Defensa bancaria ante el cibercrimen

Las TIC han supuesto al sector bancario un cambio en la forma de desarrollar su negocio y prestar servicio a sus clientes. Sin embargo, aspectos como la percepción de falta de seguridad en las operaciones on line o las dudas sobre la privacidad de las transacciones, son problemas añadidos de la banca electrónica frente a la banca tradicional. Por eso, generar más confianza a los usuarios on line es el mayor reto. ***Por C. Sánchez.***

A pesar de las amenazas de fraude bancario on line que sufren muchos clientes de las entidades en Internet, y la inseguridad que esta situación les produce a la hora de realizar sus transacciones a través de la Red, el negocio de la banca electrónica española en 2005 es mejor que el registrado el pasado año con un incremento del 22,52%. No obstante, la mayoría de los usuarios limita su contacto con el banco on line a consultas y búsquedas de información, más que a la realización de transacciones, por la falta de confianza sobre la confidencialidad y seguridad de sus operaciones.

Phising

Los clientes de las entidades que operan en Internet pueden sufrir fraude mediante ataques directos on line. Este tipo de ataques es cada vez más frecuente y, entre los distintos tipos, destaca, tanto por su alcance como por el número de casos detectados en los últimos meses, el denominado phishing que consiste en el envío masivo de correos electrónicos que fingen proceder de las propias entidades con la intención de atraer a los internautas hacia páginas web falsas con el objetivo de hacerse con información confidencial.

CUESTIONARIO

1. ¿Qué tipo de tecnología han implantado para asegurar sus sistemas de transacciones on line y pasarela de pagos con clientes?

2. ¿Cuáles son los tres principales ataques/fraudes recibidos?

3. ¿Quiénes son sus proveedores en seguridad?

4. ¿Tienen previstas otras medidas de seguridad a medio plazo?

Entre las entidades financieras cuyos clientes han sufrido ataques están tanto entidades de gran tamaño, como La Caixa, Banesto o Caja Madrid, como entidades de menor volumen, como Cajamar. Como cabria esperar, las entidades aseguran defensivamente que casi ningún cliente "ha picado" y que, por tanto, el fraude ha sido mínimo. Sin embargo, según el informe 'Dividendum 2005' presentado por el Observatorio Español de Internet (OEI), se calcula que más de 10.000 personas en España han sido víctimas de estafas por phishing, y que las entidades bancarias "no son cien por cien sinceras" sobre los problemas de seguridad, ya que muchos bancos que operan por internet que dicen recibir cien ataques al año en realidad deberían decir "cien ataques diarios". El responsable del Grupo de Delitos Telemáticos de la Guardia Civil, Juan Salom, ha explicado que la mayor parte del phishing en España proviene de las mafias de Europa del Este, que "han encontrado su agosto en estas prácticas delictivas".

El Banco de España, haciéndose eco de recientes intentos de fraude a través de Internet a los clientes de distintas entidades bancarias, se ha dirigido a las entidades de crédito, para llamar su atención sobre "la necesidad de poner los últimos avances tecnológicos al servicio de las transacciones electrónicas como requisito para poder ofrecer ese tipo de servicios y así mantener la confianza de los clientes en que ese canal es seguro, eficiente y fiable".

En este sentido, todas las entidades financieras que prestan servicios on line están tomando medidas encaminadas a solventar este fenómeno, sin grandes diferencias en lo que a seguridad se refiere. Las entidades presentes en el reportaje: Unicaja, CajaSur, Banco Pastor, Banco Sabadell, Inversis Banco, Bankinter, Banco de Valencia y Banco Urquijo, presentan tecnología basada en navegación segura y cifrada, cortafuegos, sistemas detectores de intrusiones, programas cortafuegos, firma electrónica, tarjeta de coordenadas y teclado virtual en la pantalla con permutación de caracteres, etc., como norma general.

En estos momentos, lo que preocupa al sector financiero, más que el daño económico que ocasiona, es el daño a la credibilidad y a la confianza en el servicio on line. Por eso, el futuro de la e-banca dependerá de cómo afronten las entidades este problema, de las medidas de seguridad que establezcan para evitarlo y de las soluciones que den a los clientes afectados. ☒

Banco Pastor

Rubén Suárez. Director Técnico. Banco Pastor.

"Estamos trabajando en soluciones que impidan o, al menos, minimicen el fraude cibernético".

Rubén Suárez.

1. Nuestra tecnología es la misma que la del resto de bancos y cajas, basada en navegacións egura y cifrada (https/ssl), y firma de operaciones mediante tarjeta de posiciones y teclado virtual en la pantalla.

2. Resaltaría el engaño a usuarios, comúnmente llamado phishing; la falta de diligencia en la cuestodia de claves por parte de los mismos y la ausencia de aplicación de las mínimas medidas de seguridad en sus equipos, fundamentalmente actualizaciones del sistema operativo y antivirus.

En este momento, estos fenómenos se están combatiendo con información, mediante cartas *ad-hoc* y publicación de aspectos de seguridad a tener en cuenta en nuestras páginas web.

3. IBM, Cisco, CheckPoint y TrendMicro.

4. En el ámbito de la asociación Centro de Cooperación Interbancaria (CCI), de cuyo grupo de trabajo de "Seguridad Informática" el banco forma parte, se está trabajando en estos momentos en la valoración y posterior recomendación de soluciones que impidan o, al menos minimicen, el impacto del fraude cibernético. Es intención del banco adoptar a medio plazo alguna de las soluciones que sean recomendadas.

Banco Urquijo

Luis Pérez Ureña. Diector de Internet. Banco Urquijo.

"Banco Urquijo no ha recibido ningún ataque"

1. Para el acceso de los clientes al área privada de la web, Banco Urquijo utiliza un sistema de cuatro claves (nombre de usuario, contraseña, número de tarjeta de banca a distancia y PIN) con conexión cliente-web segura (encriptación SSL 128 bits). Dichas claves permiten al cliente realizar todas las clases de consulta. Sin embargo, para aquellas operaciones que supongan movimientos de dinero, adicionalmente a las claves, se exige al cliente firmar electrónicamente dicha operación. Para ello, utilizamos una tarjeta de coordenadas aleatorias a la que sólo puede acceder el propio cliente.

2. No hemos recibido ningún ataque.

3. BM para la seguridad de los sistemas; VeriSing, como proveedor de certificados SSL; y Nokia y Cisco, firewalls.

4. Por un lado, estamos trabajando en temas como la prevención de 'ataques Dos', y ataques phishing y

Luis Pérez.

pharming, amenazas que se dan en el sector hoy en día.

Por otro lado, una de las tendencias más interesantes que estamos analizando ahora son los nuevos sistemas de autentificación segura basados en tecnologías móviles. Por ejemplo, sistemas que para un pago con tarjeta solicitan una verificación al teléfono móvil, de manera que permiten evitar fraudes con tarjetas de crédito.

Inversis Banco

Francisco Margarite. Director de Tecnología. Inversis Banco.

"La información está cifrada mediante protocolo SSL y claves de cifrado aleatorias de 128 bits".

1. Nuestro sistema trabaja en tiempo real, por lo que las operaciones efectuadas, después de realizar las verificaciones y validaciones pertinentes, se reflejarán inmediatamente en los saldos y movimientos de los productos. El cliente, después de realizar una operación, podrá comprobarla también por el resto de los canales que ofrece Inversis Banco (Centro de Atención al cliente) y en nuestras oficinas en las principales ciudades españolas.

En Inversis Banco toda la información transmitida por la red se encuentra cifrada mediante protocolo SSL y claves de cifrado aleatorias de 128 bits. El cifrado de la información evita de esta manera que personas sin autorización accedan a la información y entren a nuestra web, y garantiza la seguridad de las operaciones en la red. El servidor de Inversis Banco ha sido certificado por Verisign Inc., de forma que el cliente tiene la garantía de que realmente se ha conectado a Inversis.

Este certificado de seguridad garantiza la protección de los datos de nuestro servidor con la última tecnología de encriptación. De ahí, que estas estrictas medidas requieran el uso de navegadores que aguanten la encriptación de 128 bits (Netscape 4.04, Microsoft 4.0 o superiores). Además, su navegador le indicará que se encuentra en una conexión segura mostrando un candado en la parte inferior de la pantalla. Esta información es vital ante la avalancha de ataques de phising, conociendo de forma irrevocable que el servidor al que el cliente se ha conectado es de Inversis y no un sistema suplantado. Desde el punto de vista de autentificación de usuario, Inversis utiliza un primer nivel de acceso consultivo basado en usuario y password (cifrada con algoritmo hash SHA-1) con políticas de generación de password que garantizan la seguridad de la misma ante un ataque típico de diccionario. El segundo nivel es el de transacción. Para este caso, cada cliente posee una conjunto de ocho caracteres que

Francisco Margarite.

denominamos FIRMA y, a la hora de hacer una transacción de cualquier tipo, se solicitan dos caracteres de la misma de forma aleatoria, lo que garantiza adicionalmente que el cliente es quien dice ser.

2. Los ataques más comunes son:

- Red: Escaneo de puertos de nuestros servidores públicos, tanto servidores web, de correo electrónico como servidores FTP. Este tipo de ataque se rechaza a nivel de firewalls perimetrales.
- Aplicación Web: Intentos de ataque del tipo 'salto de directorio' utilizando URL,s maliciosas, así como ataques del tipo *Cross-Site scripting* que permite ejecutar código en el servidor web utilizando la sesión web de otro usuario. Para defendernos de estos ataques, utilizamos tanto nuestras sondas de detección de intrusos para rechazar estos ataques, como la propia programación segura de la aplicación de Inversis.
- eCorreo: Los más frecuentes son el spam y los virus. Estos son rechazados con nuestros productos de detección de spam y antivirus.

3. Indra, HP, Telefónica y, como fabricantes de productos de seguridad, contamos con CheckPoint, StoneSoft, Trendmicro, Panda Software, ISS.

4. Están previstas mejoras en el ámbito de la seguridad, como el que todo el acceso al servicio web de Inversis se realice en modo seguro (protocolo https), ampliando por tanto este protocolo, además de a la parte privada de clientes en la que ya está operativo, a la parte pública. El objetivo es garantizar al cliente que en todo momento se encuentra efectivamente en la web de Inversis y no en otra.

Los más atacados

PRÁCTICAMENTE, ninguna entidad española se ha librado de algún ataque on line indiscriminado tipo phishing, que se han multiplicado en España en los últimos meses. Entre los últimos objetivos han estado Caja Madrid, Banesto o BBVA, aunque en meses anteriores también fueron conocidos los ataques a Santander o a Banco Popular que han denunciado varios intentos de estafas dirigidas a sus clientes. Según el Observatorio Español de Internet, aproximadamente unas 10.000 personas han sido víctimas de este tipo de ataques.

En algunos casos los usuarios han recibido un correo electrónico en "Spanglish" que por gramática y aspecto visual resultaba muy sospechoso. Sin embargo, en los últimos meses los ataques se han perfeccionado notablemente y cada vez resulta más fácil creer en su autenticidad pues el correo se escribe en perfecto castellano, con los colores y gráficos corporativos e incluso redirige a una página web virtualmente idéntica a la de la entidad. Para rizar el rizo, esa página se cierra una vez hemos introducido las claves y nos reenvía a la auténtica, por lo que el cliente no aprecia nada anormal.

Caja Madrid

En el caso de Caja Madrid, uno de los últimos ataques explotaba precisamente el miedo a la inseguridad con el siguiente correo electrónico: *"Estimado cliente de Banco CAJA MADRID! Por favor, lea atentamente este aviso de seguridad. Estamos trabajando para proteger a nuestros usuarios contra fraude. Su cuenta ha sido seleccionada para verificación, necesitamos confirmar que Ud. es el verdadero dueño de esta cuenta. Por favor, tenga en cuenta que si no confirma sus datos en 24 horas, nos veremos obligados a bloquear su cuenta para su protección"*

En este caso, los datos se tecleaban en el cuerpo del mismo correo para ser posteriormente enviados a un servidor hospedado en Taiwán (http://220.130.132.190/manual/t.php) e inmediatamente el usuario era redireccionado a Caja Madrid por lo que no sospechaba nada.

Otro ejemplo de mensajes recibidos por internautas, remitido por un teórico 'Supporte Banca BBVA', pretende ser una comunicación del BBVA. Si se pincha en el enlace del correo electrónico, el receptor llegaría a una web trampa (http://bbva-support.com, ya inactiva), en lugar de a la legítima del BBVA (https://www.bbvanet.com). Quien no se fije en la dirección, no apreciará ninguna diferencia con el original.

El cliente y su máquina

Según el Departamento de Seguridad de Banesto, "hay que tener en cuenta que los fraudes on line más frecuentes, el phishing y el troyano, intentan aprovecharse del eslabón más débil en la cadena de seguridad: el usuario y su máquina, es decir, la falta de conocimientos adecuados por parte del usuario para realizar verificaciones de seguridad, y las vulnerabilidades que puede tener la propia máquina del usuario por una indebida configuración o aseguramiento.

Prevención

Las acciones que tanto Banesto como otros bancos toman contra estos fraudes se dirigen a dos objetivos, con atención preferente al usuario:

- Acción Preventiva: Mantenimiento continuo del esquema de seguridad de la entidad; Información al usuario de todos los aspectos de seguridad involucrados o que deben tenerse en cuenta a la hora de utilizar un ordenador para la banca on line; Hacer hincapié al usuario en buenas prácticas de seguridad, como, p.e, cambiar su clave cada cierto tiempo; Trabajar coordinadamente con el resto de bancos en el foro CCI consiguiendo iniciativas que dificulten la comisión de estos delitos.

- Acción Paliativa: Cuando se detecta un intento generalizado de phishing, se toman medidas especializadas, tendentes a su inmediata paralización, y se mantiene una atención constante, mediante circuitos contrastados de información. ☒

Banco Sabadell

Javier Serrano Cossío. Responsable de Seguridad Tecnológica. Banco Sabadell.

"El número de incidentes ha sido mínimo"

Javier Serrano.

1. Entre otras medidas, destacamos: Tecnologías de cortafuegos; detectores de intrusiones a varios niveles; sistemas de alarma sobre anomalías en los registros de los sistemas; mecanismos de prevención, detección y reacción ante ataques de phishing; uso de múltiples claves y certificados digitales para la realización de operaciones; ocultación parcial de información sensible; teclado virtual para la introducción de códigos confidenciales.

Adicionalmente a la tecnología, un aspecto fundamental para la protección de nuestros sistemas lo constituyen la organización, procedimientos y procesos de actuación en horario 24x7, sin los cuales la tecnología implantada perdería utilidad. En ellos destacamos: La realización de revisiones continuadas de la seguridad a distintos niveles; realización de tests de intrusión; detección y solución temprana de nuevas vulnerabilidades en los sistemas; servicios y procedimientos de actuación ante incidentes; relación con los cuerpos de seguridad y proveedores especializados; uso de metodología de desarrollo y configuración segura; formación y concienciación de las personas implicadas.

En el caso de la pasarela de pagos, estamos adheridos al estándar de seguridad 3D Secure, promovido por Visa y Mastercard, y basada en medidas similares.

2. Afortunadamente, el número de incidentes relacionados con las transacciones on line y pasarelas de pago en los que nos hemos visto involucrados ha sido mínimo y de impacto despreciable. Los principales incidentes suelen ser intentos de intrusión desde Internet, la detección de programas del tipo troyano (variante de virus informático) que pretenden robar información confidencial (número de tarjeta, claves de acceso, etc.) en PC,s desprotegidos de algún cliente, y la creación en Internet de páginas falsas con apariencia de entidad financiera, para engañar a personas a las que se les indica que disponen de una importante cantidad de dinero en la entidad falsa, que podrán retirar a cambio de una elevada comisión.

En todos los casos, la mejor forma de combatir un ataque consiste en disponer previamente de información actualizada sobre las nuevas amenazas que van apareciendo, haber implantado medidas para prevenirlas, concienciar a los clientes y disponer de un plan y un servicio especializado de actuación en horario 24x7, ya que la improvisación no ayuda en estos casos y es fundamental haber previsto medidas de reacción ante incidentes y disponer de una buena relación de contactos internos y externos con los que dar respuesta al incidente.

3. Trabajamos tanto con fabricantes nacionales como extranjeros, pues creemos que también existen buenos productos y proveedores de seguridad en España.

4. En la línea de mejora continuada de la seguridad, trabajamos desde hace tiempo de forma conjunta con las principales entidades financieras nacionales, intercambiando experiencias y determinando soluciones aplicables a los nuevos riesgos que se van identificando.

El sector financiero aúna fuerzas en el Centro de Cooperación Interbancaria

EL Grupo de Seguridad Informática del CCI surgió de la necesidad de abordar y analizar los nuevos tipos de fraude on line como el Phishing y sus variantes como: Pharming,Troyanos, SCAM. El objetivo del Grupo, desde que se formó en mayo de 2004, ha sido concienciar al cliente, coordinar iniciativas, hablar con distintos actores de la lucha contra el fraude, como los Cuerpos y Fuerzas de Seguridad del Estado y Autonómicos, operadoras de telecomunicaciones, proveedores de soluciones y servicios antifraude, etc., con el fin de elaborar una primera herramienta denominada Protocolo Antiphishing, para el Bloqueo de IP's fraudulentas, que luego ha dado lugar a algunos de los Servicios Antifraude que ahora ofrecen los proveedores del sector.

El grupo comenzó con la participación de ocho entidades financieras de reconocido nombre, que representan a todos los sectores (banca, cajas de ahorro y cooperativas de crédito y cajas rurales), a las que se han sumado otras hasta alcanzar más de catorce miembros en la actualidad.

Desde el primer momento y dada la amplitud de la materia (seguridad) a tratar, y la diversidad de temas a analizar y abordar, el grupo se ha concebido muy activo, participando en otros Foros como RESCATA de Red.es o el Foro de Evidencias Electrónicas para aunar esfuerzos y trabajo de todos los actores, además de mantener reuniones y ponencias con CFSE, Microsoft y otros proveedores.

Ante la globalización de las sociedades y la dimensión de los ataques de fraude on line, la única vía para combatirlos y prevenirlos es globalizar los esfuerzos de entidades, CFSE, Administración, industria del software de seguridad, asociaciones de Internautas, operadoras de telecomunicaciones, etc., mediante la coordinación, comunicación efectiva y acciones conjuntas.

Web del Centro de Cooperación Interbancaria.

"Es esencial dotar a los sistemas de métodos de autentificación de usuarios y validación de las operaciones, uso de one time password y Firma-e".

Los principales cometidos del CCI se pueden resumir en:

- Participación en el Foro de RESCATA de Red.es con todos los demás actores involucrados, con el fin de proponer, debatir y adoptar iniciativas y medidas coordinadas de actuación ante el fraude, además de tipificar los posibles tipos de fraude.

- Colaborar con el Foro de Evidencias Electrónicas.

- Evaluar las alternativas y requisitos de un Sistema de Autenticación y Validación Fuerte con el objetivo de mejorar los métodos de autenticación del usuario (cliente) y la validación de la firma de las operaciones en el canal de Banca a Distancia.

- Analizar iniciativas tanto Informativas como formativas a CFSE y a Usuarios con el fin de crear conciencia de seguridad y luchar así contra el fenómeno de la ingeniería social, la táctica más utilizada por los ciberdefraudadores aprovechando el desconocimiento del usuario final, así como proteger con medidas de software ofrecidas por proveedores y en colaboración con entidades, para analizar y/o ayudar al usuario a que el entorno de su PC, desde donde opera en Internet, sea más seguro ya que estas dos partes constituyen el eslabón más débil de la cadena.

- También analizar iniciativas de colaboración en la Respuesta conjunta ante Incidentes, con el fin de disponer de tipificación de los casos, actuar de manera coordinada e incluso poder llegar a cuantificar el fraude sufrido. Para ello, se analizan propuestas de unificación de esfuerzos de respuesta y control con otros Proyectos en marcha desde CCI.

Mafias organizadas

Con respecto a la situación actual de España, en el sector banca "podemos asegurar que el fenómeno de fraude on line, aunque ha venido creciendo en el último año y medio y la tendencia se mantiene, no es especialmente preocupante en cuanto a cifra. Pero si debe avanzarse en combatirlo para evitar su crecimiento porque, sin duda, el fraude on line conocido y sufrido hasta la fecha no es más que la punta de un iceberg, auspiciado por el cibercrimen de mafias bien organizadas y con recursos. Cuando vean que fraudes como el Phishing o Pharming no son rentables, evolucionarán a fraudes más sofisticados con Troyanos en los PC,s de los usuarios, como ya sucede en Iberoamérica, siendo esta última la práctica más extendida.

El fraude también puede evolucionar hacia otros tipos como la piratería de todo tipo de productos, no sólo música; por ejemplo, extorsión on line a partir de datos conseguidos de clientes. Lo más preocupante es la poca estructura necesaria para los fraudes on line: con poco esfuerzo se consigue un gran potencial de engaño y estafa, llegando a poner en tela de juicio la sociedad de la información y, sobre todo, su evolución y tendencia.

Según el CCI, el actual nivel de fraude se puede combatir "con la adopción de medidas *preventivas* (concienciación al Usuario, monitorización de dominios y señuelos, e instalación de herramientas de detección en el PC), *detectivas* (como herramientas antispyware, antivirus, antitroyanos, antiSpam, firewalls) y *correctivas* de respuesta y forenses (mantenimiento de listas y firmas de software, servicios de bloqueo de IP fraudulentas y herramientas forenses que generen evidencias y analicen el software espía utilizado)".

Además, según el CCI, es esencial dotar al método de autenticación de usuarios y validación de las operaciones de una robustez de al menos dos factores y pensar en el uso de OTP *(one time password)* y firma electrónica, como el nuevo DNI Electrónico o certificados reconocidos. Combinando todo ello con el uso de información en tiempo real al usuario para certificar que ha sido él y no otro quien ha realizado la operación.

Lógicamente, todas estas medidas suponen un coste. El beneficio será operar de manera segura y confiable por Internet evitando el fraude. ☒

PASARELAS BANCA

BANKINTER

"Los servidores web de Bankinter han sido certificados por VeriSign, autoridad certificadora internacional".

Edificio sede de Bankinter.

1. Los servidores web de Bankinter han sido certificados por VeriSign Inc., autoridad certificadora internacional, de forma que el cliente puede tener la garantía de que realmente se ha conectado con Bankinter.

- Toda la información transmitida se halla cifrada mediante protocolo TLS- SSL y claves de 128 bits. El cifrado es el proceso mediante el que se hace ininteligible la información intercambiada entre nuestros sistema y el PC del cliente, tratándose de evitar de esta manera que terceros vean, capturen o repitan la información.

- Nuestros sistemas conectados a Internet se hayan protegidos mediante cortafuegos y sistemas detectores de intrusiones, así como programas antivirus. El acceso a la información contenida en estos sistemas está limitado al personal autorizado.

- Sometemos a nuestros Sistemas de Información a Test Periódicos de Intrusión, validando los mecanismos de seguridad y control implementados frente a las últimas técnicas de ataque y vulnerabilidades conocidas. Periódicamente, empleamos los servicios de expertos independientes para realizar estos Test de forma controlada.

- Además, toda la información está almacenada de manera redundante, realizándose periódicamente las correspondientes copias de seguridad que permiten la recuperación de la información.

- En lo que respecta a la seguridad física, nuestros servidores se encuentran localizados en áreas de seguridad protegidas por medios físicos, electrónicos y humanos, con acceso controlado y limitado al personal autorizado.

Asimismo, Bankinter añade a sus páginas web una serie de medidas de seguridad para proteger sus datos y sus operaciones:

- "Pin-Pad" para la introducción de coordenadas. La introducción de coordenadas de la tarjeta de claves del cliente cada vez que opera, se realiza mediante un panel gráfico, sistema que permite eludir el riesgo de los programas conocidos como troyanos, que intentan capturar la información mediante los pulsos del teclado. Al introducir las coordenadas mediante clicks de ratón, se consigue evitar que posibles programas intrusos puedan capturar los datos secretos.

- Desconexión automática de la sesión a los 20 minutos de ausencia de uso. Cuando detectamos que no se ha realizado ninguna consulta u operación en nuestras páginas web durante 20 minutos (30 minutos en el Broker), procedemos a finalizar la sesión y desconectar al cliente. Esta medida evita que, ante un descuido o abandono por su parte, otra persona pueda operar por él en su PC.

-Obligatoriedad del cambio de contraseña en primera conexión. Para prevenir su suplantación, cuando se conecta el cliente por primera vez a nuestras páginas web, le obligamos a cambiar la contraseña. De este modo, nos aseguramos de que sólo él la conoce.

- Bloqueo de usuario ante tres intentos fallidos. El error en la introducción del usuario o la contraseña en tres ocasiones provoca la desactivación de las claves de acceso a ebankinter.com. Contamos con la posibilidad de reactivar estas claves a través de la página web, utilizando su Código de Acceso Personal a Banca Telefónica, añadiendo mayor seguridad a esta reactivación.

- Fecha y hora de última conexión. Le mostramos la fecha y la hora de su última conexión para que pueda detectar si alguien se ha conectado en su nombre en días pasados.

- Mínimo 6 caracteres para usuario y contraseña. El usuario y contraseña de ebankinter.com deben tener como mínimo 6 caracteres, lo que hace más difícil la posibilidad de que alguien las pueda deducir probando opciones.

2. El más llamativo, o el de más novedad, son los intentos de phising a los clientes, en menor medida a los nuestros que a los de otras entidades, quizá debido a que tenemos implementado el sistema de coordenadas desde su inicio.

En Bankinter, somos miembros desde su creación del Grupo de Trabajo de Seguridad del Centro de Cooperación Interbancaria, cuyo primer objetivo fue elaborar un protocolo de actuación frente a incidentes de seguridad por Phishing. Fuimos igualmente pioneros en implementar en nuestro transaccional el "Pin-Pad", mecanismo de seguridad destinado a la introducción segura de coordenadas frente a troyanos del tipo KeyLogger (capturador de pulsaciones de teclado). Asimismo, contamos con una página en Internet con consejos para todos los internautas (sean o no clientes del banco) sobre temas de seguridad en Internet, entre ellos el phising.

Entendemos que lo importante, como en otras facetas de la vida, es asimilar buenos hábitos. Para poder asimilar esto, "buenos hábitos", es necesaria la información y el asesoramiento, y esto sí es una responsabilidad que las entidades bancarias deben asumir junto con otras acciones específicas destinadas a dificultar el éxito del engaño.

4. Básicamente mantener viva nuestra línea de comunicación con clientes, intentándoles transmitir que de su colaboración depende, en gran medida, su propia seguridad.

BANCO DE VALENCIA

"Al fraude se le combate a través de información y formación a los clientes, principalmente"

1. Entre otros modernos sistemas, se ha optado por la encriptación de página de 128 bits con certificado expedido por VeriSing.

El acceso al servicio BV-i se realiza mediante claves personales, clave de usuario y clave de acceso, que son proporcionadas por una entidad certificadora. Todos los datos se encuentran en un servidor seguro y son transmitidos de manera cifrada. Para acceder a ellos y descifrarlos, son necesarias dichas claves. De esta forma, el Banco de Valencia garantiza la total confidencialidad de la información transmitida.

Para operaciones de un importe inferior a 3.000 euros basta con la clave de firma. Sin embargo, la entidad ha decidido dar un paso más en la seguridad y ofrecer la posibilidad de firmar digitalmente las operaciones que efectúe.

Con la firma digital y el envío cifrado de la información, el servicio ofrece tres elementos básicos para la seguridad en cualquier transacción electrónica: Autenticación, que garantiza que realmente es usted quien firma una operación; Integridad, es decir, los datos, al viajar cifrados, no pueden ser modificados; y No repudio en origen, con lo que el emisor que haya firmado una operación no podrá negarlo.

2. De nuestros análisis de los fraudes más comunes existentes en el mercado, destacaríamos el de facilitar las claves por el *modus operandi* de Phishing. Actualmente, y entre otras acciones, se les combate a través de información y formación a los clientes principalmente, con alerta informativa a los usuarios clientes de banca electrónica, y aparece un mensaje de advertencia en la página donde se solicitan las claves del usuario y acceso.

Además, se ha llevado a cabo la implantación de certificado para firma digital, investigación de operaciones fraudulentas, y análisis de los logs.

3. Entre otros, podemos destacar como proveedores tecnológicos en el ámbito de la seguridad a IBM, VeriSign y S21 Sec.

UNICAJA

"La mejor defensa es el ataque a las direcciones IP de donde provienen los intentos de fraude"

1. Protocolos SSL, firewalls, antivirus, IDS, IDP, tarjeta de coordenadas, teclado virtual con la permutación de caracteres.

2. Barridos de puertos, barridos de direcciones IP, búsqueda de vulnerabilidades. Se les ataca cortando las direcciones IP origen de los ataques.

3. Destacan en el ámbito de la seguridad, IBM, Checkpoint, Sun, Cisco.

4. Desarrollo de nuevas formas de autenticación de usuarios antifraude.

Sucursal de Unicaja.

IBERCAJA

"La tecnología más prometedora y factible en estos momentos es la clave pública/privada o PKI"

1. Además del cifrado de comunicaciones, se emplean chequeos de origen, usuario, etc. Nuestras transacciones on line no viajan por redes públicas sino privadas, con grupos cerrados de usuarios, lo que minimiza el riesgo. Respecto a las pasarelas de pago con clientes, se emplean, además, controles de firma electrónica de los mensajes para evitar repudios y, por supuesto, el cifrado.

2. En cuanto al conocido Phishing, se trata de combatir en dos frentes. El primero y más importante, la concienciación del cliente mediante avisos de seguridad en nuestras páginas web. Incluso, se ha hecho el esfuerzo de enviar una carta personalizada a nuestros clientes de banca explicando el procedimiento empleado por los phishers para evitar que nuestros clientes caigan en la trampa.

El segundo frente consiste en la detección temprana y el cierre de los webs donde se recoge la información de los phishers. Se echa de menos como ayuda a este problema la divulgación en los medios de la figura de los *muleros*. No estaría mal concienciar a la gente de que puede acabar en la cárcel por colaborar en un negocio de este tipo. Para combatir a los troyanos, y también en parte el phishing, se han implantado todos los medios habituales: contraseñas con teclados flotantes para evitar keyloggers, tarjetas de coordenadas en operaciones críticas, certificados en todos los servidores, etc.

Además, disponemos de controles internos de detección de operaciones sospechosas que en ocasiones nos han permitido descubrir dichas operaciones antes de que el cliente descubra que tiene un troyano. En este punto, se debe hacer hincapié también en la parte de responsabilidad del cliente, ya que tiene que ser consciente de la importancia de la seguridad de su ordenador.

3. Los más habituales en este campo: Checkpoint, Cisco, Nokia e incluso, en algunas aplicaciones como los IDS, soluciones Open Source.

4. La tecnología más prometedora y factible en estos momentos es la de clave pública/privada o PKI. El único problema que tiene es la complicación administrativa, la falta de un estándar de soporte de la clave privada y de la propia clave y su precio. Sobre todo, por parte del cliente que debería adquirir un lector de smartcard o token determinado. Sin embargo, tarde o temprano, todo habrá que montarlo utilizando estas tecnologías desde las identificaciones de los clientes hasta la comunicación entre ordenadores.

CAJA SUR

"Aunque hasta ahora ha habido una nula incidencia, las amenazas son crecientes"

1. Nuestro servicio de banca por Internet 'CajaSur en línea' se presta en colaboración tecnológica con CECA, quien nos proporciona los servicios básicos de infraestructura incluyendo los concernientes a la seguridad. Desde el punto de vista de un usuario, la seguridad se basa en un mecanismo de identificación multinivel con bloqueo por reintentos erróneos, consistente en un código de usuario y clave para acceder al sistema, junto a una tarjeta de coordenadas para autorizar las transacciones económicas. Existe también un control mediante firmas digitales para atender las situaciones donde se requiere la autorización de varios intervinientes y un sistema de niveles de usuario para limitar el importe máximo de las transacciones.

Sin entrar en detalles, desde un punto de vista técnico nuestra plataforma garantiza la seguridad en las transacciones (su integridad, confidencialidad, disponibilidad y no repudio) mediante la identificación de los usuarios, el uso de certificados digitales en lo servidores, el cifrado de las comunicaciones, las técnicas de seguimiento de sesiones para garantizar la trazabilidad de las transacciones y todo un conjunto de controles sobre la plataforma hardware y software para prevenir los intentos de ataque y evitar su éxito.

En cuanto a la pasarela de pagos, si bien parte de las medidas de seguridad que se comparten con las de la plataforma de banca on line, existen una serie de procedimientos estandarizados propuestos por las principales marcas de tarjetas a los que nosotros nos hemos adherido tan pronto como han estado disponibles. Se trata en este caso de los estándares VISA 3DSecure y Mastercard SecureCode que facilitan la identificación de los intervinientes en una transacción por Internet para garantizar el no repudio. Otra alternativa que ofrecemos a nuestros clientes en este área, y que ha tenido una gran aceptación, es la utilización de tarjetas virtuales por importe prefijado y de un solo uso, aumentando así la confidencialidad y evitando la posible captura de datos de tarjetas en páginas web poco fiables.

2. Si bien podemos transmitir un mensaje tranquilizador, habida cuenta de la hasta ahora nula incidencia en nuestros sistemas de ataques relacionados con la banca por Internet, resulta evidente que en este terreno cada día son más las amenazas a que debemos enfrentarnos y debemos trabajar en la constante mejora de las técnicas de defensa.

En un frente distinto, en lo concerniente a fraudes por Internet y seguridad en las transacciones, estamos en estrecha colaboración con el resto del sistema financiero español y muy especialmente a través del Centro de Cooperación Interbancaria, tratando de plantear una defensa conjunta contra aquellos casos en que un ataque contra una entidad requiera los servicios de una tercera para obtener los frutos de dicho fraude.

3. Nuestros servicios de banca por Internet se ofrecen en colaboración con CECA, que es uno de nuestros principales proveedores tecnológicos en este área y especialmente en lo concerniente a la seguridad. También contamos con otras empresas especializadas en áreas específicas, como VeriSign en cuanto a la certificación de servidores o a los sistemas de prevención y reacción ante intentos de fraude.

4. En el terreno de la seguridad, todas las medidas que se adopten deben estar en constante revisión y evolución. Como casos concretos, cabe destacar la reciente incorporación de teclados virtuales y el cifrado de las claves de usuario antes de su transmisión para combatir los actuales intentos de ataque mediante técnicas de phishing.

Otras medidas que vamos a implantar y cuya aplicación queda a decisión del propio usuario, son la limitación a una única localización para operar con banca electrónica (en aquellos casos donde sea aplicable, fijando la dirección IP de la máquina utilizada), o el sistema de alertas por SMS para operaciones de riesgo.

A más largo plazo, empezamos a evaluar la utilización de certificados digitales personales para la identificación de los clientes, muy especialmente atendiendo a la próxima implantación del DNI digital y a las posibilidades que éste nos pueda ofrecer. ☒