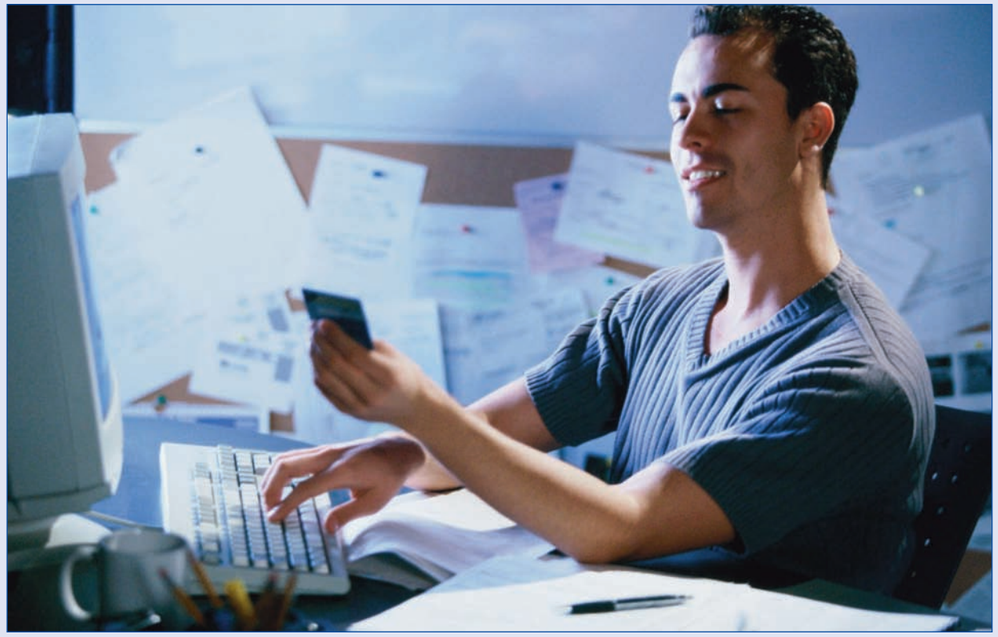

Hay que desconfiar de los supuestos correos electrónicos que nos lleguen del banco solicitándonos información privada.

DESFALCOS POR ‘PHISHING’

NO todo son ventajas en el mundo digital, también hay sofisticados delitos que han surgido al albur de las nuevas tecnologías. Diferentes formas de robar aprovechando el anonimato que ofrece la Red. Una de ellas es el ‘phishing’.

LUIS USERA

EL “phishing” es una práctica que trae de cabeza a los responsables de seguridad de los principales bancos que ven cómo van aumentando los intentos de robar a sus clientes utilizando la imagen corporativa del banco.

Este timo consiste en duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la falsa. Normalmente se utiliza con fines delictivos duplicando sitios web de bancos conocidos y enviando indiscriminadamente correos para que se visiten para ellos para que actualicen los datos de acceso a la entidad.

El procedimiento consiste en aprovechar el XXS (Cross-Site Scripting), para modificar el contenido de la Web que el usuario visualiza en su navegador.

El método. El usuario recibe un “e-mail” de un banco, entidad financiera o tienda de Internet en el que se le explica que por motivos de seguridad, mantenimiento, mejora en el servicio, confirmación de identidad o cualquier otra razón debe actualizar los datos de su cuenta. El mensaje imita exactamente el diseño (logotipo, firma, etc.) utilizado por la entidad para comunicarse con sus clientes.

El mensaje puede incluir un formulario para enviar los datos requeridos, aunque lo más habitual es que adjunte un enlace a una página donde actualizar la información personal.

Esta página, como se mencionaba anteriormente, es igual que la legítima de la entidad –algo sencillo copiando el código fuente (HTML)– y su dirección (URL) es parecida e incluso puede ser idéntica gracias a un fallo de algunos navegadores.

Si se rellenan y se envían los datos de la página las víctimas caen directamente en manos del estafador, quien puede utilizar su identidad para operar en Internet.

Ataque a la ingeniería social. En muchos casos se trata de una forma de “spam” –correos electrónicos no deseados– especialmente perniciosa, pues no sólo satura los buzones de basura, sino que pone en peligro la integridad de la información sensible del usuario con graves consecuencias.

En ocasiones, el término “phishing” se dice que es la contracción de “password harvesting fishing” –cosecha y pesca de contraseñas–, aunque esto probablemente es un acrónimo retroactivo.

De forma más general, el nombre “phishing” también se aplica al acto de adquirir, de forma fraudulenta y mediante engaño, información personal como contraseñas o detalles de una tarjeta de crédito, números de la seguridad social, documentos de identidad haciéndose pasar por alguien digno de confianza con una necesidad verdadera de tal información en un “e-mail” parecido al oficial, un mensaje instantáneo o cualquier otra forma de comunicación. Es una forma de ataque a la ingeniería social.

Este término fue creado a mediados de los años 90 por los “crackers” que intentaban robar las cuentas de AOL. Un atacante se presentaba como empleado de AOL y enviaba un mensaje inmediato a una víctima potencial. El mensaje pedía que ésta le revelara su contraseña, con variadas excusas como la verificación de la cuenta o confirmación de la información de la facturación. Una vez que la víctima notificaba la contraseña, el atacante podría tener acceso a su cuenta y utilizarla para cualquier otro propósito.

Contraofensiva. El Anti-Phishing Working Group, organización creada en EE.UU. para combatir este fraude, asegura que el número y la sofisticación de esta estafa se está incrementando de forma dramática y que “aunque la banca ‘on line’ y el comercio electrónico son muy seguros, como norma general hay que ser muy cuidadoso a la hora de facilitar información personal a través de Internet”.

En España algunos bancos han realizado campañas avisando a sus clientes de que el banco nunca se pondrá en contacto con ellos por correo electrónico para solicitarles datos privados

El “phishing” es un fraude que trae de cabeza a los responsables de seguridad de los principales bancos

Víctimas españolas

Si nos centramos en la evolución de este fenómeno en nuestro país, los datos son bastante alarmantes. La Comisión de Seguridad de la Asociación de Internautas detectó en 2006 nada menos que 1.184 ataques de phishing frente a los 293 descubiertos en 2005, lo que ha supuesto un crecimiento del 290 por ciento. De este total, 705 suplantaban a entidades financieras. Los fraudes de SCAM -ofertas falsas de trabajo- alcanzaron la cifra de 344 y por último, 135 fueron sitios web trampa de páginas verdaderas, o sitios para descargas *on line* de móviles.

La entidad financiera más atacada ha sido el BBVA, con 55 ataques; seguida de Bancaja, con 51, y Caja Madrid, con 50. A más distancia se encuentra Banesto, con 22 ataques; Banco Popular, con diez; Santander, con 11 y La Caixa, con siete. Entre las empresas no financieras destacan Ebay, con 20 ataques, y Pay Pal, con seis.

como su usuario o contraseña, por lo que siempre que reciban una solicitud semejante deben denunciarlo. Pese a estas campañas sigue habiendo gente que "pica" y, de hecho, este tipo de prácticas se fundamentan en el cálculo de probabilidades. Aunque cada vez haya más gente que sabe qué es el "phishing" y por lo tanto van a ignorar todos sus intentos, siempre habrá un porcentaje de personas con menos información que son potenciales clientes para ellos.

Aunque también hay que decir que la entidades bancarias son cada día más rápidas a la hora de cerrar las web falsas. A principios de 2005 la vida media de una web falsa era de siete a doce días de vida. En los últimos meses la seguridad de la banca esta evolucionado bastante y la vida media de estas páginas es de veinticuatro horas o dos días, dependiendo la entidad. ■

Miguel Pérez Subías [Presidente de la Asociación de Usuarios de Internet. Miembro del Observatorio del Notariado para la Sociedad de la Información]

"LA INCIDENCIA DEL 'PHISHING' EN ESPAÑA AUMENTA Y SE SOFISTICA AÑO A AÑO"

L. U.

–¿Qué es exactamente el "phishing"?

–Es el término utilizado para un fraude en Internet consistente en falsificar una página web y lanzar un e-mail masivo e indiscriminado de reclamo para ver si el receptor de ese correo "pica" y entra en la página falsa creyendo que es la original y suministra sus credenciales de acceso, las cuales caen inmediatamente en manos del defraudador.

–¿Se ha realizando algún estudio para conocer la penetración de este fraude en nuestro país?

–La incidencia del "phishing" en España aumenta y se sofistica año a año. Todas las entidades financieras han sido objeto de ataques de "phishing" sin excepción.

Todas las entidades financieras españolas han sido objeto de ataques de 'phishing' sin excepción

–¿Qué acciones están desarrollando los bancos?

–Los bancos están aplicando dos tipos de medidas: aquellas que sofistican la introducción de claves para que éstas no sean estáticas y no se vuelquen desde el teclado y otras que utilizan elementos de seguridad complementarios mediante juegos de claves en papel o avisos al móvil de las transacciones importantes, por ejemplo.

–¿Los usuarios tienen algún modo de prevenir estas estafas?

–Sí, el principal exigiendo a las aplicaciones sistemas de seguridad avanzados a ser posible a través de otras redes, como por ejemplo el teléfono móvil.

En nuestra opinión el móvil puede actuar como elemento de seguridad, tal y como sucede con la tarjeta de crédito para sacar dinero en los cajeros, ya que la información va por redes distintas; puede ser de gran utilidad para gestionar claves dinámicas sin que el usuario tenga que instalar programas en su equipo u ordenador, de esta forma la seguridad siempre viaja con el individuo y no reside en el ordenador a través del cual accedo a mi banco o tienda "on line".

–¿Hay nuevas estafas ante las que debamos estar prevenidos?

–En estos momentos las conexiones sin hilos como el "wi-fi" son un nuevo canal de fraudes ya que es posible, cuando no se cifran los datos, que cualquier persona con un ordenador situado en las proximidades de una casa u oficina pueda acceder a la información que se transmite.

Además, se están utilizando sitios alternativos, como por ejemplo los dedicados a fotos y blogs. Los usuarios reciben un correo electrónico o un mensaje instantáneo, que asegura que se lo envía un amigo que desea mostrarles las fotos de un acontecimiento reciente, tales como vacaciones o una fiesta de cumpleaños. El mensaje contiene el enlace a un sitio falso, que captura la identificación (usuario y contraseña) de la persona que accede a él y luego los envía al sitio verdadero, de tal modo que la víctima ignora en todo momento que sus datos han sido robados antes de llegar a la web auténtica. ■

CARMEN TOMÁS

Más internacionales

LOS españoles no estamos precisamente en los puestos de cabeza de los países del mundo en número de transacciones de todo tipo realizadas por Internet. Pero, en este asunto como otros a los que hemos llegado tarde, vamos haciendo nuestros pinitos. Ya es difícil en las diversas ciudades de España encontrar a alguien que no haya hecho alguna compra o haya accedido a su cuenta por la Red. Hoy sacar un billete de avión, tren o autobús, unas entradas para cualquier espectáculo o comprar un libro o un disco es cada vez más habitual.

Estamos, por supuesto, lejos de otros países. Creo que la razón fundamental no es tanto la falta de confianza, que lo será en algunos casos, como la aún escasa popularización del uso de Internet y del coste elevado del servicio en España. Sin duda, ha habido una falta clara de impulso por parte de las distintas administraciones. Sin embargo, estoy convencida de que las compañías, especialmente Telefónica, no han realizado el esfuerzo necesario para hacer más accesibles y más baratas las líneas de Internet. Claro que la confianza es todavía un factor que influye en muchos ciudadanos. Dejar los datos de la tarjeta, usar unas claves son desgraciadamente moneda bastante común. No obstante, también en esto, aunque tarde, los españoles se están incorporando al mundo de las nuevas tecnologías. Hay mucho camino por recorrer. Y así como las compañías se han afanado en propagar el uso del móvil no han hecho lo mismo con las líneas de la Red. Las administraciones deberían ya apoyar e impulsar que el uso de Internet se abarate y que los ciudadanos puedan acceder a esta riquísima fuente de información y de comodidad.

Para expertos juristas los motivos de este retraso hay que buscarlos en causas sociales y culturales. Es muy común en España ver aún las oficinas bancarias, sobre todo algunas, abarrotadas de gente en fechas cruciales y a horas determinadas.

Sin embargo, estudios recientes aseguran que en lo relativo al comercio electrónico las transacciones aumentan a un ritmo de vértigo. Está, por tanto, aumentando la confianza de los españoles en estos sistemas. Aquí la seguridad jurídica no juega un papel tan preponderante como todo lo que tiene que ver con las relaciones bancarias o la compra de acciones o el pago a proveedores. Puede ser por tanto ésta, la de las compras por Internet, una vía muy útil para que los españoles vayan entrando por el camino de la confianza y de la comodidad que supone también realizar "on line" todo lo que tenga que ver con nuestro dinero.

> **"Estudios recientes aseguran que en lo relativo al comercio electrónico las transacciones aumentan a un ritmo de vértigo. Está, por tanto, aumentando la confianza de los españoles en estos sistemas"**

Sin duda hay que ofrecer más garantías. En este sentido, la transposición de la directiva comunitaria relativa a la comercialización de servicios financieros puede ser el marco que ofrezca a los consumidores españoles la tranquilidad que le falta. No cabe duda de que el abaratamiento de costes que produce las transacciones "on line" debería ser razón suficiente para entrar en el mundo de las nuevas tecnologías, habrá más competencia y eso siempre es bueno para el consumidor. Crear seguridad y cambiar hábitos depende de todos.

Carmen Tomás es periodista.