CÓMO PROTEGER MIS DATOS PERSONALES FINANCIEROS

24 de marzo de 2015

La mayoría de los fraudes relacionados con servicios financieros se realizan para intentar apoderarse de los datos personales. Estos datos son la llave por la que los delincuentes, accederán a las cuentas, utilizarán tarjetas e incluso podrán solicitar financiación a nuestro cargo. Por todo ello, el primer paso fundamental es no revelar los datos personales o financieros a personas ajenas. Entre estos están:

- **Los relacionados con las tarjetas bancarias**: PIN de la tarjeta, número de la tarjeta o PAN, fecha de caducidad y número de seguridad que figura en la parte posterior (CVV).
- **Datos de acceso a la banca online:** Número de usuario, contraseña, firma digital.
- **Datos bancarios:** Número de cuenta
- **Información personal:** Nombre, teléfono, DNI.

Una forma muy común de intentar apropiarse de estos datos es a través del **phising**. Este fraude consiste en el envío de correos electrónicos aparentando ser de una entidad de crédito en el que se solicita verificar o actualizar sus datos de seguridad y le proporciona un enlace para hacerlo. Si se pincha en el enlace se abrirá una página Web que, aunque puede ser idéntica a la de su entidad de crédito (nombre, logotipo, etc.) es una falsificación, sin ninguna relación. Si introduce sus datos personales proporcionará la información necesaria para que accedan a la cuenta bancaria y puedan disponer de todo el dinero.

Ante ello hay que tener claro los siguientes puntos:

- Un banco nunca envía correos en los que solicite información personal.
- Nunca acceda a la banca online a través de un enlace recibido en un correo.
- Contacte con la entidad de crédito ante cualquier notificación sospechosa o si ha suministrado algún tipo de información.

El phising no sólo es exclusivo de las entidades financieras. Otros correos falsos que buscan hacerse con información privada están relacionados con sitios de comercio electrónico (Amazon, PayPal, eBay…) o redes sociales (Facebook, Linkedin,…). Ante la recepción de los mismos lo mejor es ignorarlos y borrarlos. Si detectamos que se trate de phising y accedemos proporcionando datos falsos puede que estemos permitiendo el acceso de software espía (spyware) que posteriormente intentará hacerse con las claves cuando accedamos a la web del banco.

Aunque el phishing se emplea sobre todo para engañar a clientes de entidades de crédito, también se envían muchos correos falsos que imitan ser de otras organizaciones como PayPal, eBay, Amazon, Facebook, MySpace, etc., todos con el pretexto de conseguir datos personales.

Precauciones generales si operamos por banca online

Las entidades financieras realizan importantes esfuerzos en seguridad para minimizar este tipo de fraudes, pero también está en las manos del usuario que debe tener sus equipos protegidos y actualizados, a la vez que llevar a rajatabla ciertos consejos de seguridad:

- Tener instalado y actualizado software de seguridad que incluya: antivirus, firewall y anti-spyware.
- Sistema operativo actualizado con las últimos cambios de seguridad.
- Navegador en el que esté configuradas las preferencias de seguridad.
- No deje sus claves de acceso fácilmente localizables, cerca del ordenador, agenda…
- No utilice la misma clave en banca online que en otros sitios menos seguros. Si se hacen con ella, la probarán en todos los accesos
- Tras usar su aplicación de banca online cierre la sesión. No utilice la opción de recordar contraseñas salvo en ordenadores propios de uso exclusivo en el que tenga otros mecanismos de seguridad
- Verifique que la web sea realmente la web de banca online que funciona bajo una conexión segura. En ella aparecerá un candado o llave y en la barra de direcciones aparecerá a https://... en lugar de http://...

Fuente: www.cincodias.com