

Ataque mediante phishing a los clientes de Banco Popular, Santander y Pastor

Escrito por ADICAE Centrales - 11/08/2014 10:04

ADICAE ha detectado un caso de fraude del tipo phishing (robo de identidades) para los clientes del Banco Popular. En este caso, el e-mail informa al consumidor de que, por motivos de adaptación de la normativa europea 2007/64/CE, hay que actualizar los datos de las tarjetas bancarias. Ese mismo e-mail ofrece un enlace que nos lleva a una web falsa que tiene la misma apariencia que la web del Banco Popular, pero que nos pide datos bancarios como el número de tarjeta, la fecha de caducidad, el CSC y el PIN. El enlace del correo del caso del Banco Santander, lleva a una web que ellos denominan 'segura' que nos pide todos los datos de la tarjeta. En el caso del Banco Pastor, es un archivo adjunto, un software malicioso que infectará nuestro ordenador para robar las claves. ADICAE le recuerda que el banco nunca va a solicitar claves de sus cuentas al consumidor, y menos el PIN de la tarjeta de crédito o débito.

El 'phishing' es una modalidad de estafa diseñada con la finalidad de robar los datos personales y bancarios al cliente para posteriormente suplantar su identidad ante un tercero. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o SMS sobre todo con los nuevos teléfonos smartphone. El estafador se hace pasar por nuestra entidad bancaria en una aparente comunicación oficial electrónica, mediante la cual se pretende hacer creer al receptor que su banco se pone en contacto con él, solicitándole sus claves de acceso. Dado que los mensajes y los sitios web que envían estos usuarios parecen oficiales, pueden engañar al consumidor haciéndoles creer que son legítimos.

El consumidor no debe de clicar nunca los enlaces que contenga el mensaje recibido o descargar archivos adjuntos. Si lo que quiere es acceder a la web de su banco debe de teclear directamente su dirección web, nunca guardarla en favoritos. Antes de ingresar cualquier tipo de información personal, compruebe si el sitio web es seguro fijándose si aparece con un candado en la barra de navegación o con la ese en el código http (<https://>). Además, puede revisar periódicamente en un cajero automático o en su oficina habitual los movimientos de su cuenta o tarjeta para asegurarse que no hay cambios que no hayan sido autorizados.

En caso de haber sido víctima de fraude, siga estos pasos:

1º Informe inmediatamente al banco del robo de sus datos personales y bancario y exija la anulación del cargo/s.

2º Dé de baja la tarjeta y bloquee su número de cuenta bancaria.

3º Realice una denuncia en la policía.

4º Ponga una reclamación por escrito a su entidad financiera. En caso de ayuda, el consumidor puede pasarse por una de las sedes de ADICAE, donde le podremos ayudar a elaborar su reclamación.

Más información en:

<http://blog.adicae.net/consumidores-2014/2014/07/29/ataque-mediante-phishing-para-captar-datos-bancarios-de-los-clientes-de-banco-popular/>

<http://blog.adicae.net/consumidores-2014/2014/08/04/nuevo-ataque-mediante-phishing-esta-vez-para-clientes-del-banco-santander-y-banco-pastor/>

=====