es 1995, y Angelina Jolie devela el poder de la red al ingresar a las páginas secretas del gobierno estadounidense en la película "Hackers". Más tarde, en 2006, la realidad supera a la ficción. Chile resuena en EE.UU. gracias al "Byond Team", el cuarteto de adolescentes chilenos que botaron la web de la Nasa y trajeron la polémica de los "piratas" al país.

Poco a poco, la seguridad virtual se ha ido convirtiendo en una de las principales preocupaciones de los sitios de compras online y bancos.

Al igual que en el resto del mundo, en el país las transacciones bancarias por internet se han hecho cada vez más masivas. Según datos de la Superintendencia de Bancos e Instituciones Financieras (SBIF), cada semestre unos dos millones de chilenos emplean portales bancarios, lo que también ha despertado el apetito de piratas que buscan "hackear" las cuentas.

Si al comienzo los ataques venían a través de métodos como el "phishing" (ver recuadro), ahora los robos cibernéticos se han vuelto más sofisticados. Lo último corre por cuenta de un virus que entra a los computadores, y cada vez que el cliente de un banco intenta entrar a su portal lo envía a una réplica igual, pero interferida por estafadores que copian sus claves y en segundos transfieren sus fondos a otras cuentas.

Se trata del pharming; su nombre alude a las cosechas de los granjeros, ya que recogen de a poco fondos de terceros. "Llega al computador como un virus que modifica archivos de su PC para que al momento de ingresar a la web sea enviado a una página falsa", explica el inspector Felipe Herrera, de la Brigada del Ciber Crimen de la Policía de Investigaciones (PDI).

En Chile ya existen casos de pharming que se vieron a fines de 2009, aunque por tratarse de un crimen nuevo todavía no está estipulado en la ley como tal y es archivado con otras causas, lo que no permite cuantificar con precisión el número de estafas ni el monto.

MEDIDAS DE SEGURIDAD:

Para evitar este tipo de robos, los bancos han reforzado sus medidas de protección. Aunque instituciones financieras consultadas no quisieron referirse al tema, se han implementado nuevos mecanismos para evitar ataques. Uno de ellos es la tarjeta con coordenadas, en formato digital o con plástico, mediante la cual se accede a una clave especial que puede ser utilizada durante un minuto y luego cambia.

Otra técnica son las tarjetas que el banco genera para comprar online . Por ejemplo, en Banco de Chile se llama Pago Seguro y se caracteriza por tener una clave distinta a la cuenta corriente y un monto fijo, que el cliente determina y puede ser utilizada una sola vez.

Pero aún queda camino por recorrer. BL Financial Advisors realizó un estudio en 2009, en el que detectó que entre 15 portales de bancos sólo el 47% de éstos cumplían todas las normas de seguridad.

¿CÓMO DETECTARLO?

Para descubrir este tipo de estafas hay que fijarse en el comportamiento del antivirus que tiene el computador. "A veces salta si detecta algo anormal", explica el inspector Herrera. Pero el trabajo de los bancos y las empresas de seguridad se ve desafiado día a día con las nuevas invenciones de los estafadores 2.0.

Fernando Fuentes, gerente de marketing y desarrollo de Neosecure, señala que "hoy vemos una evolución de mecanismos nuevos. Han sido tan inteligentes que usted hace una transferencia, mira su saldo y los estafadores muestran todo en orden dentro del portal, pero igual se movió dinero a otra parte", comenta.

Fuentes agrega que actualmente los métodos que mejor pueden determinar un pharming es el monitoreo de la conducta de sus clientes. "Si un usuario que siempre realiza transferencias dentro de una misma localidad y en horario diurno de pronto aparece con transacciones durante la noche, según los datos que identificamos en la red, claramente puede ser un tipo de pharming ", explica.

EN CHILE YA EXISTEN CASOS DE PHARMING, PERO NO SE REVELAN PORQUE SIGUEN EN INVESTIGACIÓN.

2 millones de personas ingresan a la página web de su banco en un semestre.

14 millones de transferencias se realizaron vía web en el mismo período.

48 millones solicitudes de información se enviaron por este medio.

73 millones de saldos se revisan por internet.

600 millones Es la cantidad de operaciones realizadas en los portales bancarios

TIPOS DE ESTAFA EN LA RED

Phishing:

Se basa en la persuasión. Es el intento por conseguir información personal mediante llamadas telefónicas, correos electrónicos y mensajes instantáneos. El objetivo del estafador es robar la identidad de una persona y sus fondos. Usan logos corporativos con temas como las actualizaciones de seguridad y ofertas de servicios nuevos, con enlaces a páginas que parecen legítimas, pero son fraudulentas.

Pharming:

No solicita la información, sino que secuestra la dirección del portal bancario y la suplanta por una página falsa, que permite extraer los datos personales de los clientes. Es mucho más complejo que el "phishing".

CLAVES PARA ENFRENTAR LAS ESTAFAS CIBERNÉTICAS

Ante los nuevos trucos para obtener claves bancarias, la Brigada del Ciber Crimen entregan consejos prácticos:

1. Visitar las páginas del banco sólo desde un computador personal, nunca desde lugares públicos.
2. Jamás digitar las claves, contraseñas o Digipass por correo electrónico ni teléfono.
3. Mantener actualizado el antivirus.
4. Ratificar si los correos recibidos de bancos son verdaderos o no.
5. Leer las medidas de seguridad que recomiendan en su banco.

Andrea Ortega Carreño