Noticia publicada en la página de la OCU-Nuevo timo cuidado con el SMS del banco.

NUEVO TIMO: CUIDADO CON EL SMS DEL BANCO

Los mensajes SMS que envían los bancos a nuestros móviles avisando de las operaciones que realizamos con tarjeta son el blanco de un nuevo timo. Hay que estar atentos.

Los mensajes SMS que envían los bancos a nuestros móviles avisando de las operaciones que realizamos con tarjeta son el blanco de un nuevo timo. Hay que estar atentos.

Las nuevas tecnologías son terreno abonado para los ciberdelincuentes: phishig, spam y otro tipo de engaños están a la orden del día.

Esta vez, la alerta es provocada por los SMS del banco.

Muchas entidades bancarias ofrecen a sus clientes la posibilidad de enviar un SMS a su móvil informando cuando se realiza una operación con la tarjeta de crédito, así como del importe que se carga.

Pues bien, parece que este servicio, muy recomendable pues es una garantía adicional de seguridad en el uso de tarjeta, ha sido el escogido para “planear” un nuevo tipo de fraude a los consumidores.

¿En qué consiste?

Al parecer, envían un SMS informando de una operación inexistente, una compra con la tarjeta con la que le han cargado un dinero y facilitando un número de teléfono para contactar en caso de duda.

Y, como es lógico, el usuario que recibe un SMS con el importe de una compra que no ha realizado se encuentra con que le piden le pedirán los datos de su tarjeta, número, fecha de caducidad, CVS para confirmarle que efectivamente se trata de un error, pero el número al que ha llamado no es el de su banco, por lo que le acaba de dar todos los datos a un desconocido.

¿Qué hacer?

Nuevo Tímo:Cuidado con el SMS del Banco

Escrito por Administrator

Sábado, 06 de Abril de 2013 21:31 -

Por tanto, si tiene dado de alta el servicio de mensajes al móvi, como un elemento más de seguridad, hace bien. Pero debe desconfiar y si le avisan de un cargo que usted no ha realizado, no llame al teléfono que le facilitan en el mensaje: llame directamente a su oficina bancaria o al número de contacto que aparece en la parte posterior de las tarjetas de crédito. Nunca llame al número que aparece en el SMS: es un ejemplo de “phishing” telefónico para hacerse con esos datos personales.