

## La seguridad en las conexiones a servidores Web: ¿cuándo puedo estar realmente seguro?

En estos últimos meses se han dado a conocer varios casos de intentos de fraude que podían afectar a los clientes de distintas entidades financieras de nuestro país: BBVA (mayo de 2003), Barclays (septiembre de 2003), Banesto (enero de 2004) o Banco Popular (febrero de 2004). Estos intentos de fraude también se han dirigido contra empresas conocidas de Internet, como la popular eBay, líder en el sector de subastas entre particulares.

El “modus operandi” de estos ataques es el siguiente: a través del envío de un mensaje de correo electrónico falso, que simula proceder del banco o empresa en cuestión, se solicitan varios datos personales a la víctima del engaño y, sobre todo, sus claves de acceso al sistema. Para ello, desde el mensaje de correo se trata de redirigir a la víctima a una página Web con la misma apariencia de la empresa original (el mismo diseño, idénticos logos, etc.) pero que resulta ser falsa, y en la que se solicitan sus datos a través de un formulario.

Así, por ejemplo, en el caso del intento de fraude contra el BBVA, se utilizaba una página Web dentro del dominio “grupobbvanet.com” que no pertenecía a esta entidad. Seguidamente se reproduce el texto incluido en uno de estos falsos mensajes enviados a través de Internet:

*Estimado cliente de BBVA,*

*Le comunicamos que próximamente, usted no se podrá suscribir en Banca Online. BBVAnet es el servicio de banca a distancia que le ofrece BBVA, disponer de este servicio le permitirá consultar su saldo, productos y realizar las transacciones bancarias mas habituales desde su ordenador, en cualquier momento, con toda la seguridad que BBVAnet le ofrece, a través de Internet.*

*Si usted desea tener la oportunidad de poder registrarse en BBVAnet, por favor acceda al sitio que se muestra a continuación. <http://w3.grupobbvanet.com/>*

*Si usted decide registrarse en nuestra banca online BBVAnet, se le contactara telefónicamente después de 24/48 horas confirmándole su suscripción y le llegara una carta por correo con la información correspondiente para que pueda acceder a su banca online en BBVAnet.*

*© BBVAnet 2000-2003 All rights reserved*

*© Banco Bilbao Vizcaya Argentaria S.A. 2000-2003 All rights reserved*

Más recientemente, el 22 de febrero de 2004 se detectó un nuevo envío indiscriminado de correos electrónicos simulando proceder del Banco Popular, donde se solicitaba a los clientes dirigirse a una dirección de su Website para mejorar la seguridad de sus cuentas. En esta ocasión, cuando el usuario hacía clic en el enlace del correo electrónico se abrían dos ventanas, la primera con la página original del Banco Popular, mientras que en la segunda se producía la petición de los datos de la cuenta del cliente, ocultando la verdadera dirección URL del servidor Web al que pertenecía, y que era el utilizado para robar los datos de la víctima.

Por otra parte, muchos de estos engaños e intentos de fraude se han visto favorecido por un fallo de seguridad en el diseño de los navegadores como Internet Explorer, que permitían incluir el símbolo @ en una URL, lo cual dejaba abiertas las puertas a posibles redirecciones a otras páginas Web distintas a las que se pretendía conectar el usuario víctima del engaño. Así, por ejemplo, si el usuario activaba un enlace del estilo: <http://www.bbva.com@186.213.32.12/formulario.htm>, su navegador se conectaría a la página Web “formulario.htm” dentro del equipo que responde a la dirección IP: 186.213.32.12, y no al esperado Website de la entidad BBVA. Esta característica de Internet Explorer fue finalmente corregida por Microsoft en febrero de 2004, con la publicación de un nuevo parche que impide el uso del símbolo @ en una URL.

En consecuencia, para garantizar la seguridad en la conexión a un determinado servidor Web, evitando intentos de engaño o fraude como los citados anteriormente, podríamos recomendar las siguientes medidas básicas de seguridad, que todo usuario debería conocer y aplicar:

1. **Actualización del navegador utilizado en su equipo**, instalando los parches que publican de forma periódica los fabricantes (en el caso del Internet Explorer, Microsoft distribuye los parches a través del servicio “*Windows Update*”).
2. **Comprobación del Certificado Digital del servidor Web** al que se conecta el usuario: para ello, se debe pulsar en el icono con forma de candado que aparece en la parte inferior derecha del navegador (en la barra de estado) cuando se accede a una zona segura, para verificar que la fecha de caducidad y el dominio del certificado digital están vigentes, y que éste ha sido emitido por una Autoridad de Certificación de confianza. Un Certificado Digital garantiza la autenticidad del servidor al que se establece la conexión, evitando los problemas derivados de ataques de manipulación de DNS, usurpación de direcciones IP, ataques semánticos mediante URLs maliciosas, etc.
3. **Comprobación de que se establece una conexión segura SSL o SET:** Las direcciones de las páginas Web seguras empiezan por “**https://**”. Las entidades bancarias y otros servicios sensibles deberían modificar la configuración de sus servidores Web para que por defecto se fuerce a los navegadores a establecer una conexión segura (https) cuando se accede a las páginas donde se encuentran los formularios de autenticación de los usuarios.
4. Nunca se debería acceder a un formulario de autenticación a través de un enlace desde otra página Web o desde el texto de un e-mail: se recomienda teclear directamente la dirección en una nueva sesión del navegador.
5. Se debe desconfiar de un correo electrónico recibido en nombre de una entidad financiera u otra institución con una solicitud para entregar datos personales. En caso de recibir un mensaje en este sentido, el usuario no deberá facilitar dato alguno y se pondrá en contacto inmediatamente con el servicio de atención al cliente del banco o empresa en cuestión para informar de la incidencia.
6. No se deberían establecer conexiones a este tipo de Websites desde lugares públicos (cibercafés, puntos de acceso a Internet en hoteles, etc.), ya que mediante “*sniffers*”, software espía instalado en los PCs u otros dispositivos se podrían capturar los datos enviados en la conexión.