


Phishing

Phishing es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea^[1] o incluso utilizando también llamadas telefónicas.^[2]

Dado el creciente número de denuncias de incidentes relacionados con el *phishing*, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas.



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Éste es un ejemplo de un intento de *phishing*. Haciéndose pasar por un correo electrónico oficial, trata de engañar a los clientes del banco para que den información acerca de su cuenta con un enlace a la página del *phisher*.

Historia del *phishing*

Origen del término

El término *phishing* proviene de la palabra inglesa "*fishing*" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo".^[3] A quien lo practica se le llama *phisher*.^[4] También se dice que el término *phishing* es la contracción de *password harvesting fishing* (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo, dado que la escritura 'ph es comúnmente utilizada por hackers para sustituir la f, como raíz de la antigua forma de hacking telefónico conocida como phreaking.^[5]

La primera mención del término *phishing* data de enero de 1996. Se dio en el grupo de noticias de *hackers alt.2600*,^[6] aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias *hacker 2600 Magazine*.^[7] El término *phishing* fue adoptado por quienes intentaban "pescar" cuentas de miembros de AOL.

Phishing en AOL

Quienes comenzaron a hacer *phishing* en AOL durante los años 1990 solían obtener cuentas para usar los servicios de esa compañía a través de números de tarjetas de crédito válidos, generados utilizando algoritmos para tal efecto. Estas cuentas de acceso a AOL podían durar semanas e incluso meses. En 1995 AOL tomó medidas para prevenir este uso fraudulento de sus servicios, de modo que los *crackers* recurrieron al *phishing* para obtener cuentas legítimas en AOL.

El *phishing* en AOL estaba estrechamente relacionado con la comunidad de *warez* que intercambiaba software falsificado. Un *cracker* se hacía pasar como un empleado de AOL y enviaba un mensaje instantáneo a una víctima potencial. Para poder engañar a la víctima de modo que diera información confidencial,^[8] el mensaje podía contener textos como "verificando cuenta" o "confirmando información de factura". Una vez el usuario enviaba su contraseña, el atacante podía tener acceso a la cuenta de la víctima y utilizarla para varios propósitos criminales, incluyendo el

spam. Tanto el *phishing* como el *warezing* en AOL requerían generalmente el uso de programas escritos por crackers, como el AOLHell.

En 1997 AOL reforzó su política respecto al *phishing* y los *warez* fueron terminantemente expulsados de los servidores de AOL. Durante ese tiempo el *phishing* era tan frecuente en AOL que decidieron añadir en su sistema de mensajería instantánea, una línea de texto que indicaba: «no one working at AOL will ask for your password or billing information» («nadie que trabaje en AOL le pedirá a usted su contraseña o información de facturación»). Simultáneamente AOL desarrolló un sistema que desactivaba de forma automática una cuenta involucrada en *phishing*, normalmente antes de que la víctima pudiera responder. Los *phishers* se trasladaron de forma temporal al sistema de mensajería instantáneo de AOL (AIM), debido a que no podían ser expulsados del servidor de AIM. El cierre obligado de la escena de *warez* en AOL causó que muchos *phishers* dejaran el servicio, y en consecuencia la práctica.^[9]

Intentos recientes de *phishing*

Los intentos más recientes de *phishing* han tomado como objetivo a clientes de bancos y servicios de pago en línea. Aunque el ejemplo que se muestra en la primera imagen es enviado por *phishers* de forma indiscriminada con la esperanza de encontrar a un cliente de dicho banco o servicio, estudios recientes muestran que los *phishers* en un principio son capaces de establecer con qué banco una posible víctima tiene relación, y de ese modo enviar un correo electrónico, falseado apropiadamente, a la posible víctima.^[10] En términos generales, esta variante hacia objetivos específicos en el *phishing* se ha denominado *spear phishing* (literalmente *pesca con arpón*). Los sitios de Internet con fines sociales también se han convertido en objetivos para los *phishers*, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad.^[11] Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques *phishing* en redes sociales.^[12] A finales de 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace logrando redireccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios.^[13]

Técnicas de *phishing*

La mayoría de los métodos de *phishing* utilizan la manipulación en el diseño de el correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por *phishers*; por ejemplo en esta URL: <http://www.nombredetubanco.com/ejemplo>, en la cual el texto mostrado en la pantalla no corresponde con la dirección real a la cual conduce. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares^[14]). Por ejemplo, el enlace <http://www.google.com@members.tripod.com/> puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente). Este método ha sido erradicado desde entonces en los navegadores de Mozilla^[15] e Internet Explorer.^[16] Otros intentos de *phishing* utilizan comandos en JavaScripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

En otro método popular de *phishing*, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como Cross Site Scripting) los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos

necesarios.

Otro problema con las URL es el relacionado con el manejo de Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios (por ejemplo *dominio.com* se ve similar a *dominio.com*, aunque en el segundo las letras "o" hayan sido reemplazadas por la correspondiente letra griega *ómicron*, "o"). Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones. A pesar de la publicidad que se ha dado acerca de este defecto, conocido como IDN spoofing^[17] o ataques homógrafos,^[18] ningún ataque conocido de phishing lo ha utilizado.

Lavado de dinero producto del *phishing*

Actualmente empresas ficticias intentan reclutar teletrabajadores por medio de correo electrónicos, chats, irc y otros medios, ofreciéndoles no sólo trabajar desde casa sino también otros jugosos beneficios. Aquellas personas que aceptan la oferta se convierten automáticamente en *víctimas* que incurren en un grave delito sin saberlo: el blanqueo de dinero obtenido a través del acto fraudulento de *phishing*.

Para que una persona pueda darse de alta con esta clase de «empresas» debe rellenar un formulario en el cual indicará, entre otros datos, su número de cuenta bancaria. Esto tiene la finalidad de ingresar en la cuenta del *trabajador-víctima* el dinero procedente de estafas bancarias realizadas por el método de *phishing*. Una vez *contratada*, la víctima se convierte automáticamente en lo que se conoce vulgarmente como *mulero*.

Con cada acto fraudulento de *phishing* la víctima recibe el cuantioso ingreso en su cuenta bancaria y la empresa le notifica del hecho. Una vez recibido este ingreso, la víctima se quedará un porcentaje del dinero total, pudiendo rondar el 10%-20%, como comisión de trabajo y el resto lo reenviará a través de sistemas de envío de dinero a cuentas indicadas por la *seudo-empresa*.

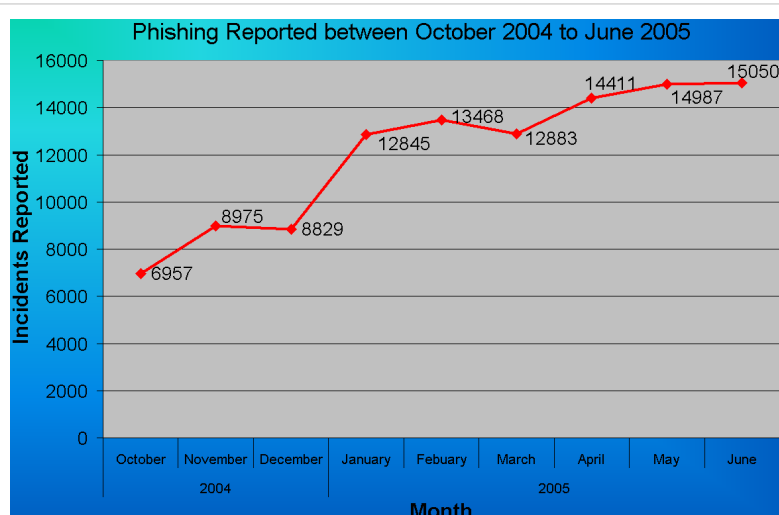
Dado el desconocimiento de la víctima (muchas veces motivado por la necesidad económica) ésta se ve involucrada en un acto de estafa importante, pudiendo ser requerido por la justicia previa denuncia de los bancos. Estas denuncias se suelen resolver con la imposición de devolver todo el dinero sustraído a la víctima, obviando que este únicamente recibió una comisión.

Fases

- En la primera fase, la red de estafadores se nutre de usuarios de chat, foros o correos electrónicos, a través de mensajes de ofertas de empleo con una gran rentabilidad o disposición de dinero (*hoax* o *scam*). En el caso de que caigan en la trampa, los presuntos intermediarios de la estafa, deben rellenar determinados campos, tales como: Datos personales y número de cuenta bancaria.
- Se comete el *phishing*, ya sea el envío global de millones de correos electrónicos bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria (*phishing*) o con ataques específicos.
- El tercer paso consiste en que los estafadores comienzan a retirar sumas importantes de dinero, las cuales son transmitidas a las cuentas de los intermediarios (*muleros*).
- Los intermediarios realizan el traspaso a las cuentas de los estafadores, llevándose éstos las cantidades de dinero y aquéllos —los intermediarios— el porcentaje de la comisión.

Daños causados por el *phishing*

Los daños causados por el *phishing* oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Este tipo de robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal a los *phishers*, incluyendo números de tarjetas de crédito y números de seguridad social. Una vez esta información es adquirida, los *phishers* pueden usar datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.



Una gráfica muestra el incremento en los reportes de phishing desde octubre de 2004 hasta junio de 2005.

Se estima que entre mayo de 2004 y mayo de 2005, aproximadamente 1,2 millones de usuarios de computadoras en los Estados Unidos tuvieron pérdidas a causa del *phishing*, lo que suma a aproximadamente \$929 millones de dólares estadounidenses.^[19] Los negocios en los Estados Unidos perdieron cerca de 2000 millones de dólares al año mientras sus clientes eran víctimas.^[20] El Reino Unido también sufrió el alto incremento en la práctica del *phishing*. En marzo del 2005, la cantidad de dinero reportado que perdió el Reino Unido a causa de esta práctica fue de aproximadamente £12 millones de libras esterlinas.^[21]

Anti-Phishing

Existen varias técnicas diferentes para combatir el *phishing*, incluyendo la legislación y la creación de tecnologías específicas que tienen como objetivo evitarlo.

Respuestas organizativas

Una estrategia para combatir el *phishing* adoptada por algunas empresas es la de entrenar a los empleados de modo que puedan reconocer posibles ataques. Una nueva táctica de *phishing* donde se envían correos electrónicos de tipo phishing a una compañía determinada, conocido como *spear phishing*, ha motivado al entrenamiento de usuarios en varias localidades, incluyendo la Academia Militar de West Point en los Estados Unidos. En un experimento realizado en junio del 2004 con *spear phishing*, el 80% de los 500 cadetes de West Point a los que se les envió un correo electrónico falso fueron engañados y procedieron a dar información personal.^[22]

Un usuario al que se le contacta mediante un mensaje electrónico y se le hace mención sobre la necesidad de "verificar" una cuenta electrónica puede o bien contactar con la compañía que supuestamente le envía el mensaje, o puede escribir la dirección web de un sitio web seguro en la barra de direcciones de su navegador para evitar usar el enlace que aparece en el mensaje sospechoso de *phishing*. Muchas compañías, incluyendo eBay y PayPal, siempre se dirigen a sus clientes por su nombre de usuario en los correos electrónicos, de manera que si un correo electrónico se dirige al usuario de una manera genérica como («Querido miembro de eBay») es probable que se trate de un intento de *phishing*.

Respuestas técnicas

Hay varios programas informáticos *anti-phishing* disponibles. La mayoría de estos programas trabajan identificando contenidos phishing en sitios web y correos electrónicos; algunos software *anti-phishing* pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los *phishers*, ya que reducen el número de correos electrónicos relacionados con el *phishing* recibidos por el usuario.

Muchas organizaciones han introducido la característica denominada «pregunta secreta», en la que se pregunta información que sólo debe ser conocida por el usuario y la organización. Las páginas de Internet

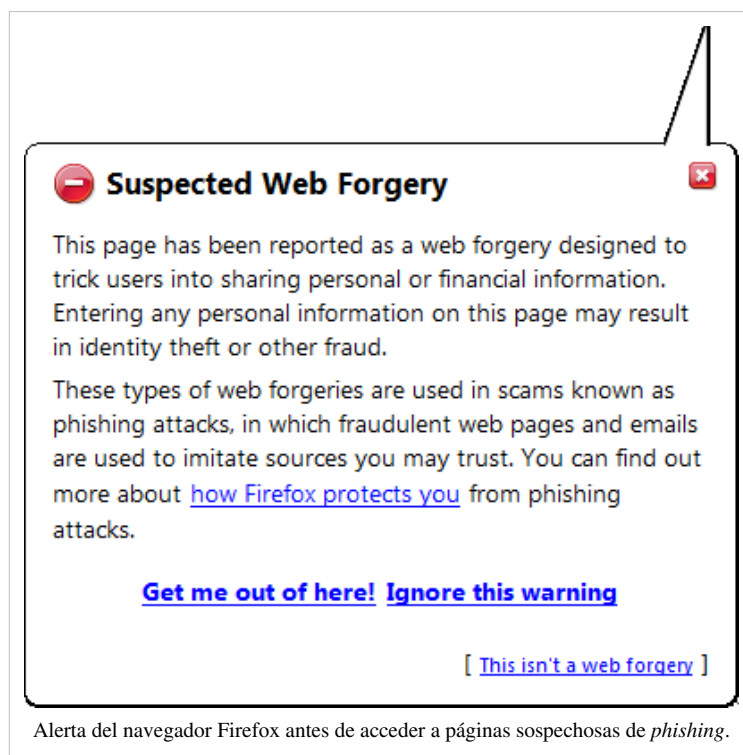
también han añadido herramientas de verificación que permite a los usuarios ver imágenes secretas que los usuarios seleccionan por adelantado; si estas imágenes no aparecen, entonces el sitio no es legítimo.^[23] Estas y otras formas de autenticación mutua continúan siendo susceptibles de ataques, como el sufrido por el banco escandinavo Nordea a finales de 2005.^[24]

Muchas compañías ofrecen a bancos y otras entidades que sufren de ataques de phishing, servicios de monitoreo continuos, analizando y utilizando medios legales para cerrar páginas con contenido phishing.

El [www.apwg.org/ Anti-Phishing Working Group}, industria y asociación que aplica la ley contra las prácticas de *phishing*, ha sugerido que las técnicas convencionales de *phishing* podrían ser obsoletas en un futuro a medida que la gente se oriente sobre los métodos de ingeniería social utilizadas por los *phishers*.^[25] Ellos suponen que en un futuro cercano, el *pharming* y otros usos de *malware* se van a convertir en herramientas más comunes para el robo de información.

Respuestas legislativas y judiciales

El 26 de enero de 2004, la FTC (Federal Trade Commission, la Comisión Federal de Comercio) de Estados Unidos llevó a juicio el primer caso contra un *phisher* sospechoso. El acusado, un adolescente de California, supuestamente creó y utilizó una página web con un diseño que aparentaba ser la página de America Online para poder robar números de tarjetas de crédito.^[26] Tanto Europa como Brasil siguieron la práctica de los Estados Unidos, rastreando y arrestando a presuntos *phishers*. A finales de marzo de 2005, un hombre estonio de 24 años fue arrestado utilizando una *backdoor*, a partir de que las víctimas visitaron su sitio web falso, en el que incluía un *keylogger* que le permitía monitorear lo que los usuarios tecleaban.^[27] Del mismo modo, las autoridades arrestaron al denominado *phisher kingpin*, Valdir Paulo de Almeida, líder de una de las más grandes redes de *phishing* que en dos años había robado entre \$18 a \$37 millones de dólares estadounidenses.^[28] En junio del 2005 las autoridades del Reino Unido arrestaron a dos hombres por la práctica del *phishing*,^[29] en un caso conectado a la denominada «Operation Firewall» del Servicio Secreto de los Estados Unidos, que buscaba sitios web notorios que practicaban el *phishing*.^[30]



Alerta del navegador Firefox antes de acceder a páginas sospechosas de *phishing*.

La compañía Microsoft también se ha unido al esfuerzo de combatir el *phishing*. El 31 de marzo del 2005, Microsoft llevó a la Corte del Distrito de Washington 117 pleitos federales. En algunos de ellos se acusó al denominado *phisher* "John Doe" por utilizar varios métodos para obtener contraseñas e información confidencial. Microsoft espera desenmascarar con estos casos a varios operadores de phishing de gran envergadura. En marzo del 2005 también se consideró la asociación entre Microsoft y el gobierno de Australia para educar sobre mejoras a la ley que permitirían combatir varios crímenes cibernéticos, incluyendo el *phishing*.^[31]

El phishing como delito

General

Diversos países se han ocupado de los temas del fraude y las estafas a través de Internet. Uno de ellos es el Convenio de Cibercriminalidad de Budapest^[32] pero además otros países han dedicado esfuerzos legislativos para castigar estas acciones.

Algunos países ya han incluido el phishing como delito en sus legislaciones, mientras que en otros aún están trabajando en ello.

Argentina

En Argentina, el 19 de septiembre de 2011 fue presentado un proyecto para sancionar el Phishing^[33], bajo el N° de Expediente S-2257/11, Proyecto de Ley para tipificar el Phishing o Captación Ilegítima de Datos^[34] en el Senado de la Nación. Mediante este proyecto se busca combatir las diferentes técnicas de obtención ilegítima de información personal.

Estados Unidos

En los Estados Unidos, el senador Patrick Leahy introdujo el Ley Anti-Phishing de 2005 el 1 de marzo de 2005. Esta ley federal de anti-*phishing* establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de correo electrónico con la intención de estafar a los usuarios podrían recibir una multa de hasta \$250,000 USD y penas de cárcel por un término de hasta cinco años.^[35]

Algunos estados tienen leyes que tratan las prácticas fraudulentas o engañosas o el robo de identidad y que también podría aplicarse a los delitos de phishing. Aquí^[36] se puede encontrar los estados que actualmente castigan este tipo de delitos.

Referencias

- [1] Tan, Koon. Phishing and Spamming via IM (SPIM). Internet Storm Center. (<http://isc.sans.org/diary.php?storyid=1905/>). 5 de diciembre de 2010
- [2] (http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1193304,00.html). Ed Skoudis. Phone phishing: The role of VoIP in phishing attacks. 13 de junio de 2006
- [3] Suplantación o robo de identidad (phishing)a (<http://www.ri5.com.ar/ayudaphishing.php>)
- [4] Stutz, Michael AOL: A Cracker's Paradise? (<http://wired-vig.wired.com/news/technology/0,1282,9932,00.html/>) 29 de enero de 1998
- [5] "phishing, n." OED Online, March 2006, Oxford University Press. Oxford English Dictionary Online. (<http://dictionary.oed.com/cgi/entry/30004304/>). 9 de agosto de 2006
- [6] "phish, v." OED Online, March 2006, Oxford University Press. Oxford English Dictionary Online. <http://dictionary.oed.com/cgi/entry/30004303/9> de agosto de 2006
- [7] Ollmann, Gunter. Phishing Guide: Understanding and Preventing Phishing Attacks. Technical Info. (<http://www.technicalinfo.net/papers/Phishing.html>). 10 de julio de 2006.
- [8] AOL: A Cracker's Paradise? (<http://wired-vig.wired.com/news/technology/0,1282,9932,00.html/>). Michael Stutz. *Wired News*. 29 de enero de 1998
- [9] History of AOL Warez (<http://www.rajuabju.com/warezirc/historyofaolwarez.htm>). 28 de septiembre de 2006.
- [10] Phishing for Clues, Indiana University Bloomington (<http://www.browser-recon.info/>), 15 de septiembre de 2005 (en inglés)

- [11] <http://www.pcworld.com/resource/article/0,aid,125956,pg,1,RSS,RSS,00.asp/> Phishing Scam Takes Aim at MySpace.com. Jeremy Kirk. IDG Network. 2 de junio de 2006 (en inglés)
- [12] Tom Jagatic and Nathan Johnson and Markus Jakobsson and Filippo Menczer. Social Phishing (<http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf/>). A publicarse en Communications of the ACM. 3 de junio del 2006. (en inglés)
- [13] Malicious Website / Malicious Code: MySpace XSS QuickTime Worm (<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708/>). Websense Security Labs. 5 de diciembre de 2006.
- [14] Berners-Lee, Tim. Uniform Resource Locators (<http://www.w3.org/Addressing/rfc1738.txt/>), IETF Network Working Group, 28 de enero de 2006
- [15] Fisher, Darin. Warn when HTTP URL auth information isn't necessary or when it's provided (https://bugzilla.mozilla.org/show_bug.cgi?id=232567). Bugzilla. 28 de agosto de 2005
- [16] Microsoft. A security update is available that modifies the default behavior of Internet Explorer for handling user information in HTTP and in HTTPS URLs (<http://support.microsoft.com/kb/834489/>) *Microsoft Knowledgebase Database*. 28 de agosto de 2005
- [17] Evgeniy Gabrilovich and Alex Gontmakher. The Homograph Attack (http://www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf/) *Communications of the ACM* 45(2):128. febrero del 2002
- [18] Johanson, Eric. The State of Homograph Attacks Rev1.1. (http://www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf/) *The Shmoo Group*. 11 de agosto de 2005.
- [19] Kerstein, Paul: "How Can We Stop Phishing and Pharming Scams?" (<http://www.csoonline.com/talkback/071905.html/>), CSO, 19 de julio de 2005.
- [21] Richardson, Tim: "Brits fall prey to phishing" (http://www.theregister.co.uk/2005/05/03/aol_phishing/), *The Register*, 3 de mayo de, 2005.
- [22] Bank, David: "'Spear Phishing' Tests Educate People About Online Scams" (http://online.wsj.com/public/article/0,,SB112424042313615131-z_8jLB2WkfcVtgDAWf6LRh733sg_20060817,00.html?mod=blogs/), *The Wall Street Journal*, 17 de agosto de 2005.
- [23] "Security: Bank to Require More Than Passwords," (<http://www.cnn.com/2005/TECH/ptech/07/14/banking.security.ap/index.html/>) CNN, July 14, 2005.
- [25] Kawamoto, Dawn: "Faced with a rise in so-called pharming and crimeware attacks, the Anti-Phishing Working Group will expand its charter to include these emerging threats." (<http://www.zdnetindia.com/news/features/stories/126569.html/>), ZDNet India, 4 de agosto de 2005.
- [26] Legon, Jeordan: "Phishing' scams reel in your identity" (<http://www.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html/>), CNN, 26 de enero de 2004.
- [27] Leyden, John: "Trojan phishing suspect hauled in" (<http://www.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html/>), *The Register*, 4 de abril de 2005.
- [28] Leyden, John: "Brazilian cops net 'phishing kingpin'" (http://www.channelregister.co.uk/2005/03/21/brazil_phishing_arrest/), *The Register*, 21 de marzo de 2005.
- [29] "UK Phishers Caught, Packed Away," (<http://www.eweek.com/article2/0,1895,1831960,00.asp/>) *eWEEK*, junio 27 de 2005.
- [30] Nineteen Individuals Indicted in Internet 'Carding' Conspiracy. (<http://www.cybercrime.gov/mantovaniIndict.htm/>) 20 de noviembre del 2005
- [31] Microsoft Partners with Australian Law Enforcement Agencies to Combat Cyber Crime. (http://www.microsoft.com/australia/presspass/news/pressreleases/cybercrime_31_3_05.aspx/) 24 de agosto del 2005.
- [32] http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF
- [33] Borghello Cristian, Temperini Marcelo Cruzada por la Identidad Digital (<http://cruzada.elderechoinformatico.com/>) Marzo 2012.
- [34] <http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&numexp=2257/11&tipo=PL&tConsulta=1>
- [35] "Phishers Would Face 5 Years Under New Bill," (<http://informationweek.com/story/showArticle.jhtml?articleID=60404811/>) Information Week, 2 de marzo de 2005.
- [36] <http://www.ncsl.org/issues-research/telecom/state-phishing-laws.aspx>

Enlaces externos

Información sobre phishing

- Grupo Activo Anti-Phishing (<http://www.anti-phishing.org>) (en inglés)
- Amenazas en la era digital - Informe sobre el Phishing y otras amenazas para las Entidades Financieras (<http://www.iberfinanzas.com/index.php/Articulos-informes/Amenazas-en-la-era-digital.html>)
- INTECO, equipo que gestiona incidentes de phishing en España (http://cert.inteco.es/Respuesta_y_Soporte/Gestion_de_Fraude_Electronico/)

Legislación

- Duke Law & Technology Review (<http://www.law.duke.edu/journals/dltr/articles/2005dltr0006.html>) - Tapando los agujeros provocados por el phishing: legislación contra tecnología.

Fuentes y contribuyentes del artículo

Phishing *Fuente:* <http://es.wikipedia.org/w/index.php?oldid=67939157> *Contribuyentes:* 32X, A ver, Aanggiiee, Acratta, Airunp, Alakasam, Aleja1994.17, Alejobd, Alexav8, Alextrevelian 006, Alvaro qc, Anita londoño, AnselmiJuan, Antur, Anvarstudios, Aofvilla, Asqueladd, Atila rey, Baiji, Barcex, Belgrano, Bogart NSSME, Bonilla daniel, Bryan alexander giraldo, Chuck es dios, Ciudadano77, Cmontero, ColdWind, Corrector1, Creosota, Crisborghe, Damianiencowiki, Damifb, Danniela lopez, David0811, Diana marcela correa, Diegusjaimes, Diotime, Dives, Dodo, Dr. Fasilier, Edison bolaños, Eduardosalg, Edupedro, Elisardojm, Emijrp, Ernesto Graf, FViolat, Filipino, GermanX, Ginés90, Gizmo II, Greek, Gusama Romero, Gusgus, Halfdrag, Helmy oved, Ialad, Ignacio Icke, Irm, Itz37, J. A. Gélvez, Jacoream, Jennixyta96, Jfwiki, Jkbw, Jkdd.laura, Jondel, Julianortega, Jynus, KErosEnE, Kakico, Kariime kaztro, Lady marin, Lasneyx, Laura Fiorucci, Leonpolanco, Lucien leGrey, MKernel, Magister Mathematicae, Mansoncc, Matdrones, Matw13, Mazu castañeda, Melissa Savedra, Mortadelo2005, Mouse, Moylop260, Mpeinadopa, Muffinman, Nachosan, Olidata14, Pabloh, Paintman, Pedro Felipe, Pólux, Qwertyytrewq qwerty, RGLago, Richy, RubiksMaster110, Sabbut, Salesian Party, Saloca, Savh, Seanver, Sergio Andres Segovia, Shalbat, Sitatunga, Soro 04, SuperBraulio13, Superzerocool, Taichi, Technopat, Tirithel, UA31, Vandal Crusher, Wedrey, Wikiléptico, Zuirdj, 346 ediciones anónimas

Fuentes de imagen, Licencias y contribuyentes

Archivo:PhishingTrustedBank.png *Fuente:* <http://es.wikipedia.org/w/index.php?title=Archivo:PhishingTrustedBank.png> *Licencia:* Public Domain *Contribuyentes:* Andrew Levine

Archivo:Phishing chart.png *Fuente:* http://es.wikipedia.org/w/index.php?title=Archivo:Phishing_chart.png *Licencia:* Public domain *Contribuyentes:* Original uploader was ZeWrestler at en.wikipedia

Archivo:Firefox 2.0.0.1 Phising Alert.png *Fuente:* http://es.wikipedia.org/w/index.php?title=Archivo:Firefox_2.0.0.1_Phising_Alert.png *Licencia:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contribuyentes:* AVRS, KErosEnE, PolhoNinja, Remember the dot, 1 ediciones anónimas

Licencia

Creative Commons Attribution-Share Alike 3.0 Unported
[//creativecommons.org/licenses/by-sa/3.0/](http://creativecommons.org/licenses/by-sa/3.0/)