Lunes, Febrero 06, 2012

Banca electrónica más segura: las amenazas

Escrito por CXO Community Latam
Viernes, 25 de Noviembre de 2011 06:00

Blog - Seguridad | Informática
Usar puntuación: / 3
Malo Bueno Puntuar
COMPARTIR

Cuando una persona utiliza la banca electrónica juega un rol m importante en mantenerse seguro mientras está en línea. La ra que los hackers que buscan robar la identidad bancaria en líne la PC no a los sistemas de banca electrónica.

Es posible trabajar con el banco para hacer que la experiencia electrónica sea más segura si se comprende cómo funcionan lo ataques, se siguen las buenas prácticas básicas de seguridad utilizan opciones avanzadas de seguridad.

Los sistemas bancarios tienen una seguridad excelente, por lo criminales cibernéticos no atacan los sistemas bancarios sino computador.

Los hackers usan la suplantación de identidad o las aplicacion software financiero maliciosas (software malicioso) que instalar PC para robar datos como nombres de usuarios, contraseñas e secretos compartidos que el usuario le facilita al banco y que confirman respuestas a preguntas como "¿Cuál fue su primer aut

La suplantación de identidad es un ataque que se da en dos partes. El usuario recibe un mail que parece legítimo y cree en lo desde su banco, pero cuando hace click en un link lo direcciona a la página de un hacker que está tan bien hecha que parece página del banco. Al intentar iniciar sesión en el sitio falso de un hacker, se le da la contraseña bancaria a un ladrón.

Por otra parte, las aplicaciones de software maliciosas son programas que, mediante un engaño, la persona accede a instalar. usuario cree que está instalando algo inofensivo y útil, como por ejemplo un codificador de audio, música gratuita o un juego. E problema es que también recibe el software malicioso sin darse cuenta.

Hay muchos tipos de software maliciosos. Los Keyloggers (registrador de teclas) monitorean lo que se escribe en busca de cla banca electrónica, después capturan las pulsaciones de teclas y las envían al hacker. Los llamados Scareware pueden abrir ur ventana emergente que se parece a un aviso del banco intentando que la persona llene un formulario. Los software maliciosos redireccionar el buscador a una página de un hacker al ingresar la dirección de la página del banco. El riesgo está en que, sin el usuario le está dando información confidencial a un criminal cibernético.

Otros programas pueden apropiarse de la computadora y manejarla remotamente o incluso, invadir sesiones de banca en línea dinero al usuario sin que se dé cuenta. Este ataque, llamado Man in the browser, generalmente está reservado para adquisicio cuentas corporativas de alta rentabilidad.

Por último, el estudio realizado en 2011 por el Instituto Ponemon sobre la confianza en los negocios bancarios dio como resulta 42 por ciento de los pequeños negocios en los Estados Unidos ha sido víctima de algún tipo de fraude de banca en línea el añ

Lo mas importante para protegerse cuando se esta en línea es asegurarse de que nadie robe su nombre de usuario y contrase
contraseñas robadas son la raíz del problema de la seguridad en la banca en línea y de Internet en su totalidad. Cualquier pers
tenga su contraseña puede acceder a sus cuentas. Es por eso que un segundo factor de autenticación a través de algo que pc
usuario es una medida de seguridad muy fuerte, ya que el delincuente deberá robar algo físico además de la contraseña para c
un fraude en línea.

Autor: Samuel Hourdin, Director de la División en Latinoamérica de eBanking, Gemalto