

Noviembre de 2004



McAfee Research
Informe Técnico N.º 04-004

Anti-Phishing: Prácticas recomendadas para Empresas y Consumidores

Gregg Tally
Roshan Thomas
Tom Van Vleck

1 Introducción

Phishing es una forma de estafa por Internet, en que los atacantes intentan convencer a los consumidores a divulgar información personal confidencial. Normalmente, las técnicas involucran *e-mails* y sitios Web fraudulentos que fingen ser *e-mails* y sitios Web legítimos. Los *e-mails* fraudulentos pueden ser considerados una forma malintencionada de *e-mail* en masa no-solicitado, generalmente conocido como "spam." Los consumidores se quedan vulnerables al robo de identidades y a pérdidas financieras a través de transacciones fraudulentas. Las instituciones financieras están en riesgo debido al gran número de transacciones fraudulentas realizadas con la información robada. Los ataques de *phishing* son, a menudo, eventos en gran escala cuyo blanco son miles de consumidores, o más, esperando que una parte de ellos sea engañada. Un porcentaje relativamente grande de destinatarios realmente responde a dichos *e-mails* pues parecen legítimos y su autenticidad no puede ser fácilmente verificada. Las estimaciones de respuesta varían entre el 1% y el 20%, dependiendo del ataque. Los atacantes pueden copiar fácilmente imágenes, enlaces y textos de sitios Web legítimos para hacer que el *e-mail* parezca auténtico [KOPR]. Debido a la escala de los ataques, la posibilidad de ocurrir enormes pérdidas financieras es grande. Algunos ataques involucran un millón o más de *e-mails* de *phishing*.

Como observó el Grupo de Trabajo Anti-*Phishing* [APWG], los clientes de muchos bancos y varias instituciones financieras vienen siendo los blancos de ataques de *phishing*. Los objetivos son, generalmente, el robo de números de cuentas de tarjetas de crédito y débito y PIN. Clientes de otras empresas también vienen siendo los blancos de operaciones de robo de identidad.

La amenaza del *phishing* está aumentando rápidamente. El APWG informó 176 ataques únicos de *phishing* en el mes de enero de 2004 [APJA]. Hasta abril, el número de ataques únicos por mes creció para 1.125 [APAP], alcanzando a 1.422 en junio [APJU]. Clientes de instituciones financieras, empresas minoristas y proveedores de servicios de Internet fueron blancos frecuentes.

Muchas organizaciones y empresas distintas propusieron alteraciones básicas en la infraestructura de *e-mail* para ayudar a aliviar el *spam*, lo que, por fin, reduciría los problemas con el *phishing*. El Grupo de Investigaciones Anti-Spam, del Grupo de Trabajo de Investigaciones de Internet, es una de dichas organizaciones [ASRG]. Hasta que se efectúen dichas alteraciones, las instituciones financieras y sus clientes pueden tomar medidas para ayudar a reducir el riesgo de los ataques de *phishing*. Dichas medidas cubren una autenticación más rigurosa para las transacciones electrónicas, la distribución más amplia de productos anti-*spam*, antivirus y *firewall* personal, además de la distribución de software de protección de privacidad.

Nuestras soluciones propuestas presuponen que las empresas y los consumidores seguirán usando por muchos años alguna forma de hardware y software existentes hoy día. No creemos que sea práctico proponer alteraciones radicales en esta base instalada como parte de una solución de corto plazo. Por lo tanto, las soluciones que proponemos son compatibles con productos ampliamente usados por consumidores y empresas, incluso los actuales navegadores y servidores de Web, aplicaciones y servidores de *e-mail* y sistemas operativos estándar.

En el corto plazo, hay poca chance de que las empresas cambien sus formas consagradas de verificación de identidad, tales como números de documentos personales y apellido de soltera de la madre. Nuestra propuesta es hacer más difícil que los atacantes logren acceso a dicha información.

Este *white paper* presenta un panorama de los estadios de un ataque típico de *phishing*. También proponemos una serie de prácticas recomendadas para que las empresas y sus clientes reduzcan el impacto de los futuros ataques de *phishing*.

2 Estadios de los Ataques de *Phishing*

Los ataques de *phishing* involucran diversos estadios:

- El atacante obtiene las direcciones de *e-mail* de las víctimas. Dichas direcciones pueden ser presumidas u obtenidas desde varias fuentes.
- El atacante genera un *e-mail* que parece legítimo y solicita que el destinatario realice alguna acción.
- El atacante envía un *e-mail* a sus víctimas de forma que parezca legítimo y oscurezca la verdadera fuente.
- Dependiendo del contenido del *e-mail*, el destinatario abre un adjunto malintencionado, llena un formulario o visita un sitio Web.
- El atacante recopila la información confidencial de la víctima y puede explotarla en el futuro.

El atacante tiene varias formas de ejecutar dichos pasos. También hay contramedidas que las víctimas pueden utilizar para frustrar algunos de ellos. Los árboles de ataque que damos a continuación muestran los pasos que el atacante (y la víctima) necesitan realizar para un ataque de *phishing* exitoso. Los árboles también muestran algunas maneras por las cuales las actuales tecnologías pueden ser usadas para reducir la vulnerabilidad a los ataques de *phishing*.

En el diagrama, el estado 'Inicio' está en el tope. Las acciones del atacante y de la víctima son mostradas como bordes o líneas entre los rectángulos. Cada rectángulo contiene el recurso o la condición que el atacante intenta alcanzar. El ataque es frustrado si pasar al estado de 'Ataque Frustrado'. El ataque será exitoso si alcanza el estado final 'Atacante Obtiene Información Confidencial del Usuario'.

Debido al tamaño y a la complejidad del árbol, lo dividimos en cuatro secciones. La primera sección muestra los estadios del ataque que son comunes a todos los métodos. Cada uno de los métodos de ataque es detallado en su propio diagrama. Dichos métodos son los siguientes:

- Instalación de Troyanos (software malintencionado que no se comporta como espera el destinatario).
- Utilización de fraude para convencer al destinatario la continuación de algunas instrucciones.
- Utilización de spyware para interceptar comunicaciones legítimas entre la víctima y una empresa legítima. El *spyware* es un programa que recopila secretamente información sobre las actividades del usuario (tecleo, sitios Web visitados, etc.), transmitiendo dicha información a terceros.

Como muestra la Figura 1 a continuación, el ataque de *phishing* empieza con el envío de un *e-mail* a las víctimas. El atacante crea el *e-mail* con el objetivo inicial de hacer que el destinatario crea que el *e-mail* pueda ser legítimo y que se lo debe aceptar. Los atacantes obtienen direcciones de *e-mail* en diversas fuentes, incluso por generación semialeatoria, buscándolos en fuentes en Internet y listas de direcciones que el usuario creía confidenciales [CNET]. El filtrado de *spam* puede bloquear muchos de los *e-mails* de *phishing*. Si las instituciones cuyos clientes reciben *phishing* regularmente utilizan *e-mails* autenticados (con PGP o S/MIME, por ejemplo), el destinatario podrá percibir que el *e-mail* no posee una firma válida, bloqueando, por lo tanto, el ataque. Tras la apertura del *e-mail* por el usuario, el contenido tendrá que ser suficientemente realista para llevar al destinatario a seguir sus instrucciones.

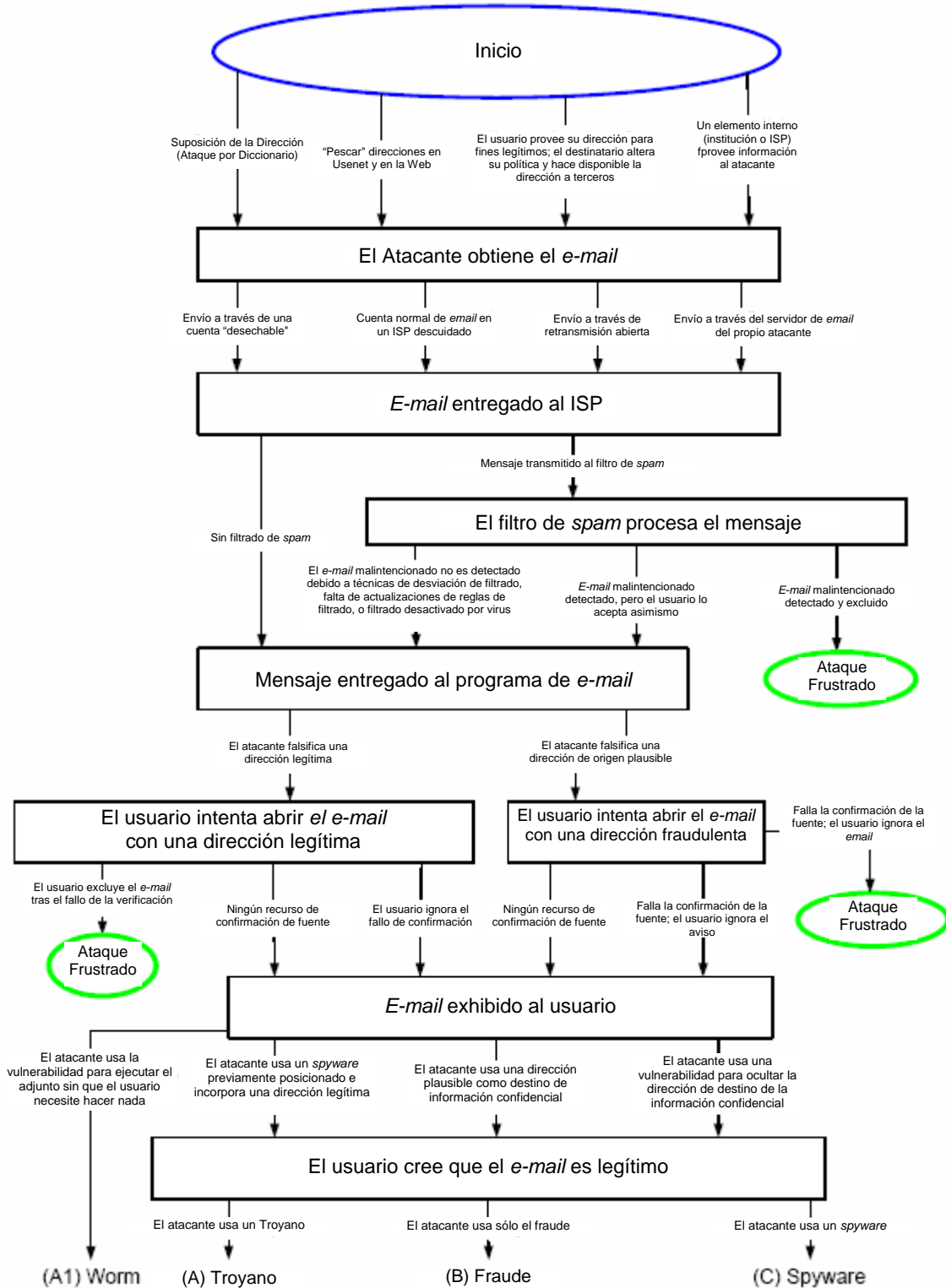


Figura 1 – Métodos comunes del Árbol de Ataques

Worms y Troyanos

En la Figura 2, el atacante continúa el ataque, enviando un adjunto de *e-mail* que finge ser bienintencionado, por ejemplo, una tarjeta virtual o un salvapantallas. En verdad, el adjunto contiene un programa ejecutable que intercepta las comunicaciones posteriores entre la computadora de la víctima y una institución legítima. El programa espía transmite la información al atacante por la red. Programas antivirus, detección de intrusiones en el *host* y programas de *firewall* personal pueden bloquear muchos ataques en esta situación.

Fraude

La Figura 3 muestra una continuación de la secuencia de ataque de la Figura 1, utilizando sólo el fraude. El ataque no involucra ninguna vulnerabilidad y ningún otro programa. El atacante utiliza la ley de los grandes números para asegurar que por lo menos algunos de los destinatarios se convenzan de que el *e-mail* es legítimo y sigan las instrucciones. El SSL (*Secure Socket Layer*) brinda alguna protección si el sitio Web del atacante lo utiliza, pero sólo si el destinatario está atento a los avisos del navegador sobre caracteres inválidos. Programas comerciales de protección de privacidad también pueden ser útiles, avisando al usuario cuando está en el momento de enviar información confidencial a destinos cuestionables.

Spyware (Programas Espías)

La Figura 4 muestra el atacante utilizando un programa espía previamente posicionado en la computadora de la víctima para extraer información confidencial. Esto se puede realizar través de un ataque anterior por *worm* o Troyano (véase la Figura 2) o por otros medios. A menudo, el *spyware* puede ser detectado por programas especializados en detección de *spyware* y por muchos antivirus disponibles comercialmente. Además, los *firewalls* personales y los sistemas de detección de intrusiones en el *host* pueden, a menudo, impedir que el *spyware* transmita información confidencial a terceros.

3 Prácticas recomendadas

Las “prácticas recomendadas” presentadas a continuación para empresas y consumidores solucionan muchos problemas percibidos en la discusión sobre los estadios de los ataques de *phishing* en la Sección 2. Dichas soluciones se dividen en dos categorías generales:

Prácticas recomendadas para Empresas

- Establezca políticas corporativas y divúlguelas a los consumidores: Cree políticas corporativas de contenido de *e-mail* para que no se puedan confundir los mensajes legítimos con *phishing*. Divulgue dichas políticas a los clientes y sígalas.
- Cree una manera para que el consumidor confirme si el *e-mail* es legítimo: El consumidor debe ser capaz de identificar si el *e-mail* proviene de la institución, no de un *phisher*. Para eso, la institución remitente necesita establecer una política para incluir información de autenticación en *todos los e-mails* enviados por ella a los consumidores.
- Autenticación más rígida en los sitios Web: Si las instituciones no solicitan información confidencial de los clientes para la entrada en un sitio Web (por ejemplo, números de documentos o contraseñas), se queda más difícil para que los *phishers* extraigan dicha información del consumidor.
- Monitoree Internet en busca de sitios Web que puedan ser de *phishing*: Generalmente, el sitio Web de *phishing* aparece en algún lugar de Internet antes del envío de los *e-mails* de *phishing*. A menudo, dichos sitios Web se apropian indebidamente de marcas comerciales de empresas para que parezcan legítimos.
- Implemente soluciones antivirus, de filtrado de contenido y anti-spam de buena calidad en el punto de contacto (*gateway*) con Internet: La exploración antivirus en el *gateway* establece una capa de defensa más allá de la exploración antivirus en la propia máquina. Filtre y bloquee sitios Web de *phishing* conocidos en el *gateway*. El filtrado de *spam* en el *gateway* ayuda a los usuarios finales a evitar mensajes no deseados y *e-mails* de *phishing*.

Prácticas recomendadas para el Consumidor

- Bloquee automáticamente mensajes malintencionados/fraudulentos: Los detectores de *spam* pueden ayudar a evitar que el consumidor tenga que abrir *e-mails* sospechosos, pero no son infalibles.
- Detecte y excluya automáticamente los programas malintencionados: A menudo, los programas espías son parte de un ataque de *phishing*, pero pueden ser eliminados por muchos programas disponibles en el mercado.
- Bloquee automáticamente la salida de información confidencial a terceros malintencionados: Aunque el consumidor no logre identificar visualmente el verdadero sitio Web que recibirá la información confidencial, existen productos de *software* que lo logran.
- Siempre desconfíe: Si usted no está seguro de que un *e-mail* es legítimo, llame a la institución que aparentemente envió el *e-mail* para verificar su autenticidad.

Ninguna de dichas soluciones constituye, individualmente, una respuesta completa al problema.

Recomendamos una combinación de contramedidas que:

- Reducirá el número de ataques de *phishing* enviados a los consumidores;
- Aumentará la probabilidad de que el consumidor reconozca un *ataque de phishing*; y
- Reducirá las oportunidades de que el consumidor provea inadvertidamente información confidencial.

La concienciación sigue esencial para que los consumidores conozcan tanto las técnicas de *phishing* como la manera por la cual las empresas legítimas se comunican con ellos por *e-mail* y por la Web.

Algunas de las soluciones propuestas exigen software en la computadora del consumidor. Si se adopta

dicha solución, será la base para más soluciones con un poco más de esfuerzo de mantenimiento. Las recomendaciones dadas a continuación añaden detalles a las prácticas recomendadas para empresas y consumidores relacionadas más arriba. Hay otras estrategias de largo plazo que exigen la cooperación de los Proveedores de Servicios de E-Mail y de los Proveedores de Servicios de Internet (ISP), que también deberán entrar en vigor en poco tiempo. Una de dichas estrategias es el abordaje de laves de Dominio, recientemente defendida por Yahoo!™ y la exploración de *e-mail* en el *gateway*.

3.1 Prácticas recomendadas para las Empresas

3.1.1 Establezca Políticas corporativas uniformes

3.1.1.1 Evite hiperenlaces incorporados

Problema

A menudo, los *e-mails* comerciales legítimos poseen hiperenlaces al sitio Web de la empresa, que solicitan que el consumidor envíe información confidencial, incluso el nombre del usuario y la contraseña. Los *phishers* aprovechan dichos enlaces incorporados para llevar a los consumidores a revelar dicha información a sitios Web fraudulentos.

Abordaje

Aunque la incorporación de hiperenlaces en los *e-mails* pueda facilitar la navegación del consumidor, eso también crea más oportunidades de fraude. Las vulnerabilidades en algunas versiones del Microsoft Internet Explorer pueden brindarle al *phisher* la oportunidad de disfrazar el verdadero destino de una URL. Una alternativa más segura es incluir en el *e-mail* un enlace no pulsable que el consumidor necesite teclear o cortar y pegar en el navegador. Muy probablemente, los clientes regulares tendrán el enlace de la institución en su lista de sitios preferidos, facilitando aún más dicho proceso.

Este abordaje funcionará mejor si la política institucional es frecuentemente divulgada a los clientes y si todas las comunicaciones con los clientes siguen dicha política. La uniformidad es esencial.

Ventajas

- El número de ataques de *phishing* a través de URL engañosas puede ser reducido.
- Ni la empresa ni el consumidor necesitan instalar nuevos programas.

Desventajas

- La navegación del consumidor será negativamente afectada, aunque muy poco.
- Quizás algunos grupos e individuos de la institución no siempre sigan la política, llevando a la falta de uniformidad y a la confusión entre los consumidores.
- Quizás no siempre los consumidores se comporten de la manera que mejor atienda a sus intereses. Pueden seguir siendo engañados por *e-mails* fraudulentos con hiperenlaces incorporados.
- Los consumidores que reciben *e-mails* fraudulentos, pero que no son clientes de la institución, pueden no estar al tanto de la política.

Recomendación

Las instituciones deben evaluar con cuidado el impacto sobre la comodidad para el consumidor respecto al aumento de la seguridad que brinda la implementación de esta política. Ello puede ser adecuado para muchas instituciones.

3.1.1.2 Evite formularios de *e-mail*

Problema

Los *phishers* utilizan formularios de *e-mail* para recolectar información personal de los consumidores. Si la institución legítima también utiliza dichos formularios, será difícil para el consumidor distinguir entre *e-mails* legítimos y fraudulentos.

Abordaje

Como ocurre con los hiperenlaces incorporados, los formularios de *e-mail* pueden simplificar la navegación del consumidor cuando la institución solicita información. Sin embargo, el mecanismo es fácilmente usado por los *phishers* para recolectar la misma información, dando poca oportunidad para que el consumidor confirme la fuente del e-mail.

La institución debe informar a los consumidores de que los *e-mails* legítimos nunca contendrán formularios solicitando información personal.

Ventajas

- Los ataques de *phishing* a través de formularios de *e-mail* pueden ser reducidos.
- Ni la empresa ni el consumidor necesitan instalar nuevos programas.

Desventajas

- La comodidad para el consumidor será ligeramente afectada.
- Quizás algunos grupos e individuos de la institución no siempre sigan la política, llevando a la falta de uniformidad y a la confusión entre los consumidores.
- Quizás no siempre los consumidores se comporten de la manera que mejor atiende a sus intereses. Pueden seguir siendo engañados por *e-mails* fraudulentos con formularios incorporados.
- Los consumidores que reciben *e-mails* fraudulentos, pero que no son clientes de la institución, pueden no estar al tanto de la política.

Recomendación

Las instituciones deben evaluar cuidadosamente el impacto sobre la comodidad para el consumidor respecto al aumento de la seguridad que brinda la implementación de esta política. Probablemente esto sea adecuado para la mayoría de las instituciones.

3.1.2 Mecanismos de verificación de e-mail

3.1.2.1 E-mails firmados digitalmente

Problema

Los clientes no cuentan con un medio infalible para verificar la autenticidad de los mensajes potencialmente importantes provenientes de instituciones legítimas.

Abordaje

Las instituciones deben establecer una política por la cual todas las comunicaciones de alto valor por *e-mail* con los clientes sean digitalmente firmadas con una clave privada autorizada. Al recibir el *e-mail*, el destinatario verifica la autenticidad a través de la clave pública de la institución. Existe una probabilidad muy pequeña de que un *phisher* logre crear una firma válida para un *e-mail* fraudulento.

PGP y S/MIME son ejemplos de tecnologías de firma digital, pero muchos usuarios creen que son muy difíciles de usar. Hasta hoy, dichas tecnologías no han sido ampliamente adoptadas.

Ventajas

- Las firmas digitales son extremadamente difíciles de falsificar.
- Los mensajes pueden ser verificados automáticamente por lectores de *e-mail*.
- Se las pueden usar como mecanismo de recuperación en un sistema de autenticación múltiple cuando se pierdan los *tokens*.

Desventajas

- Es poco probable que el consumidor común instale y mantenga una tecnología de firma digital.
- Los que no son cliente de la institución no conocerán la política de la institución de firmar todos los *e-mails*.

Recomendación

Para un pequeño número de cuentas de clientes con transacciones de alto valor, este abordaje vale la consideración.

3.1.2.2 Estructura de Política de Remitentes (SPF)

Problema

A menudo, los *e-mails* de *phishing* falsifican el dominio de envío de la institución tenida por objetivo.

Abordaje

Las especificaciones SPF que se están desarrollando en IETF [SPF] están intentando definir un mecanismo por el cual los destinatarios puedan verificar si un servidor remitente tiene la autorización para enviar mensajes de parte del dominio de origen. Por sí sola, la SPF no impide todas las formas de *spam* porque los remitentes de *spam* pueden registrar dominios desechables con registros de SPF para pasar por las pruebas de SPF. Con los *e-mails* de *phishing*, esto es más difícil porque el dominio de envío en el *e-mail* necesita ser plausible para el destinatario humano como un dominio de envío legítimo de la institución cuestionada.

La SPF necesita que los propietarios de dominios legítimos publiquen registros SPF en el servicio de nombres de dominio (DNS). La fiscalización del SPF se puede realizar en el agente de transferencia de *e-mail* (MTA) de destino, en el agente de distribución de *e-mail* (MDA), o en el agente de usuario de *e-mail* (MUA). Existen problemas con el encaminamiento de los mensajes que necesitan modificaciones

para legitimar el encaminamiento de *e-mails*, tales como alteración de encaminamiento para reenvío.

Los usuarios finales necesitan conocer el dominio de envío al inspeccionar el *e-mail*. Si el asunto y el cuerpo de un *e-mail* afirman que son del banco del destinatario, pero la dirección "De" es absurda, SPF no ayudará. El usuario será responsable de imaginar que hay una discrepancia en la dirección "De" y en el contenido del mensaje.

Ventajas

- Obliga a los *phishers* a usar dominios de envío que no son idénticos al nombre del dominio de envío legítimo.
- No es necesario ningún software o hardware más para el cliente final si el ISP realiza la verificación de SPF en el MTA.

Desventajas

- Las especificaciones están todavía en evolución, pero una cierta adopción ya empezó.
- No es totalmente a prueba de fraudes, pero eleva el nivel de la seguridad. Los *phishers* aún pueden crear dominios que parecen reales y registrar registros de SPF de dichos dominios.
- Si los *phishers* no imitan el dominio de envío, la SPF no será eficaz. Los usuarios finales necesitan verificar si el remitente corresponde al contenido del *e-mail*.

Recomendación

Las instituciones deben publicar los registros de SPF de sus dominios de envío de *e-mail*. A medida que cada vez más ISP y servidores de *e-mail* empiecen a verificar los registros de SPF, la solución se volverá más eficaz.

3.1.2.3 Personalización visual o sonora de e-mails

Problema

El cliente común no cuenta con un medio sencillo de verificar la autenticidad de los mensajes provenientes de instituciones legítimas.

Abordaje

Este abordaje ofrece un mecanismo visual o sonoro para verificar la autenticidad de los *e-mails*. Así como ocurre con la actual práctica de adjuntar la fotografía del titular en las tarjetas de crédito emitidas por los bancos, las instituciones podrían incluir una fotografía del cliente en todas las comunicaciones electrónicas. Este es un método sencillo y confiable para que el cliente de un banco reconozca los mensajes legítimos sin que necesite precisar instalar ningún software más en su máquina. Los clientes deficientes visuales utilizarían un objeto de identificación alterno (quizás una "imagen sonora" o una palabra de acceso) adjuntado adecuadamente.

Observe que la única manera de que este mecanismo sea exitoso es que sea acompañado por una campaña informativa de la institución para anunciar el nuevo "Mecanismo Seguro de Comunicación."

Ventajas

- El cliente final no necesita ningún software o hardware más.
- Los mensajes pueden ser fácilmente verificados por usuarios sin conocimientos sofisticados.
- El valor de las tarjetas de crédito "personalizadas" ya establecido en el mercado; se puede asociar fácilmente con dicho mensaje de marketing.

- Reduce la probabilidad de ataques en gran escala, pues los *phishers* necesitan recopilar mensajes anteriores de la institución para cada cliente para obtener la información de personalización.
- Se puede usar este abordaje como mecanismo de recuperación en un sistema de autenticación múltiple cuando se pierdan los *tokens*.

Desventajas

- Gastos considerables de marketing para divulgar el mensaje "No acepte mensajes que no contienen su fotografía".
- Aumento considerable del costo de generación de los mensajes.
- Los clientes necesitan comparecer en persona a la institución para que se saque su fotografía. Quizás eso no sea adecuado para empresas virtuales que no cuentan con instalaciones físicas. Otros medios, tales como distribución de contraseñas o fotos por correo convencional, pueden ser necesarios para dichas empresas. Sin embargo, sería preferible que cada institución utilizara fotos exclusivas para que eventuales fallos de seguridad en una de ellas no se multiplicaran en cascada, convirtiéndose en vulnerabilidades para todas.
- Las instituciones deben proteger rígidamente la base de datos que contiene los datos de autenticación (fotos, clips de sonido o contraseñas).
- El método no es completamente a prueba de fraude, pero eleva el nivel de seguridad.

Recomendación

Para ciertas instituciones, especialmente las que emiten tarjetas de crédito, esta puede ser una solución viable si ya capturan imágenes digitales para tarjetas de crédito u otras finalidades.

3.1.2.4 Numeración secuencial de e-mails

Problema

El cliente común no cuenta con un medio simple de verificar la autenticidad de los mensajes provenientes de instituciones legítimas.

Abordaje

Otra variación de este mecanismo es incorporar el equivalente a una numeración secuencial a cada *e-mail* enviado por la institución. Los números de secuencia serían una forma previsible de autenticación que el consumidor podría verificar fácilmente. Aquí está un ejemplo de encabezamiento de autenticación:

Fecha: 16 de enero de 2004

Número de Serie: JJH0017

El último *e-mail* que le enviamos fue el JJH0016 el 10 de diciembre de 2003.

El próximo *e-mail* que le enviaremos tendrá el número de serie JJH0018.

Observe que este mecanismo sólo será exitoso si se lo acompaña por una campaña informativa de la institución para anunciar el nuevo "Mecanismo Seguro de Comunicación."

Ventajas

- El cliente final no necesita ningún software o hardware más.
- El valor de las tarjetas de crédito "personalizadas" ya establecidas en el mercado puede asociarse fácilmente con dicho mensaje de marketing.
- Reduce la probabilidad de ataques en gran escala, pues los estafadores necesitan recopilar mensajes anteriores de la institución para cada cliente para obtener la información de personalización.

- Se puede usar este abordaje como mecanismo de recuperación en un sistema de autenticación múltiple cuando se pierdan los *tokens*.

Desventajas

- Un poco más de dificultad de confirmación por el destinatario debido a la necesidad de mantener el *e-mail* más reciente.
- Quizás los consumidores no verifiquen los números de secuencia.
- Aumento considerable en el costo de generación de los mensajes.
- La institución necesita proteger de manera estricta la base de datos que contiene los números de secuencia.
- No es completamente a prueba de fraudes, pero aumenta el nivel de seguridad.

Recomendación

Si no es posible obtener imágenes digitales o información semejante de personalización, esta es la segunda solución más confiable. Sin embargo, también es la más propensa a fallos para un gran número de consumidores.

3.1.2.5 Incorporación del Nombre del consumidor al *e-mail*

Problema

El cliente común no cuenta con un medio sencillo de verificar la autenticidad de los mensajes de instituciones legítimas.

Abordaje

La forma más sencilla de este mecanismo es simplemente incorporar el nombre del cliente al *e-mail*, por ejemplo, "Estimado Sr. Jones". Algunas empresas ya usan esta técnica. Sin embargo, si la dirección de *e-mail* del consumidor contiene el nombre del consumidor, los *phishers* pueden lograr deducir un porcentaje considerable de los nombres. Los *phishers* no tienen nada que perder si sus suposiciones no están correctas.

Ventajas

- El cliente final no necesita ningún otro software o hardware.
- Los mensajes pueden ser fácilmente verificados por usuarios que no poseen un conocimiento sofisticado.
- Reduce la probabilidad de un ataque exitoso en larga escala, pues los *phishers* necesitan recopilar o suponer la información de personalización de muchos consumidores.

Desventajas

- No siempre los consumidores percibirán que falta su nombre en el *e-mail*.
- Gastos considerables de marketing para divulgar el mensaje "No acepte mensajes que no lleven su nombre".
- Las instituciones deben proteger de manera rígida la base de datos que contiene los datos de autenticación (nombre del consumidor).
- No es completamente a prueba de fraudes, pero aumenta el nivel de seguridad.

Recomendación

Todas las instituciones deben emplear este abordaje. Si esta es la política predominante en todas las

instituciones, los consumidores podrán acostumbrarse a esperar la presencia de su nombre en los e-mails.

3.1.3 Mecanismos de Autenticación segura

3.1.3.1 Autenticación por *tokens* seguros

Problema

Golpes de ingeniería social, tales como el *phishing*, siempre serán posibles con tal de que la víctima conozca toda la información necesaria para realizar una transacción.

Abordaje

El objetivo final de los ataques de *phishing* es llevar la víctima a divulgar información confidencial. A menudo, dicha información es el nombre de usuario y la contraseña usados para acceder a un sitio Web legítimo. Si los usuarios no conocen la información de autenticación, este tipo de ataque será imposible.

Una forma de hacerlo es proveer *tokens* seguros (físicos) a los usuarios y exigir una secuencia de estímulo-respuesta en todas las transacciones electrónicas con la institución. En este tipo de sistema de autenticación, el *token* físico es una contraseña desechable válida sólo para la persona que posee el *token*. El *token* genera una nueva contraseña desechable a cada *login*, de forma que no importa si el atacante obtiene el valor. Además, el usuario no puede generar los valores anticipadamente, de forma que no hay como divulgar accidentalmente la información a un atacante.

Dichos *tokens* ya tienen un uso limitado. Algunas empresas exigen que sus funcionarios usen dichos *tokens* para acceder remotamente a las computadoras.

Algunos bancos y algunas empresas de tarjetas de crédito también poseen un recurso semejante para realizar transacciones con una tarjeta inteligente [GEMP] [MAST]. Una alternativa a la emisión de nuevos *tokens* físicos es integrar la función a las nuevas tarjetas de crédito. Sin embargo, las soluciones de tarjetas inteligentes generalmente exigen la conexión de un lector a la computadora. Además, se encontraron vulnerabilidades de seguridad en algunas tarjetas inteligentes.

Ventajas

- El usuario no puede divulgar accidentalmente la información necesaria para realizar una transacción electrónica.
- Todos los fraudes necesitan de acceso físico al *token*.
- El usuario no puede optar por autenticarse de forma a evadirse a la política de seguridad.
- Ya existen normas para la implementación de dichos sistemas. Véase <http://www.emvco.com>.
- La duplicación de la tarjeta física exige mucho más sofisticación, aunque la víctima provea su PIN.

Desventajas

- Por sí solos, los *tokens* seguros no impiden que el usuario provea información que se pueda usar como medio para realizar una transacción. Específicamente, la información usada para identificar una persona, por ejemplo, el apellido de soltera de la madre, todavía se puede obtener y llevar a actividades fraudulentas.
- La emisión de *tokens* tiene un costo, aunque dicho costo puede variar según el tipo de equipo elegido.
- El usuario puede necesitar llevar con él varios *tokens*, uno para cada servicio a que se suscribe.
- Se necesitan actualizaciones de software en el fabricante para que se realice la autenticación estímulo-respuesta.

- Hay costos considerables para la implementación y el mantenimiento de la solución, incluso la atribución inicial de los *tokens* y la revocación.
- Inicialmente, los usuarios pueden rechazar la inconveniencia adicional y los costos que se les pasarán.
- Para que sean seguras, las soluciones de *token* seguro y tarjetas inteligentes exigen amplia ingeniería de seguridad y atención a los muchos detalles correlatos.

Recomendación

Así como ocurre con las firmas digitales, este método puede ser adecuado a un pequeño número de clientes con transacciones de alto valor. Los consumidores y las empresas de EE.UU. ya fueron reacias a usar *tokens* anteriormente.

3.1.3.2 Emulación de *tokens* seguros por software para autenticación

Problema

Golpes de ingeniería social, tales como el *phishing*, siempre serán posibles con tal de que la víctima sepa toda la información necesaria para realizar una transacción. Los *tokens* de seguridad física pueden ayudar, pero su implementación puede ser dispendiosa.

Abordaje

El abordaje es muy semejante al abordaje de Token Seguro, pero sin la necesidad de otros equipos. En cambio, una aplicación atribuida a un cierto usuario provee los valores de respuesta para la autenticación electrónica. Ejecutado en una PC, se puede evitar que el usuario necesite retectar los valores de estímulo y respuesta. Si se lo hace, el sitio Web necesitará autenticarse en el simulador de *Token* Seguro para impedir que los usuarios sean llevados a conectarse a sitios Web malintencionados.

Para usar dicho abordaje, las instituciones necesitan distribuir el software a los consumidores a través de CD u otros medios físicos para evitar nuevas oportunidades de *phishing*. También es necesario que el software sea asignado con una clave específica para cada consumidor.

Una variante de dicho abordaje es la de desarrollar programas compatibles con teléfonos móviles y PDA para que los usuarios puedan llevar su autenticación con ellos y usarla en otras computadoras. El usuario necesitaría teclear su PIN y el valor de estímulo en el móvil o en el PDA, y eso, a su vez, generaría la respuesta. Entonces, el usuario teclearía el valor de respuesta en la aplicación de web para concluir la autenticación.

Ventajas

- El usuario no puede divulgar la información necesaria para realizar una transacción electrónica.
- Todos los fraudes exigen que se conozca el valor original en el simulador de Token Seguro.
- El usuario no puede optar por autenticarse para evadirse a la política de seguridad.
- Los costos de distribución de software deben ser mucho menores que los costos de la distribución de *tokens* físicos.

Desventajas

- Por sí sólo, el método no impide que el usuario provea información que se pueda usar como medio para realizar una transacción. Específicamente, la información usada para identificar una persona, por ejemplo, el apellido de soltera de la madre, todavía se puede obtener y llevar a actividades fraudulentas.
- Existe el costo de producción de los CD.
- Existen costos considerables para la implementación y el mantenimiento de la solución, incluso la distribución inicial de los CD y la revocación.

- A veces, los usuarios no poseen el software necesario cuando no están en la computadora de casa. Si se ejecuta el software ejecutado en un móvil o PDA, se puede aliviar el problema.
- El simulador de Token Seguro puede ser vulnerable a la corrupción, pues utiliza la seguridad de un sistema operativo patrón. Si el software fuese ejecutado en un celular o PDA, también se puede aliviar problema.

Recomendación

Si el costo de los *tokens* físicos es prohibitivo, se debe llevar en cuenta esta solución. Se la debe usar junto con otras tecnologías que impidan la divulgación no intencional de más información confidencial.

3.1.4 Monitorice Internet en busca de Sitios Web que puedan ser de Phishing

3.1.4.1 Monitoreo activo de la Web

Problema

La Figura 1 ilustra que el contenido de Web presente en *e-mails* de *phishing* es obtenido desde fuentes legítimas, con URL dirigidas a fuentes ilegítimas.

Abordaje

Este abordaje involucra el desarrollo de lo equivalente a las pruebas de admisibilidad de "lista blanca" de marcas comerciales y contenidos-clave. Las empresas de servicios de monitoreo implementan soluciones que utilizan agentes para monitorear continuamente el contenido de la Web, buscando activamente todas las instancias del logotipo de un cliente, de su marca comercial o de su contenido-clave de Web. La institución cliente presenta a la empresa proveedora del servicio de monitoreo una "lista blanca" de usuarios autorizados del logotipo, de la marca comercial y del contenido-clave. Cuando los agentes detectan usuarios no autorizados de logotipos, marcas comerciales u otros contenidos de la Web, la institución cliente puede tomar medidas de resolución.

Algunas empresas, tales como NetCraft [NETC] y NameProtect, ya ofrecen servicios de busca de sitios Web potencialmente fraudulentos para clientes. No está claro si el nivel deseado de respuesta automatizada ya está disponible.

Ventajas

- Los propietarios de contenido son alertados respecto a posibles usuarios clandestinos de contenido reservado.
- Órdenes de "cese y desista" son generadas como resultado del monitoreo activo de contenido y de la identificación de uso inadecuado.
- Las reglas de filtrado de *spam* pueden ser rápidamente actualizadas por los proveedores para bloquear *e-mails* que contengan referencias a sitios Web malintencionados.

Desventajas

- Exigencia del monitoreo activo.
- El desfase entre la identificación y la acción de eliminación de uso puede, asimismo, resultar en varios robos de información particular.

Recomendación

Se debe llevar en cuenta esta técnica como parte de un paquete de iniciativas de reducción del impacto económico de las amenazas de *phishing*.

3.1.5 Filtrado en el Gateway

3.1.5.1 Exploración antivirus en el Gateway

Problema

A menudo, los ataques de *phishing* involucran programas malintencionados, incluso Troyanos y programas de *backdoor* que roban información confidencial. El antivirus de *desktop* es eficaz sólo si la base de datos de reglas es actualizada regularmente.

Abordaje

Con la exploración del tráfico de la Web y del *e-mail* en la frontera de la red (*gateway*) en busca de programas potencialmente malintencionados, las instituciones pueden evitar que un gran número de códigos malintencionados logren entrar en la red. Es mucho más fácil y rápido para una gran institución actualizar un número relativamente pequeño de *scanners* de *gateway* que verificar si todos los *scanners* de *desktop* están actualizados. Las actualizaciones automatizadas de exploración de virus en *desktops* ayudan, pero todavía son más lentas que las actualizaciones para el *gateway*. Debido a la velocidad con que se propagan algunos programas malintencionados, una hora o algunos minutos pueden representar toda la diferencia.

La exploración antivirus en el *gateway* debe ser combinada con la exploración en las computadoras. Una parte del tráfico cifrado no puede ser sometida a la exploración en el *gateway*, y se la debe someter a la exploración en la computadora. Igualmente, los usuarios móviles no siempre están protegidos por el *scanner* de *gateway* cuando no están en la oficina.

Ventajas

- Se puede impedir que los códigos malintencionados entren en la red.
- La exploración en el *gateway* permite actualizaciones rápidas de un número relativamente pequeño de nodos de exploración.
- Ya existen productos eficaces de varios fabricantes.

Desventajas

- Una parte del tráfico de la red no puede pasar por la exploración.
- Los usuarios móviles no están protegidos por la exploración en el *gateway*.

Recomendación

La exploración antivirus en el *gateway* debe ser combinada con la exploración antivirus en la computadora como parte de una estrategia de defensa en niveles contra códigos malintencionados.

3.1.5.2 Filtrado de Contenido en el Gateway

Problema

Normalmente, los ataques de *phishing* involucran un sitio Web malintencionado que, en la mayoría de las veces, está activo antes de la transmisión del primer *e-mail* de *phishing*.

Abordaje

Si la institución se entera de un sitio Web de *phishing*, deberá bloquear el acceso a dicho sitio Web por la red. Puede hacerlo de varias maneras, pero principalmente con la implementación de reglas de bloqueo de las URL malintencionadas en el *gateway*. Trabajando con un proveedor de servicios de monitoreo de red, las instituciones (especialmente los ISP) pueden ser avisados anticipadamente sobre los sitios Web de *phishing* y proteger a los usuarios de su red contra el acceso a ellos.

Ventajas

- Muy eficaz para bloquear el acceso a sitios Web de *phishing* conocidos, sin esperar que el ISP lo retire del servidor.
- Ya existen productos eficaces de varios fabricantes.

Desventajas

- Puede exigir la configuración manual de *firewalls* y otros dispositivos de *gateway* para implementar las reglas de bloqueo.

Recomendación

Si la institución posee un firewall o un *gateway* adecuados, debe pensar en bloquear los sitios Web de *phishing* conocidos.

3.1.5.3 Filtrado de *spam* en el *Gateway*

Problema

No siempre los usuarios de la red logran detectar *e-mails* fraudulentos que parecen provenir de una institución legítima.

Abordaje

Como muestra la Figura 1, el filtrado de *spam* puede bloquear algunos *e-mails* fraudulentos antes de que logren alcanzar al usuario. Los *e-mails* de *phishing* son una forma específica de *spam*. En esta versión del filtrado de *spam*, la institución instala el filtrado en el *gateway* de *e-mail*. Se puede tratar el *spam* de varias maneras, incluso la marcación, (modificación del asunto), exclusión y cuarentena.

Ventajas

- Los *e-mails* fraudulentos pueden ser bloqueados antes de que el usuario pueda contestarlos, bloqueando el ataque en su estadio inicial.
- Los usuarios finales no necesitan instalar ningún software en sus PC.
- Ya existen productos eficaces de varios fabricantes.

Desventajas

- La detección de *spam* está mejorando, pero, como los remitentes de *spam* cambian constantemente sus técnicas, ninguna solución puede ser el 100% precisa. Debido a dichas imperfecciones, los usuarios pueden optar por leer todos los *e-mails* sospechosos antes de excluirlos. El usuario necesita aprender a reconocer los falsos positivos.

Recomendación

El filtrado anti-*spam* en el *gateway* debe ser implementado en redes grandes y en los ISP.

3.2 Prácticas recomendadas para el Consumidor

3.2.1 Bloquee automáticamente los e-mails malintencionados/fraudulentos

3.2.1.1 Filtrado anti-spam en la computadora

Problema

No siempre los consumidores logran detectar los *e-mails* fraudulentos que aparentemente provienen de una institución legítima.

Abordaje

Como muestra la Figura 1, el filtrado anti-spam puede bloquear algunos *e-mails* fraudulentos antes de que logren alcanzar al consumidor. Los *e-mails* de *phishing* son una forma específica de *spam*. En esta versión del filtrado de *spam*, el consumidor debe instalar un software en la computadora y configurarlo.

Ventajas

- Los *e-mails* fraudulentos pueden ser bloqueados antes que el usuario pueda contestarlos, bloqueando el ataque en su estadio inicial.
- Ya existen productos eficaces de varios fabricantes.

Desventajas

- La detección de *spam* está mejorando, pero, como los remitentes de *spam* cambian constantemente sus técnicas, ninguna solución puede ser el 100% precisa. Debido a dichas imperfecciones, los usuarios pueden optar por leer todos los *e-mails* sospechosos antes de excluirlos. El usuario necesita aprender a reconocer los falsos positivos.
- Las soluciones anti-spam para PC exigen que el consumidor compre, instale y mantenga el software. Debido a las grandes variaciones de capacidad técnica, algunos consumidores pueden no implementar la tecnología de manera eficaz.

Recomendación

Los consumidores deben pensar en comprar y usar productos de filtrado de *spam*. Deben aprender a reconocer los falsos positivos y negativos para que no ignoren las decisiones correctas que toma el filtro.

3.2.1.2 Filtrado anti-spam en el Gateway

Problema

No siempre los consumidores logran detectar los *e-mails* fraudulentos que parecen provenir de una institución legítima, y pueden no instalar el filtrado anti-spam en sus PC.

Abordaje

Como muestra la Figura 1, el filtrado anti-spam puede bloquear algunos *e-mails* fraudulentos antes de que consigan llegar al consumidor. Los *e-mails* de *phishing* son una forma específica de *spam*. En esta versión del filtrado de *spam*, el proveedor de servicios de *e-mail* instala el filtrado anti-spam en el *gateway* de *e-mail*.

Existen varias maneras de insertar el filtrado anti-spam en el ciclo de procesamiento de *e-mails*. Un abordaje en tres niveles puede contener:

- Nivel 1: Filtrado en el proveedor de servicios (ISP o servicio de *e-mail*) para todos los clientes de

- e-mail*;
- Nivel 2: Filtrado en un *appliance* de red para todos los usuarios en la LAN; y
- Nivel 3: Filtrado en cada computadora a través de aplicaciones de protección de *desktop*.

Ventajas

- Los *e-mails* fraudulentos pueden ser bloqueados antes de que el usuario pueda contestarlos, bloqueando el ataque en su estadio inicial.
- Con el filtrado en un proveedor de servicios o en un *appliance* de red, el consumidor no necesita instalar ningún software.
- Si el proveedor de servicios excluye mensajes sospechosos, el consumidor nunca abrirá nada que haya sido detectado.
- Ya existen productos eficaces de varios fabricantes.

Desventajas

- Las instituciones atacadas no pueden controlar si los ISP de sus clientes proveen filtrado de *spam* en el *gateway*.
- La detección de *spam* está mejorando, pero, como los remitentes de *spam* cambian constantemente sus técnicas, ninguna solución puede ser el 100% precisa. Debido a dichas imperfecciones, los usuarios pueden optar por leer todos los *e-mails* sospechosos antes de excluirlos. El usuario necesita aprender a reconocer los falsos positivos.

Recomendación

Muchos ISP y muchas instituciones ya proveen filtrado de *spam* en sus *gateways* de *e-mail*. Si su ISP no lo provee aún, pídale que lo haga.

3.2.2 Detección y exclusión de programas malintencionados

3.2.2.1 Software Antivirus y Anti-spyware

Problema

Los programas espías (*spyware*) interceptan invisiblemente las comunicaciones entre el consumidor y las instituciones legítimas.

Abordaje

Como muestran las Figuras 2 y 4, el *spyware* puede ser distribuido a los consumidores por *e-mail* y, posteriormente, interceptar comunicaciones legítimas entre los usuarios y sitios Web legítimos. Muchos consumidores ya instalaron programas antivirus, que ayudan a reducir el riesgo de dicha forma de ataque. Los programas antivirus detectan muchas formas de programas malintencionados (*malware*), incluso el *spyware*, pudiendo excluirlo cuando se lo encuentre. La mayoría de los programas antivirus funciona de manera casi invisible para el consumidor, afectando poco a sus operaciones normales. Los programas anti-*spyware* pueden explorar la computadora en busca de posibles programas espías, y son, en general, capaces de eliminarlos.

Ventajas

- Detecta y excluye el *spyware* antes de que logre interceptar información confidencial.
- Existen pocos falsos positivos.

Desventajas

- La detección es imperfecta, pero está mejorando.
- Los archivos de características (“firmas”) necesitan actualización regular; de lo contrario, el software pierde su eficacia contra los ataques más recientes.
- A veces, el software anti-*spyware* puede eliminar algunos “programas espías” necesarios para la operación correcta de programas legítimos. Normalmente, se avisa al consumidor cuando la eliminación del *spyware* tiene dicha consecuencia.
- El consumidor debe comprar e instalar el software, a menos que el proveedor de la computadora instale una versión previamente, antes de la compra.

Recomendación

Los consumidores deben instalar programas antivirus, con opciones activadas para detectar programas potencialmente indeseables. Los consumidores también deben mantener sus programas antivirus actualizados. También deben pensar en instalar una de las aplicaciones gratis de detección de *spyware*. Deben cuidar para instalar una aplicación confiable de detección de *spyware*, pues algunas vienen siendo acusadas de ser programas espías.

3.2.3 Bloqueo automático del envío de información confidencial a terceros malintencionados

3.2.3.1 Servicio de privacidad de *desktops*

Problema

Como muestra la Figura 3, los usuarios pueden ser inducidos a enviar datos confidenciales a sitios Web inseguros y malintencionados.

Abordaje

Paquetes de software disponibles en el mercado pueden monitorear el tráfico de Web saliente respecto a un conjunto de datos que el usuario puede definir. Normalmente, los datos definidos son información que identifican al usuario, tales como nombre, CPF y números de tarjetas de crédito. Si se encuentra cualquiera de dichos conjuntos de datos en uno de los paquetes enviados, el paquete se queda retenido hasta que el usuario confirme si los datos deben ser enviados al destino verdadero, o si se debe interrumpir la transmisión de los datos. Si el usuario indica que los datos no deben ser enviados, los datos confidenciales son eliminados del paquete.

Una de las dificultades para los consumidores con ese tipo de producto es identificar la información confidencial que se debe proteger, además de los sitios Web específicos que se deben poner en listas de liberación/bloqueo. Cuando se mantiene correctamente la información, dichos productos pueden hacer un trabajo muy eficaz de prevención de una amplia gama de ataques de *phishing*.

Ventajas

- Ya existen productos disponibles hoy día en el mercado.
- Aunque la URL de destino pueda no ser aparente al consumidor, el software logra ver el verdadero destino y bloquea la divulgación indeseable de la información.

Desventajas

- Exige la instalación de software en la computadora del consumidor.

Recomendación

Este abordaje es esencial para bloquear algunos ataques de ingeniería social que serán exitosos a pesar de la autenticación segura, del antivirus, del anti-spyware y de los programas anti-*spam*. Los consumidores ya pueden instalar dichos productos.

3.2.4 Siempre desconfíe

3.2.4.1 Teclee las direcciones de la Web y verifique su autenticidad

Problema

Varias exploraciones pueden ocultar la verdadera dirección de Web de un enlace aparente y redirigir el navegador a un sitio Web de *phishing*.

Abordaje

Existen varias maneras por las cuales un *phisher* puede hacer que un *e-mail* parezca legítimo. Además, puede ser difícil determinar la verdadera dirección de Web detrás de enlaces incorporados en *e-mails*. Generalmente, es más seguro teclear en el navegador la dirección de Web deseada que pulsar en enlaces incorporados. Si usted no está seguro sobre la autenticidad de un *e-mail*, contacte directamente con la institución remitente.

Ventajas

- No se necesita ningún otro software

Desventajas

- Direcciones de Web largas son aburridas de teclear y propensas a errores.
- Puede ser difícil verificar algunos *e-mails*.

Recomendación

Conozca la política de su institución respecto a la solicitud de información personal confidencial. En caso de duda, consulte a la institución por teléfono o a través de un *e-mail* para un contacto que usted ya conozca.

4 Conclusión

El *phishing* es distinto a las estafas tradicionales en la escala del fraude que se puede cometer. Los artistas de las estafas existen hace siglos, pero el *e-mail* y la Red Mundial les brindaron las herramientas para alcanzar a miles o millones de víctimas potenciales en cuestión de minutos, a un costo prácticamente inexistente. Con los ataques de *phishing*, los estafadores todavía necesitan conquistar la confianza del consumidor para que logren éxito. Como no existe contacto personal entre el atacante y el consumidor, el consumidor cuenta con muy poca información para decidir si un *e-mail* o sitio Web es legítimo.

La solución técnica definitiva para el *phishing* involucra alteraciones considerables en la infraestructura de Internet cuya implementación está más allá de la capacidad de cualquier institución. Sin embargo, existen medidas que se pueden tomar inmediatamente para reducir la vulnerabilidad del consumidor a ataques de *phishing*. Aquí están algunas:

Para las Empresas:

- Establecer políticas corporativas y divulgarlas a los consumidores.
- Darle al consumidor una manera de verificar la legitimidad de los *e-mails*.
- Autenticación más robusta en los sitios Web.
- Monitorear Internet en busca de posibles sitios Web de *phishing*.
- Implementar soluciones antivirus, de filtrado de contenido y anti-*spam* de buena calidad en el punto de contacto (*gateway*) con Internet.

Para los Consumidores:

- Bloquear automáticamente *e-mails* fraudulentos/malintencionados.
- Detectar y excluir automáticamente programas malintencionados.
- Bloquear automáticamente el envío de información confidencial a terceros malintencionados.
- Desconfiar siempre.

Todas las tecnologías susodichas ya están disponibles y los consumidores y las instituciones interesadas en proteger a sus clientes ya las pueden implementar.

5 Agradecimientos

Además de los autores mencionados en la cubierta, los siguientes científicos e ingenieros de McAfee Research contribuyeron con este *white paper*:

Brian Appel
David Carman
Mark Feldman
Michael Heyman
Jin Horning
Roger Knobbe
Patrick LeBlanc
Erik Mettala
Steve Schwab
Deborah Shands

6 Referencias bibliográficas

[APWG] *Grupo de Trabajo Anti-Phishing*, "Propuestas de Soluciones para la Amenaza de Estafas de Falsificación de E-mails", diciembre de 2003.

[APJA] *Grupo de Trabajo Anti-Phishing*, "Informe de Tendencias de Ataques de *Phishing*, enero de 2004".

[APAP] *Grupo de Trabajo Anti-Phishing*, "Informe de Tendencias de Ataques de *Phishing*, abril de 2004".

[APJU] *Grupo de Trabajo Anti-Phishing*, "Informe de Tendencias de Ataques de *Phishing*, junio de 2004".

[ASRG] Grupo de Investigaciones Anti-Spam, <http://asrg.sp.am/index.shtml>.

[CNET] McCullagh, Declan, "Treasury breaks word on e-mail anonymity," <http://news.com.com/2100-1028-5137488.html>, CNet News.com, 8 de enero de 2004.

[GEMP] *GEMPLUS S.A.*, "Folleto GemAuthenticate", 2003.

[KOPR] *Koprowski, Gene J.*, "Cuidado con las Estafas de Falsificación", UPI Technology News, enero de 2004.

[MAST] *MasterCard International, Inc.*, "Oportunidades de Crecimiento OneSmart: Tres Paquetes de Creación de Negocios para Emisores", 2003.

[NETC] *NetCraft Ltd*,

http://news.netcraft.com/archives/2004/01/02/phishing_identity_theft_and_banking_fraud_detected.html, 2004.

[SPF] M. W. Wong, M. Lentzner, "El Formato de Registros SPF y Protocolo de Pruebas", IETF MADRID Borrador para Internet, 11 de julio de 2004.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del cliente. El equipo McAfee PrimeSupport® de técnicos de soporte colaboradores y altamente cualificados brinda soluciones hechas a la medida, brindando asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas clientes. McAfee Research, líder mundial en sistemas de información e investigaciones de seguridad, sigue encabezando la innovación en el desarrollo y el refinamiento de todas nuestras tecnologías.

McAfee, IntruShield, Protection-in-Depth, Entercept, Intrusion Intelligence y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo asociado a la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. © 2004 Network Associates Technology, Inc. Todos los derechos están reservados.