MÁS ALLÁ DEL *PHISHING* EN LOS ORDENADORES[1]

Mª Nieves Pacheco Jiménez
Prof. Contratada Doctora
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Fecha de publicación: 7 de octubre de 2015

1. Introducción

El presente estudio sigue la estela de los artículos publicados en CESCO sobre servicios de pago, transacciones vía Internet y fraude online. Concretamente es la continuación del estudio publicado en julio pasado titulado "Responsabilidad cuasi objetiva del proveedor de servicios de pago por las transferencias fraudulentas", que analizaba la SAP Madrid de 4 de mayo de 2015 (JUR 2015/151311) cuyo fallo, basado en los artículos 30 y siguientes de la Ley de Servicios de Pago (Ley 16/2009, de 13 de noviembre), fue la condena a la entidad bancaria a reembolsar a su cliente el importe que sumaban las transferencias realizadas de forma fraudulenta y sin la autorización del demandante mediante una técnica conocida como *phishing*.

Phishing es una forma de abuso informático que utiliza *spam*, mensajes de correo electrónico o sitios web falsos, suplantando en este caso la identidad de la fuente fiable (v. gr, Banco), con la finalidad de adquirir la información confidencial sobre contraseñas de cuentas bancarias o cualquier otra información. Una de las modalidades más peligrosas del *phishing* es el *pharming*. Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS "Domain Name System" o Sistema de Nombres de Dominio), que se encarga de convertir una dirección tecleada en el navegador a una dirección IP numérica, para conducir al usuario a una página web falsa, en apariencia idéntica a la web de confianza pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios. El fraude se produce a través de ejemplares de *malware* diseñados para modificar el sistema de resolución de nombres local ubicado en un fichero denominado HOSTS

[1] Trabajo realizado en el marco del Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia (Subprograma Estatal de Generación de Conocimiento) otorgado al Grupo de investigación y centro de investigación CESCO, *Mantenimiento y consolidación de una estructura de investigación dedicada al Derecho de consumo*, dirigido por el Prof. Ángel Carrasco Perera de la UCLM, Ref.: DER2014-5606-P.

(usado por el sistema operativo para guardar la correspondencia entre dominios de Internet y direcciones IP)[2].

Los principales daños provocados por el *phishing* son: robo de identidad y datos confidenciales de los usuarios; pérdida de productividad; consumo de recursos de las redes corporativas (v. gr., ancho de banda, saturación del correo, etc.).

La Oficina de Seguridad del Internauta (OSI) ha elaborado una serie de excusas frecuentes que aparecen en los correos de *phishing* para justificar la necesidad de facilitar los datos personales, a saber: problemas de carácter técnico; recientes detecciones de fraude y urgente incremento del nivel de seguridad; nuevas recomendaciones de seguridad para prevención del fraude; cambios en la política de seguridad de la entidad; promoción de nuevos productos; premios, regalos o ingresos económicos inesperados; accesos o usos anómalos a tu cuenta; inminente desactivación del servicio; falsas ofertas de empleo[3].

2. Casos recientes de *phishing*

Según la Memoria anual de reclamaciones del Banco de España de 2012, las solicitudes recibidas por pagos fraudulentos a través de Internet suponían un 0,3% del total de las recibidas. Y esta cifra sigue aumentando paulatinamente… El pasado año la OSI alertaba de campañas de *phishing* contra varias entidades bancarias (Banco Santander, Banco Popular, Bankia, ING Direct) con el objetivo de engañar a los usuarios para que éstos hiciesen clic en un enlace que les redirigía a una web maliciosa que suplantaba la identidad del Banco para así capturar sus claves y datos.

Aprovechado esos avisos, la OSI realizaba recomendaciones[4] para evitar ser víctima de este tipo de fraudes: no abrir correos de usuarios desconocidos o que no se hayan solicitado, eliminándolos directamente; no contestar en ningún caso a dichos correos; tener la máxima precaución al seguir enlaces sospechosos en correos aunque sean de contactos conocidos, así como al descargar ficheros adjuntos de correos. Asimismo,

[2] *Vid*. http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

[3] *Vid*. https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

[4] *Vid*. http://www.osi.es/es/actualidad/avisos/2014/01/campana-de-phishing-al-banco-santander
http://www.osi.es/es/actualidad/avisos/2014/03/detectada-campana-de-phishing-que-suplanta-al-banco-popular
http://www.osi.es/es/actualidad/avisos/2014/04/detectada-nueva-oleada-de-correos-fraudulentos-que-se-hacen-pasar-por-bank
http://www.osi.es/es/actualidad/avisos/2014/04/campana-de-phishing-contra-ing-direct

recordaba los consejos que generalmente facilitan los Bancos en su sección de seguridad: cerrar todas las aplicaciones antes de acceder a la web del Banco; escribir directamente la url en el navegador (en vez de llegar a ella a través de enlaces disponibles desde páginas de terceros o en correos electrónicos); asegurarse de que la web comienza por https://, para que los datos viajen cifrados por la Red; verificar la legitimad del sitio web; no acceder al servicio de Banca online desde ordenadores públicos; desconfiar de las solicitudes de datos personales a través del correo electrónico del Banco.

De conformidad con un estudio actual realizado por Karpersky Lab y B2B International, realizar movimientos financieros a través de las webs de los Bancos se ha convertido en un hábito entre los usuarios, pero un gran número de ellos (el 55%) se siente vulnerable cuando realiza transacciones financieras en la Red, sintiéndose más seguros empleando sus ordenadores antes que dispositivos móviles[5], aunque sólo un 19% de los usuarios no hacen nada por proteger sus datos financieros online.

Pero el *phishing* no se agota en los Bancos, la OSI también ha alertado de este fraude en la Agencia Tributaria, a través de correos electrónicos que utilizaban como pretexto una modificación en la declaración del Impuestos de Sociedades instando a descargarse una aplicación de nombre TAPE, que en realidad era un *malware* que se instalaba en los ordenadores de los usuarios y, al ejecutarse, cifraba los archivos para que fuesen inaccesibles y así solicitar el pago de un rescate[6]. Asimismo, en pasarelas de pago online (v. gr., PayPal, Mastercard[7], Visa) mediante excusas como cambio de normativa del servicio, cierre incorrecto de la sesión de usuario, mejoras en las medidas de seguridad o detección de intrusión en los sistemas de seguridad. Y también en páginas de compra-venta y subastas como Amazon o eBay, o en servicios de almacenamiento en la nube (v. gr. Google Drive, Dropbox).

---

[5] El 85% de los españoles encuestados usan sus ordenadores o portátiles para realizar pagos online, el 56% usa sus *tablets*, el 46% sus *smartphones* y sólo el 9% de los propietarios de una *smart* TV admite que la utiliza para este tipo de operaciones. (*Vid*. http://globbsecurity.com/usuarios-banco-online-vulnerables-34760/).

[6] Los asuntos identificados eran los siguientes: Actualizado: Agencia Tributaria. Es importante actualizar: Agencia Tributaria. Notificación: Agencia Tributaria. Prestar atención: Agencia Tributaria.
Vid. https://www.osi.es/es/actualidad/avisos/2015/03/campana-de-correos-fraudulentos-que-suplantan-la-agencia-tributaria

[7] Concretamente, en enero del pasado año, se advirtió de una campaña masiva de correos fraudulentos haciéndose pasar por la asistencia técnica de Mastercard con el objetivo de engañar al usuario simulando ser una actualización del reglamento de la UE (conteniendo un fichero adjunto de nombre Actualización.zip) para poder utilizar la tarjeta de crédito, con la finalidad de que el propio usuario descargase un formulario y rellenase datos tales como nombre del titular, número de tarjeta, fecha de vencimiento, pin, etc.
Vid. http://www.osi.es/es/actualidad/avisos/2014/01/campana-masiva-de-phishing-de-mastercard

3. *Phishing* en *smartphones* y *tablets*

Aunque generalmente asociamos el *phishing* con el correo electrónico, cada vez es más frecuente el fraude a través de otros medios como los mensajes intercambiados a través de aplicaciones de mensajería instantánea o mensajes en redes sociales[8]. De hecho, una de las principales razones por las que estos ataques son tan eficientes es la constante evolución y sofisticación de las técnicas y herramientas del *phishing*[9]. La ciberdelicuencia tiene, pues, un último objetivo, los *smartphones* y *tablets*, basándose en la proliferación de acciones que se pueden realizar desde estos dispositivos y la facilidad que supone en pantallas de dimensiones más pequeñas distinguir páginas web reales de falsas.

Según el estudio "Mobile malware: A network view" realizado en 2015 por Alcatel-Lucent, más de 1500 millones de *smartphones* están conectados a Internet en el mundo (alrededor del 60% de la navegación en Internet se produce a través de ellos); y al menos unos 16 millones están infectados[10]. Es más, los expertos señalan que el número

[8] Según una investigación realizada por Kaspersky Lab, en 2013 más del 35% de los ataques *phishing* iban dirigidos a usuarios de redes sociales. La herramienta *antiphishing* de los productos de Kaspersky detectó más de 600 millones de accesos a páginas *phishing* que se hacían pasar por redes sociales conocidas; un 22% de los casos eran páginas falsas de Facebook.
Vid. https://blog.kaspersky.es/por-que-es-rentable-el-phishing-y-como-funciona/4428/

[9] *Vid*. https://blog.kaspersky.es/por-que-es-rentable-el-phishing-y-como-funciona/4428/

[10] *Vid*. http://tecnologia.elpais.com/tecnologia/2015/09/15/actualidad/1442327365_650658.html
https://www.alcatel-lucent.com/solutions/malware-reports
Concretamente, la plataforma Android es la más afectada por el *malware*. Y ello porque permite instalar aplicaciones de terceros que, a su vez, instalan troyanos; a diferencia de los iPhone, cuyas aplicaciones están sólo disponibles a través de Apple. En 2014, los cinco *malware* más importantes detectados en Android fueron:
- Android.Adware.Uapush.A (45.57% del total)
- Android.Trojan.Ackposts.a (17.08% del total)
- Android.MobileSpyware.SmsTracker (14.67% del total)
- Android.Adware.Counterclank (9.56% del total)
- Android.MobileSpyware.SpyMob.a (1.87% del total)

No obstante, hace unas semanas un *malware* conocido como "XcodeGhost" ha afectado a aplicaciones desarrolladas para Mac OS X e iOS (iPhone y iPad), entre ellas algunas tan conocidas como: Angry Birds 2.1.1, PDFReader, PDFReader Free, Wallpapers10000, WinZip, WinZip Sector, WinZip Standard. El propósito del *malware* sería robar información personal, bancaria, credenciales de redes sociales, etc. de los dispositivos infectados. Aunque Apple ya ha retirado de la AppStore todas las aplicaciones afectadas, los usuarios que hayan instalado alguna de las aplicaciones listada en la sección de recursos afectados, deberían hacer y por este orden: 1º) Desinstalar las aplicaciones de la lista que se encuentren instaladas en el dispositivo. 2º) Modificar las credenciales (nombre de usuario y contraseña) de los servicios que hayamos usado después de haber instalado la aplicación (o aplicaciones) comprometida. En caso de duda, modificar las credenciales de los servicios que se usen desde el dispositivo afectado.
Vid. http://www.osi.es/es/actualidad/avisos/2015/09/el-malware-vuelve-colarse-en-la-apple-store

de virus para estos dispositivos, fácilmente manipulables, empieza a equipararse al de los ordenadores convencionales. Tal y como se apunta desde Karpersky (especialistas en antivirus y software de seguridad para PCs, MAC, Móviles, Servidores, Tabletas y Empresas), existe un exceso de confianza con los móviles ya que no hay percepción de riesgo, a diferencia de la consciencia de seguridad que se va adquiriendo en los ordenadores. Existen numerosas formas de contagio, a saber: a) descarga de aplicaciones maliciosas[11]; b) anuncios que aparecen insistentemente en la pantalla tras visitar ciertas páginas[12]; c) correos electrónicos que proceden de falsos Bancos o redes sociales[13]; d) conexión a través de una "free Wifi" falsa[14] que acceda a Facebook, banco o correo electrónico.

4. Conclusión

Las facilidades que nos aportan las nuevas tecnologías tienen su contrapunto en la continua exposición a ataques de ciberdelincuentes a través de múltiples y variados mecanismos (entre ellos el *phishing*). Para evitar posibles fraudes, es imprescindible que los usuarios conozcamos la existencia de esas técnicas (es evidente que disponer de información al respecto nos ofrece cierta ventaja) y estar alerta al recibir emails sospechosos o que induzcan al miedo (por ejemplo, un aviso de movimiento no autorizado en la cuenta corriente), evitando hacer clic en ellos sin pensar en lo que realmente pueden ser. En este punto es fundamental actualizar nuestro software anti-virus, anti-s*pyware* y *firewall* para evitar potenciales ataques, así como seguir las recomendaciones de la OSI anteriormente señaladas. No obstante, si hemos sucumbido a la curiosidad o al miedo y hemos terminado haciendo clic en un enlace de *phishing*, no todo está perdido mientras no hayamos introducido información personal; y, en el peor de los casos, si así lo hemos hecho, lo más conveniente es cambiar inmediatamente las contraseñas e informar oportunamente a la fuente fiable (entidad bancaria, organismo público, etc).

[11] Este tipo de *software* malicioso se suele descargar en tiendas no oficiales (generalmente juegos gratuitos o versiones de aplicaciones comerciales). Tienen apariencia de programas conocidos y permiten a los delincuentes robar datos personales, de localización, mandar troyanos o suscribirnos a teléfonos Premium de cobro.

[12] Denominado "adware": al visitar ciertas páginas web se instala automática alguna publicidad que ya no se puede dejar de ver repetidamente; los delincuentes se llevan una comisión de estos anuncios.

[13] Estos correos incluyen las típicas imágenes falsas de bancos o redes sociales, redirigiendo a una réplica falsa de la web para hacerse con las claves de la cuenta real del usuario.

[14] Suelen ubicarse en lugares públicos como aeropuertos o estaciones. Una vez se accede, el móvil se convierte en una puerta abierta a todo tipo de *malware*.