Métodos de autenticación en el Webmail

Estos documentos han sido escritos y publicados por:

Chema Alonso, MVP de Windows Security y escribe diariamente en su blog de "Un Informático en el lado del mal".

Chema trabaja en Informática 64 y escriben en los blogs Un Informático en el lado del mal y vista-tecnica

Recopilación: Cristian Borghello, Director de www.segu-info.com.ar - V1.0 – 090801

Publicado en Segu-Info

Correos falseados en Yahoo!, Gmail y Hotmail

(I) http://elladodelmal.blogspot.com/2009/06/correos-falseados-en-yahoocom-gmailcom.html

(II) http://elladodelmal.blogspot.com/2009/06/correos-falseados-en-yahoocom-gmailcom_09.html

(III) http://elladodelmal.blogspot.com/2009/06/correos-falseados-en-yahoocom-gmailcom_11.html

(IV) http://elladodelmal.blogspot.com/2009/06/correos-falseados-en-yahoocom-gmailcom_14.html

(V) http://elladodelmal.blogspot.com/2009/06/correos-falseados-en-yahoocom-gmailcom_23.html

Hace ya mucho tiempo que escribí un artículo sobre el famoso filtro Sender ID que implementó Spectra a partir de lo que inicialmente iba a ser el ***Checker ID*** pero que acabó haciendo uso del registro de ***Sender Policy Framework*** (***SPF***) con el objetivo de intentar añadir una nueva forma de detectar correos con direcciones de remitente falsificadas. No garantiza que el correo sea legítimo, pero intenta detectar cuando es claramente ilegítimo.

El registro original creado para Sender Policy Framework es identificado en los servidores DNS como *v=spf1* y se creó para identificar el servidor usado en el comando ***HELO*** y el dominio que se utiliza en la dirección configurada en ***MAIL FROM***.

Sender ID utilizar el registro ***SPF*** del DNS pero intenta identificar más elementos. Aparecerá en los registros DNS como *v=spf2.0*, pero con uno de los siguientes modos: *spf2.0/mfrom,pra*; *spf2.0/mfrom* o *spf2.0/pra*. Esto es porque Sender ID intenta validar no sólo el servidor que aparece en ***HELO*** y el dominio en ***MAIL FROM***. En este caso se añade también a la comprobación una ecuación llamada ***PRA (Purported Responsible Address)*** que se saca de comprobar la dirección que aparece en: ***MAIL FROM***, ***SENDER***, ***RESENT-FROM***, ***RESENT-SENDER***. Si existe la validación *spf2.0/pra* en el filtro ***Sender ID***, estas cuatro tienen que ser la misma y además deben estar en el registro ***SPF*** del servidor DNS. Un filtro *v=spf1* será equivalente a un *v=spf2.0/mfrom*.

El filtro ***SPF*** y ***Sender ID*** son similares, ambos usan el mismo registro, la misma configuración, pero si se configura ***Sender ID*** con la validación *spf2.0/pra* algunos mails en listas de correo pueden dar problemas al ser tomados como no autenticados.

La idea es que las empresas marquen las IPs por las que sale el correo legítimo de su organización mediante un registro txt en el dns de tipo spf. Así, las empresas receptoras de correos desde esos dominios sólo tienen que consultar al DNS y ver si la IP que le entrega el correo de ese dominio es uno de las válidas

siguiendo la política de ***Sender Policy Framework*** o la de ***Sender ID***. ¿Y si no la cumple?

Pues si un correo del dominio A viene desde una IP que no está en la lista de direcciones IP legítimas para enviar correo marcadas por la empresa A….¿qué se debería hacer con él? Seguro que la mayoría pensáis que se debería tirar a la basura. La pregunta es… ¿se está usando masivamente?

Yahoo!, por su parte, optó por seguir una estrategia distinta mediante de la firma del correo legítimo y olvidarse de la solución simple del registro ***SPF*** en el DNS. En su caso, si el mensaje no va firmado por ***Yahoo!*** entonces debe tomarse como un correo ilegítimo. Para eso utiliza el protocolo DKIM (Domain Keys identified Mail) y cualquier servidor que recibe el correo puede comprobar la firma del mismo ya que la clave pública utilizada para firmar el correo se encuentra en el servidor DNS. La idea de ***Yahoo!*** es que si el correo no llega firmado por los servidores de ***Yahoo!*** entonces puede ser falso.

En el esquema de ***SPF/Sender ID*** cabe la posibilidad del falseo de direcciones IP o del DNS Spoofing (que se lo digan a Kamisky). El otro problema que sucede es que un mail puede ser enviado desde una IP falsa pero que aparezca como enviado por alguien legítimo, como si fuera una lista de mails. Para evitar esto los clientes de correo intentan dejar, cada vez más claro, cuando alguien envía el correo en lugar de otro.

En el esquema de autenticación por el que apuesta ***Yahoo!*** no cabe estos problemas, o el correo es enviado por un servidor de ***Yahoo!*** que lo firma o no. Sin embargo no se ha impuesto masivamente y la mayoría de los servidores no implementan la interpretación de la firma. Sin embargo, el problema del DNS le seguiría afectando.

Ahora, conociendo estas configuraciones, la pregunta es.. ¿cómo se comportará cada uno de ellos ante la recepción de correos con direcciones falseadas o no falseadas?Para hacer estas pruebas primero se comprueba si tienen configurado el registro SPF los dominios de prueba: Gmail.com, Yahoo.com y Hotmail.com. Se puede comprobar con esta URL: Consulta registro SPF

Hotmail.com configura registro SPF v=spf1

Gmail configura el registro SPF en v=spf1

Yahoo! no configura registro SPF

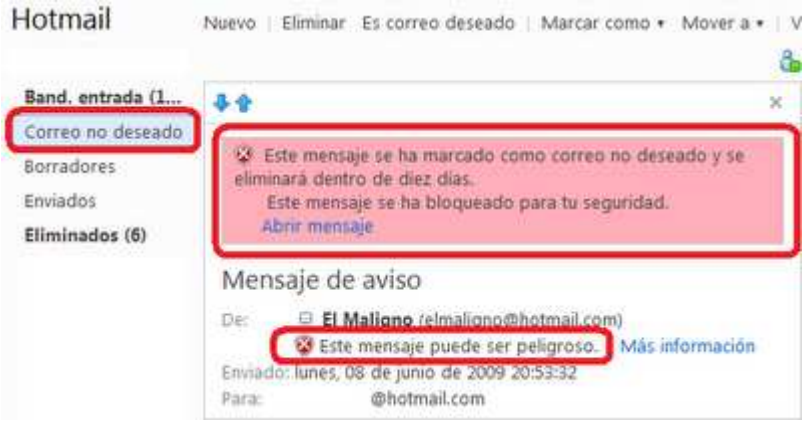
Los resultados son que Gmail y Hotmail configuran sus registros SPF pero Yahoo.com no lo hace, ya que usa DKIM. La pregunta es.... ¿cómo implementan el reconocimiento de correos legítimos o falseados en la práctica?

Para comprobar las medidas de detección de correos ilegítimos, se han enviado mails con todas las posibilidades, legítimos, ilegítimos, con y sin spf, con y sin DKIM e incluso legítimos sin spf enviados desde el MX. Estos son los resultados.

Hotmail

Hotmail recibe un correo desde una dirección falsa de Hotmail

Si enviamos un correo con una dirección de email suplantando a un remitente de Hotmail, el resultado es que el correo va a la carpeta de spam con una alerta roja y se identifica el correo como potencialmente peligroso. Entra en la carpeta de spam porque está marcado como softfail en el registro spf con la opción ~all.



Hotmail detecta suplantación de su dominio

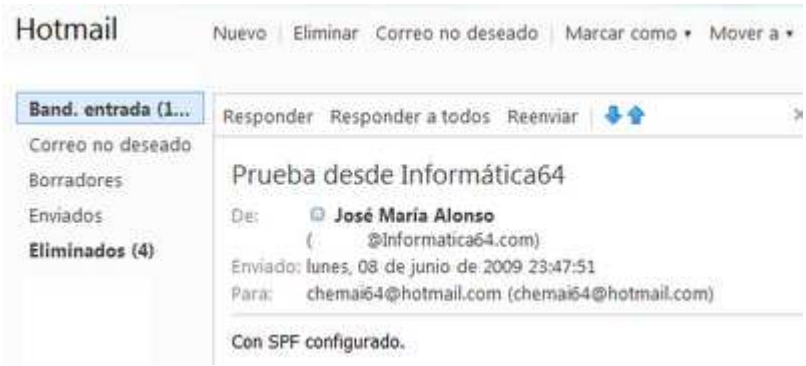
Hotmail recibe un correo falso desde una dirección de un dominio con SPF

Si se envía el correo con una dirección falseada de una empresa que tiene registro SPF, como por ejemplo de Gmail, el correo aparece en Hotmail en la carpeta de spam como sospechoso y con una alerta amarilla que indica que es posible que ese no sea un remitente conocido. En este caso desde Gmail que también los marcar como softfail.

Detecta que no viene de una IP en el SPF y lo mete en la carpeta de spam

Hotmail recibe un correo legítimo de un dominio con SPF

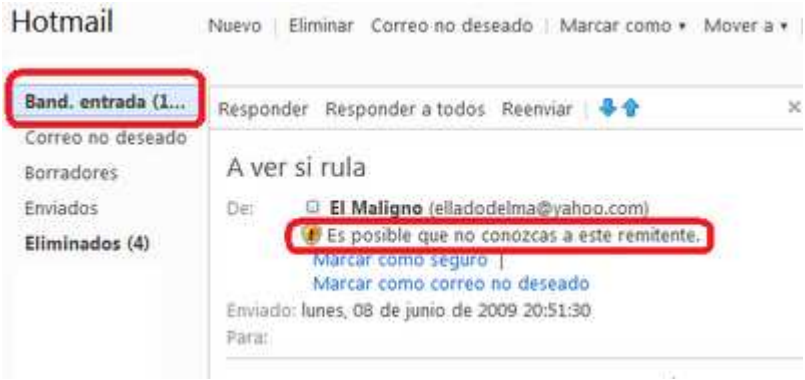
Como era de esperar, se comprueba el regisro SPF, es correcto y lo pone en la bandeja de entrada sin ninguna alerta de seguridad.



Correo desde Informática64

Hotmail recibe un correo desde una dirección falsa de un dominio sin SPF

Si se envía el correo con una dirección falseada de una empresa que NO tiene registro SPF, este aparece en la Bandeja de Entrada, pero con una alerta similar. En este caso el correo está enviado con una dirección falsa desde Yahoo.com.



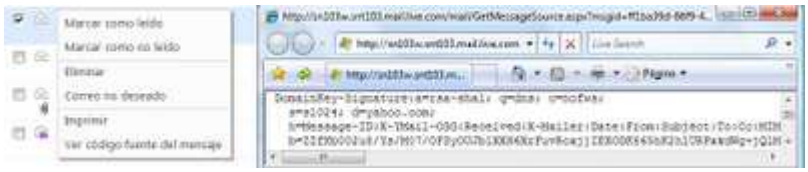
El filtro de comprobación SPF no detecta si es o no legítimo y lo pone en el inbox con una alerta

Hotmail recibe un correo legítimo de una dirección de un dominio sin SPF pero que viene firmado con DKIM

En este caso se ha enviado un correo electrónico válido desde una dirección de Yahoo.com. Hotmail no es capaz de decir que el correo es falso, ya que no hay registro SPF y lo marca con una alerta.

Correo legítimo marcado

Sin embargo, el correo es legítimo y viene firmado con el protocolo DKIM como se puede ver en la cabecera del mismo correo.

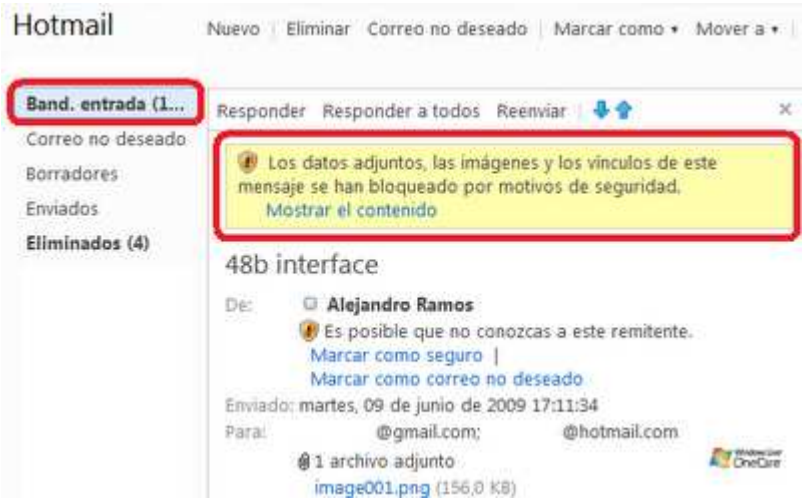


Correo firmado con DKIM. No garantiza el emisor, pero sí que ha salido de ese servidor.

Esta comprobación es desaprovecha por Hotmail a la hora de legitimar el correo. Es posible ver que el correo está firmado correctamente en la cabecera SMTP del correo.

Hotmail recibe un correo legítimo desde un dominio sin SPF pero que es envíado desde un servidor MX

Otra de las comprobaciones que se prueba es enviar un correo legítimo desde un dominio sin registro spf pero que sale desde un servidor MX del dominio. Puede ser que correo legítimo de un dominio llegue desde IPs distintas a las de los intercambiadores de correo, pero si el correo llega desde el MX entonces se puede decir que es legítimo. Así que, en el caso de que una organización no tenga spf, pero su correo salga desde el MX existen herramientas para comprobar que es legítimo. En este caso, Hotmail no comprueba esta opción y el correo, que es legítimo, queda sin embargo marcado con una alerta de seguridad.



Correo legítimo enviado de la IP de un MX sin registro SPF ni DKIM

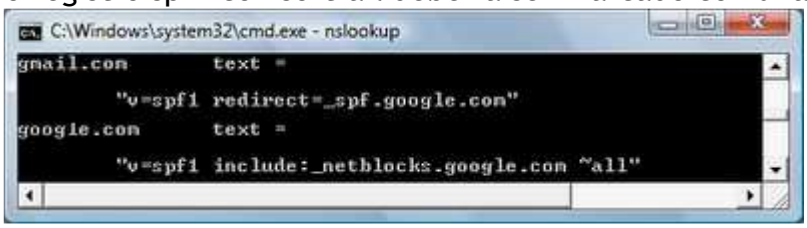
En resumen, Hotmail implementa su registro spf1 con softfail, comprueba su suplantación y la suplantación de los demas dominios mediante Sender ID, pero no realiza ninguna comprobación DKIM ni MX para quitar alertas de seguridad a correos legítimos.

GMail

Gmail ha sido, quizás, de estos tres sistemas de correo electrónico en web el que menos me ha gustado. Es curioso ver como Gmail se decanta por dar al resto de los servidores de correo el máximo posible de información para que validen los correos emitidos desde gmail.com, pero, por el contrario, el no realiza ninguna validación correcta. Gmail parece querer relegar todo su control contra correos ilegítimos en la herramienta web a su filtro Anti-spam. Sin embargo, llama poderosamente la atención como a nivel de servidor SMTP sí valida todo. Veamos las pruebas.

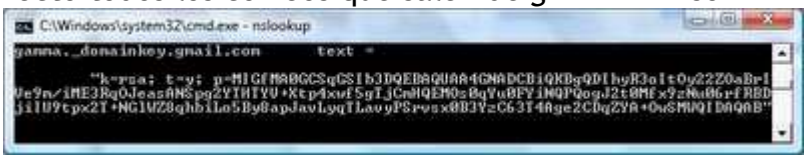
Gmail recibe un correo con una dirección falsa de remitente desde Gmail.com

Este correo, viene desde una IP que no está en el SPF de *gmail.com*, así que, según su propio registro spf1 con softfail debería ser marcado con una alerta.



Registro spf de gmail.com

Además, este correo no viene firmado con DKIM por uno de los servidores de Gmail, cuando por defecto todos los correos que salen de *gmail.com* son firmados.



Clave pública gamma utilizada para firmar correos gmail.com

Conclusión, debía de dar una alerta de posible correo ilegítimo y no la da. Mal hecho.

El correo entra en la bandeja de entrada sin alerta

Gmail recibe un correo con una dirección falsa de un dominio con SPF

Como era de esperar, el correo no recibe ninguna alerta de peligrosidad o falsedad. Sin embargo, es curioso, pues Gmail sí tiene esa información. Si se

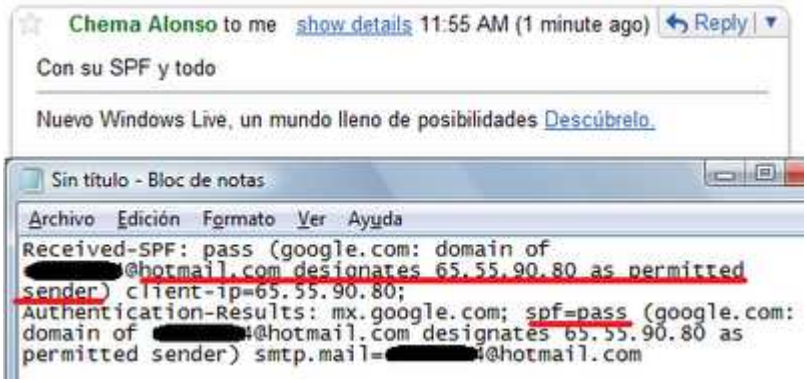
echamos un vistazo a la cabecera original del mensaje se puede ver que el mensaje no pasa la validación SPF e incluso, como Hotmail marca la IP de origen como una NO permitida.

Correo falso con remitente hotmail.com y cabecera

Esa información podía ser utilizada por Gmail para poner una alerta, pero no lo hace. Mal hecho.

Gmail recibe un correo legítimo de un servidor con SPF

Ya que no da alertas negativas de correos no comprobados, se podía utilizar una aproximación distinta y mostrar alertas positivas para correos sí validados. Para ver si hay alguna diferencia entre el legítimo y el falso se ha enviado un correo desde una cuenta legítima de Hotmail. El correo pasa el filtro SPF pero la herramienta NO da ninguna alerta positiva. Es decir, en la herramienta web no se ve ninguna diferencia entre el que NO pasa y el que pasa el filtro SPF.



Correo Legítimo que pasa el filtro spf como se ve en la cabecera

Tiene herramientas para diferenciar un correo que viene de un Sender autorizado y otro que no, pero no lo hace. Mal hecho

Gmail recibe legítimo desde un dominio sin SPF pero que envía desde el MX

Al no mostrar ninguna alerta en correos que no pasan el SPF, no tiene mucho sentido hacer esta prueba, pues con una comprobación de este registro sólo se

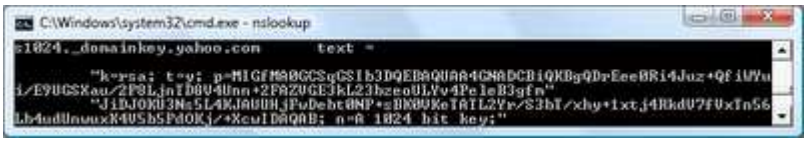
podrían validar correos cuando vengan desde la IP de un MX legítimo desde un dominio sin registro SPF en el DNS.

Legítimo desde un server marcado en el MX

El cliente Web de Gmail, de nuevo, no muestra ningún cambio. Mal hecho.

Gmail recibe un correo falso de un servidor que firma sus mensajes con DKIM

Para hacer esta prueba se utiliza *Yahoo.com* que firma todos sus correos salientes con DKIM.



Clave pública s1024 de Yahoo.com utilizada para firmas correos

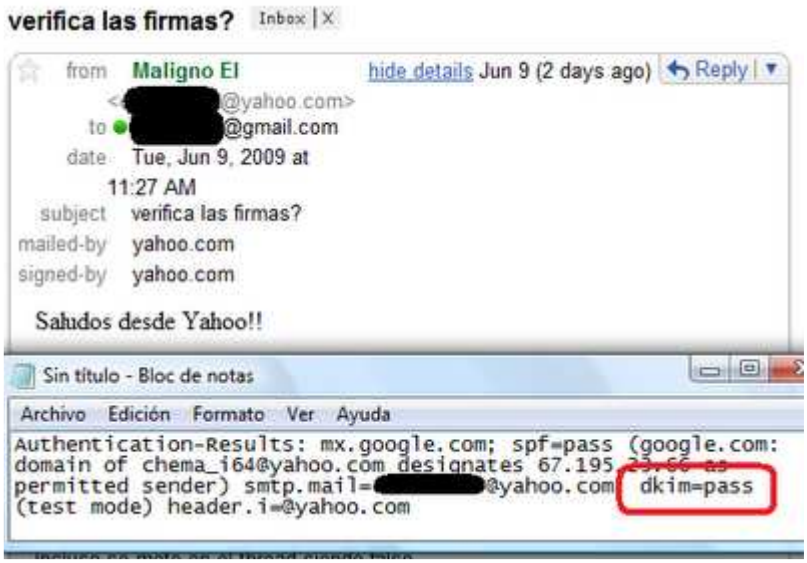
Sin embargo, en este caso, este correo no viene firmado, por lo que no se puede dar ninguna alerta positiva.

Correo sin firmar recibido desde Yahoo

Como se puede apreciar en la imagen anterior el mensaje se ve sin ninguna alerta negativa de no estar firmado.

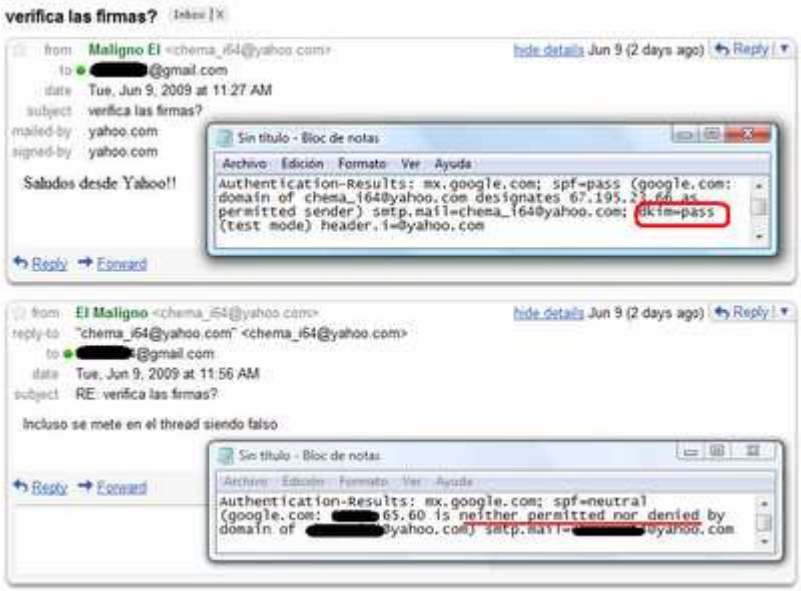
Gmail recibe un correo legítimo firmado con DKIM

En este caso Gmail comprueba correctamente la firma DKIM del correo recibido. Esto se puede ver en la cabecera del correo original.Sin embargo, el cliente web de Gmail no muestra una alerta positiva en el interface de que el correo ha sido validado.



Gmail comprueba firma DKIM pero no alerta de ello. Mal hecho.

La diferenciación entre correos legítimos o no legítimos sin alertas funciona tan ***sumamente mal*** que es posible enviar un correo falso dentro de la conversación de un correo legítimo y gmail los intercala como si ambos fueran buenos sin dar ninguna alerta. Sólo hay que poner el ***RE:*** en el asunto del mensaje.



Correo legítimo y correo falso en el mismo thread

Conclusiones GMail

1) Gmail firma sus mensajes salientes con DKIM y comprueba la firma DKIM de los entrantes, pero sin embargo no muestra ninguna alerta negativa de los no firmados ni positiva de los firmados.

2) Gmail autentica con el registro SPF los servidores de correo saliente legítimos y comprueba si el correo viene de un servidor autorizado por el SPF.

3) El cliente Web de Gmail no muestra ninguna alerta, ni negativa ni positiva, de si se ha comprobado o no. Al no mostrar alertas negativas por correos que no vengan desde una IP autorizada por el SPF no da ayudas a un usuario a detectar una posible falsificación.

4) Gmail mezcla en el interface tanto los correos legítimos como los no legítimos.

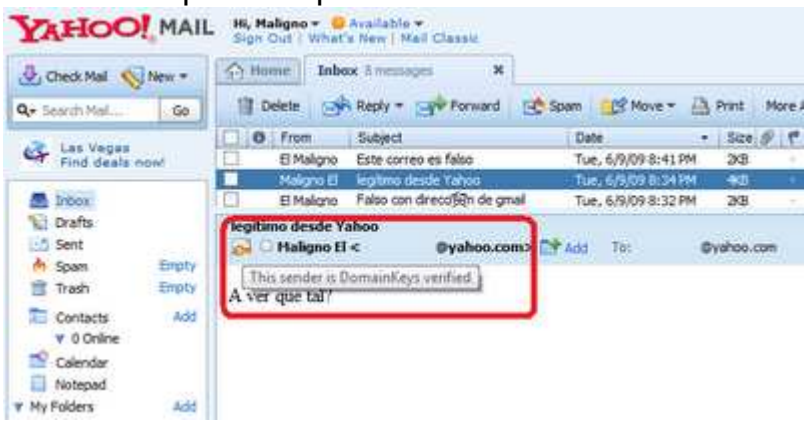
En resumen, aunque desde el interface es posible acceder a la cabecera original del mensaje recibido, Gmail por web no ayuda para nada a los usuarios a detectar posibles correos falseados. Los servidores de correo, por el contrario, hacen los deberes y tienen tanto las comprobaciones SPF como DKIM implementadas. La herramienta Web tiene que mejorar en este aspecto.

Yahoo!

El último de los correos web analizados en este artículo es el de Yahoo! El sistema por el que apuesta este servicio está basado en el uso de DKIM. Para ello, como se vio en la tercera parte de esta serie, Yahoo! publica las claves públicas con las que los servidores firman los correos legítimos que salen de ellos. Por otro lado, como ya se vio en la primera parte, Yahoo! no tiene tan siquiera configurado el registro SPF en los servidores DNS. Conociendo esta configuración inicial, los resultados con las pruebas son los siguientes.

Yahoo! recibe un correo electrónico de una cuenta legítima de Yahoo.com

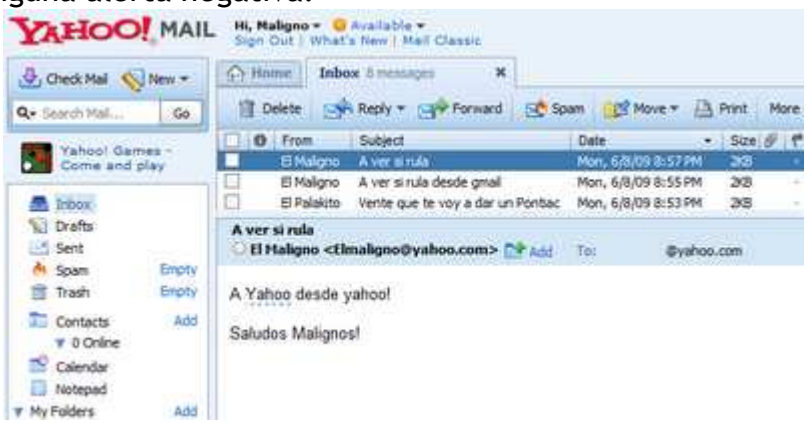
En este caso, el correo aparece firmado por uno de los servidores de Yahoo! utilizando una cabecera DKIM. Yahoo! lo comprueba y le muestra al usuario una alerta positiva, garantizando la veracidad de procedencia de este correo. Éste es el único de los tres sistemas de correo que muestra alertas positivas en los correos recibidos garantizando las pruebas que se han realizado.



En la bandeja de entrado y con alerta positiva

Yahoo! recibiendo un correo electrónico falso desde un dominio Yahoo.com

Como es de suponer, este correo no llega firmado por ningún servidor, por lo que no puede comprobar ninguna firma DKIM. Sin embargo, la política de Yahoo! es no mostrar ninguna alerta negativa.



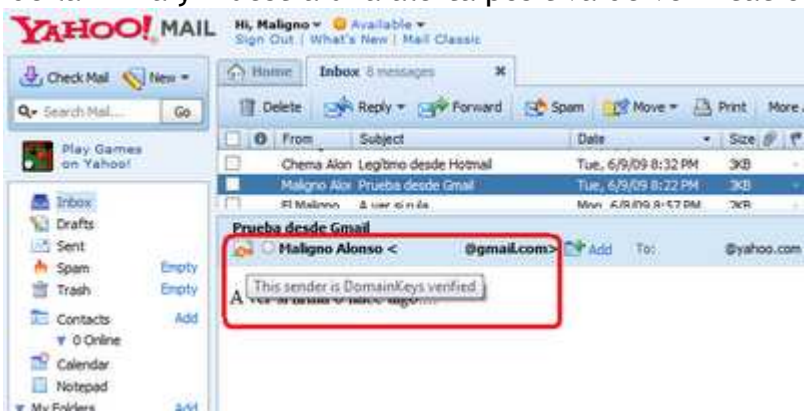
Sin alerta a la bandeja de entrada

Esto es porque la configuración que tiene el sistema DKIM de Yahoo! en sus servidores es de *softfail*, es decir, no garantiza que todos los correos que salen de los servidores de Yahoo! salgan firmados, lo que ayuda bastante poco. Al igual que Hotmail configura sus registros *spf* con *softfail*, no garantizando que todos los correos lleguen desde Hotmail, Yahoo! hace algo similar. En este caso se realiza con la opción ***~o*** en lugar de con la opción ***-o*** en el registro de tipo *txt* *_domainkey.yahoo.com* de los servidores DNS. El sistema, como se puede apreciar con el operador ***t=y*** indica que se encuentra en modo test, es decir, en pruebas.

Configuración DKIM en Yahoo.com

Yahoo! recibiendo un correo legítimo firmado con DKIM

Para realizar esta prueba se ha enviado un correo desde Gmail. Este servido firma los correos con DKIM y pueden ser comprobados. Yahoo! realiza la comprobación de la firma y muestra una alerta positiva de verificación.



A la bandeja de entrada y con alerta positiva

Yahoo! recibiendo un correo falso de un dominio que firma con DKIM

En la prueba primera, en la que se veía el comportamiento con un correo falso de *yahoo.com*, se puede ver cómo reacciona, es decir, sólo muestra alertas positivas si puede comprobarlo. No muestra ninguna alerta y cae en la bandeja de entrada.

Sin alerta negativa y en la bandeja de entrada

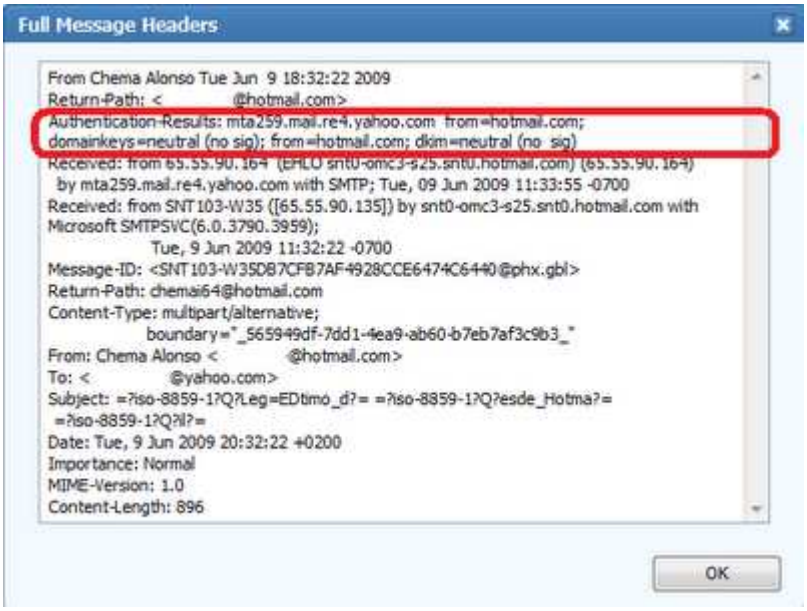
Sin embargo, al hacerlo con Gmail el resultado es curioso. Mientras que Gmail sí tiene publicadas las claves de firma, como se vio en la tercera parte del artículo, no publica la configuración de DKIM en el DNS. Para ello debería existir un registro *_domainkey.gmail.com* de tipo *txt* en el servidor DNS que **NO** existe. Se ha de suponer que el sistema está en test y no garantiza que todos los correos lleguen firmados.

Yahoo! recibiendo un correo legítimo desde un servidor con SPF configurado

Sorprende que Yahoo! no haga ningún aprecio a los registros SPF. En este caso el registro es legítimo y Yahoo! no muestra ninguna alerta positiva de comprobación del correo.

Sin alerta postiva, en la bandeja de entrada

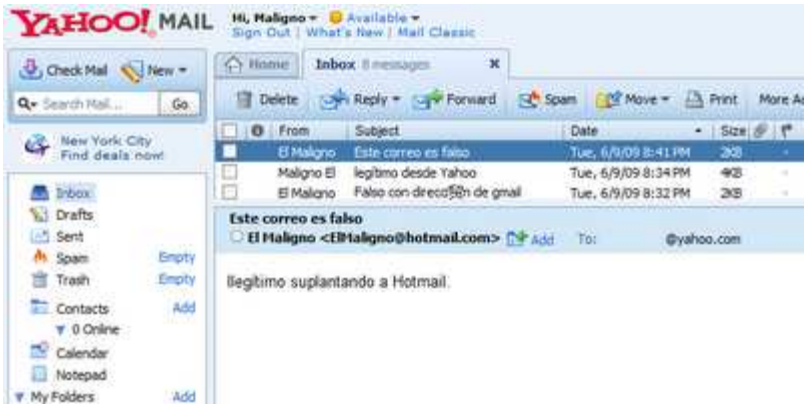
Se puede ver, mirando la cabecera del correo electrónico, que Yahoo!, a diferencia de Gmail que consultaba el registro pero no mostraba ninguna alerta, directamente no realiza la comprobación al servidor DNS.



En la cabecera sólo comprueba DKIM, no comprueba SPF

Yahoo! recibiendo un correo falso desde un servidro con SPF configurado

Como era de esperar, la validez del correo electrónico recibido es exactamente la misma que si fuera legítimo. Al obviar directamente el registro SPF se pierde mucha información.



Sin alerta a la bandeja de entrada

Yahoo! recibiendo correos legítimos desde dominios sin SPF usando el MX

Una de las garantías de validez de un remitente que se puede añadir, como ya se comentado en lo que va de artículo, es que el correo venga desde un dominio que no tiene configurado el registro SPF, pero viene desde uno de los servidores MX. Yahoo! al no hacer aprecio directamente al registro SPF anula cualquier uso que se pueda dar al registro MX para validar un correo, por lo que le da exactamente igual si es legítimo o no.

Conclusiones Yahoo!

Yahoo! realiza correctamente las validaciones de correos que vienen firmados con DKIM mostrando una alerta positiva. Sin embargo, el no consultar los registros SPF parece una limitación enorme y una pérdida de información que no traslada al usuario para ayudarle a tomar una decisión. Además, a diferencia de Gmail, no realiza la comprobación, con lo que no vale con leer la cabecera completa del mensaje para saber si es legítimo o no y es labor del usuario realizar las pruebas contra los servidores DNS. Por supuesto, tampoco realiza comprobación MX.

En resumen, deja muchas validaciones sin realizar.

Comprobaciones para saber si un correo es legítimo o no

La pregunta que uno se puede realizar es … ¿por qué no se utilizan todas las medidas disponibles? Supongo que es el eterno problema de balance entre seguridad y carga de trabajo, porque si no, no parece demasiado lógico.

Teniendo en cuenta que todas las cabeceras SMTP pueden ser comprobadas desde los interfaces web de Gmail, Hotmail y Yahoo!, el siguiente es un árbol de decisión que se puede aplicar para decidir si un correo recibido es o no legítimo. Hay que tener presente que se tiene como base supuesta que:

A) No hay un bug de DNS como el descrito por Kaminsky.

B) Realizar IP Spoofing hoy en día en consultas al DNS en Internet es difícil.

C) La conexión es desde una red segura sin MITM.

Si esos condicionantes se dan en tu situación, entonces es posible realizar el siguiente algoritmo para obtener más y mejor información sobre la legitimidad de un correo electrónico.

PRIMERO: Comprobación de DKIM

A) Si el correo viene firmado con DKIM y está comprobado deberemos tomar el correo como Legítimo.

- *Yahoo!*: Se hace automáticamente y pone un icono de autenticado.
- *Gmail*: Realiza la comprobación pero sólo aparecen en la cabecera SMTP y no en el interfaz web. Hay que comprobar que la firma DKIM aparezca como autenticada.
- *Hotmail*: no realiza la comprobación DKIM por lo que en la cabecera SMTP aparecerá la cabecera DKIM pero hay que hacer la comprobación de la firma manualmente (Poco divertido).

B) Si no viene firmado se debe comprobar la política del servidor DNS de la organización respecto a DKIM comprobando si existe política de fallo respecto a DNS, es decir, si en el registro *_domainkey.dominio.com* aparece la opción ***o*=-**.

a. Si aparece la opción ***o*=-** entonces el correo deberá ser tomado como Ilegítimo.

b. Si no aparece la opción ***o*=-** porque o no hay política, como en el caso de *Gmail*, o aparece la opción ***o*=~**, se debería pasar al paso SEGUNDO.

SEGUNDO: Comprobación de firma SPF

Se comprueba el registro SPF del dominio del remitente.

A) Si este tiene registro SPF se comprueba la dirección del servidor de envío contra la lista de IPS permitidas por el registro SPF y la política spf de comprobación: *spf1 - spf2/mfrom - spf2/mfrom,pra - spf2/pra*.

a. Si la IP cumple y los valores del remitente o del pra entonces se marca el

correo como Legítimo.

- *Hotmail* lo pone en la bandeja de entrada sin alertas.
- *Gmail* hace la comprobación pero sólo se puede ver en la cabecera SMTP del correo.
- *Yahoo!* no hace la comprobación y habría que realizarla manualmente (poco divertido).

b. Si no, se comprueba la política de *fail* o *softfail*:

- *-all*: Se debería marca como Ilegítimo.

- *Hotmail* lo hace automáticamente y el correo llega con alerta roja a la carpeta de SPAM
- *Gmail* lo comprueba pero sólo se puede ver en la cabecera SMTP.
- *Yahoo!* no lo comprueba.

- *~all*: Se debería marcar como Dudoso.

- *Hotmail* lo pone con una alerta en amarillo en la carpeta de correo no deseado.
- *Gmail* lo comprueba y se puede ver en la cabecera SMTP solamente.
- *Yahoo!* no lo comprueba.

B) Si no tiene registro SPF se comprueban los valores MX del dominio del remitente. Esta comprobación no es realizada ni por Yahoo!, ni Hotmail ni por Gmail y dejan recaer el resto de alertas en filtros antispam.

a. Si la IP del servidor que ha entregado el mail es una de los intercambiadores de correo, entonces el correo se marca como Legítimo.

b. Si la IP no es una de los servidores MX entonces se marca como Dudoso.

Toda esta lógica de detección de correos legítimos o no legítimos ayuda a valorar mejor la autenticidad de los remitentes de correos electrónicos en aquellos entornos en los que no se utilizan firmas digitales. Hay que recordar que el uso de ***S/MIME*** o ***PGP*** es mucha mejor garantía para comprobar el remitente de un correo. Estos sistemas descritos en este artículo, basados en dirección IP de los servidores, no muestran ninguna diferencia cuando hay servidores vulnerados o mal configurados que pueden ser utilizados por atacantes externos o internos de la red para suplantar remitentes.

Por último, me gustaría recordar que, independientemente que uses o no este método, debes tomar como falsos todos los correos que se suponga que has enviado tú y no lo hayas hecho.

Banca, Phishing y SPF

Hace unos años abrí una carpeta en mi buzón de correo llamada "Estafas" donde voy situando todos los mails que me llegan de phishing, muleros, venta fraudulenta, etc... Esta carpeta se ha ido llenando al cabo de los años y hoy en día tiene más de 1.000 correos que utilizo para explicar cosas en las charlas.

Desde que migramos nuestro servidor a Exchange Server 2007 y se realizó un assesment de las opciones de Anti-Spam, la verdad es que me cuesta recibir algún correo que llevar a la boca de esa carpeta.

El otro día, repasando con Joshua Sáenz, MVP de Exchange Server y compañero de I64, las opciones y el funcionamiento de los filtros ante correos suplantados, comprobamos el funcionamiento del servidor ante diferentes tipos de spam. Al final, no sabía si besar a Joshua o al Exchange Server 2007 por lo bien que se portan ambos.

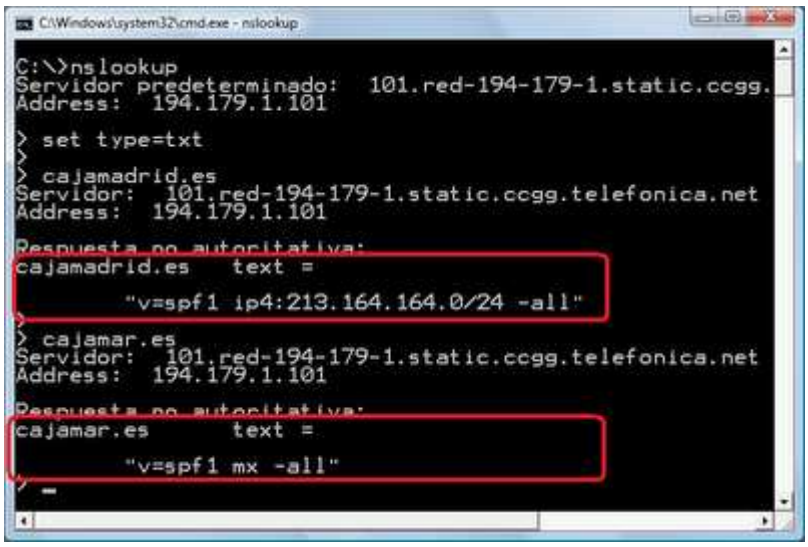
El servidor tiene configurados filtros con RBL, filtro de Reputación (basado en registro PTR, estadística de SCL de los correos recibidos de ese servidor y prueba de proxy abierto), filtro de contenido (basado en la tecnología del IMF), soporte para recepción de correos cifrados con canal TLS y filtro de Sender ID.

Esta configuración ha hecho que, por ejemplo, correos de phishing tradicional que suplantan a bancos, hayan dejado de entrar en mi buzón tiempo ha. Esos correos que dicen venir del equipo técnico de un banco para que cambies la contraseña o entres en tu cuenta pinchando en el siguiente link. Esto me sucedió mucho durante un periodo con Cajamadrid.es.

Sin embargo, esto ya no me sucede jamás, porque la gente de Cajamadrid.es ha hecho los deberes y ha configurado el registro SPF en el DNS dando información a los servidores de correo que implementan Sender Policy Framework o Sender ID de quiénes son los servidores autorizados.

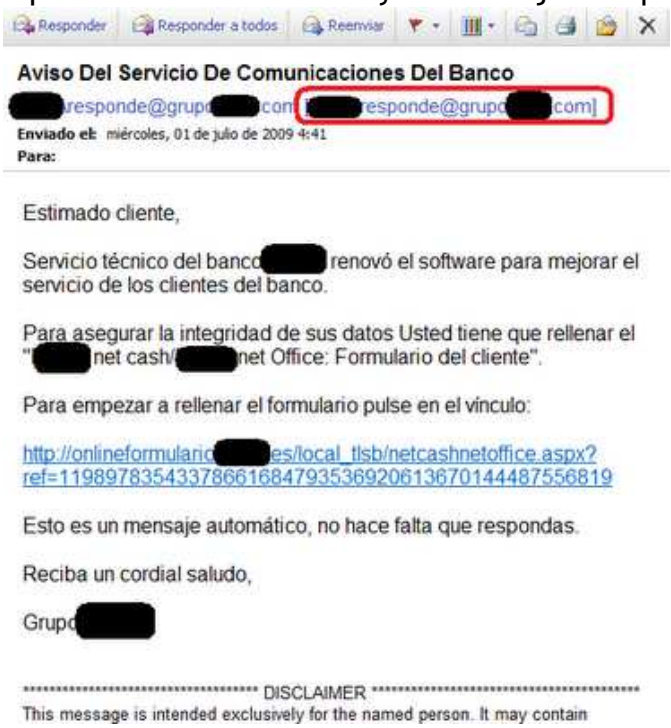
El uso del registro SPF ayuda especialmente a las entidades bancarias, víctimas tradicionales del envío de correos electrónicos falsos desde sus dominios, a evitar que llegen al usuario final. Es un sencillo gesto, configurar un registro TXT en el DNS y se consigue que un porcentaje mayor de correos falsos en su nombre no lleguen a las posibles víctimas. Y eso se transforma en dinero.

Así, he podido ver que algunos han hecho los deberes, como Cajamadrid o Cajamar, ambas con registro SPF con la opción -all para que todos los correos que vengan de una IP no dada de alta en él sean destruidos automáticamente.



Registro SPF de Cajamadrid.es y Cajamar.es

Sin embargo, hoy recibí un correo falso de un banco y....alto, esto no puede ser. Algo falla. Si los bancos han puesto el registro SPF y yo tengo el Sender ID configurado...¿cómo es posible que haya entrado este mail? La respuesta es bien fácil, una de las dos premisas no es cierta... y me ha dejado flipado.


Responder | Responder a todos | Reenviar

Aviso Del Servicio De Comunicaciones Del Banco

[redacted]responde@grupo[redacted]com [redacted]responde@grupo[redacted]com]

Enviado el: miércoles, 01 de julio de 2009 4:41

Para:

Estimado cliente,

Servicio técnico del banco[redacted] renovó el software para mejorar el servicio de los clientes del banco.

Para asegurar la integridad de sus datos Usted tiene que rellenar el "[redacted]net cash/[redacted]net Office: Formulario del cliente".

Para empezar a rellenar el formulario pulse en el vínculo:

http://onlineformulario[redacted]es/local_tlsb/netcashnetoffice.aspx?ref=11989783543378661684793536920613670144487556819

Esto es un mensaje automático, no hace falta que respondas.

Reciba un cordial saludo,

Grupo[redacted]

********** DISCLAIMER **********

This message is intended exclusively for the named person. It may contain

Correo falso de un supuesto Banco

Tras comprobar el registro SPF del DNS del banco del mail he podido constatar la no existencia del mismo. Esta acción la he repetido con muchos bancos y las respuestas han sido desalentadoras, casi nadie implementa ese registro. ¿Por qué?.

Lo cierto es que un banco que se gasta pasta en auditorías de seguridad y que se gasta pasta en la lucha contra el fraude debería tener implementada una de las medidas más baratas y que más información ofrece a los usuarios a la hora de detectar correos falsos. Pero no es así. ¿Alguien me lo explica?. Haz una prueba con el DNS de tu banco y dime que encuentras...

¿Por qué mis correos llegan como Spam?

Esta es una de las preguntas que más me hacen siempre que hablo de algo que tiene que ver con correo electrónico. Tiempo ha me hicieron escribir una lista de medidas para mejorar los resultados en los motores antispam de los correos electrónicos legítimos emitidos por una empresa. Aunque no son todas las medidas que se pueden aplicar, ésta es una buena lista de precauciones.

Muchas de las verificaciones que se realizan para validar o no un correo se realizan sobre la dirección IP del servidor utilizado para enviar el correo electrónico, para tener una IP cuidada es recomendable.

1. Marca las IP de los servidores autorizados para enviar correo en tu dominico con el registro SPF en el DNS. Esto hará que las comprobaciones del registro SPF de Sender Policy Framework y Sender ID sean positivas.
2. Comprueba que tus IPs no estén en listas RBL (Real-time Blackhole List). Si tu IP cae en una de estas listas muchos de los servidores no aceptarán tus correos. Ten siempre una IP de backup limpia e intenta, cuando caiga, sacarla de todas las listas. Muchas se alimentan las unas de las otras, así que revisa todas.
3. No compartas la IP con varios dominios si es posible y menos si no los controlas tú, ya que la IP pude caer en una RBL tanto por mal uso de tu dominio como por mal uso de cualquier otro.
4. Ten la IP a nombre de tu empresa e intenta controlar los registros PTR. Algunos filtros comprueban el valor del registro PTR en el DNS para autenticar el nivel.
5. Actualiza el software y configúralo de forma segura. Los filtros de reputación realizan comprobaciones reversas para ver si está mal configurado el servidor y puede ser víctima de los spammers. Si es así, no admiten correos de tu dominio.
6. Firma digitalmente tus correos con DKIM para que se puedan autenticar el dominio del emisor aquellos dominios que hagan uso de él.
7. Evita correos con múltiples destinatarios o contigo mismo en el destinatario, eso suele hacer subir el **SCL** (Spam Confidence Level) del correo.
8. Usa antivirus en el correo saliente. Si un usuario de tu red queda infectado puede intentar infectar a otros mediante el envío del malware por correo electrónico. Si un dominio detecta que le llega malware de tu dominio meterá tu IP en las RBLs.
9. Si tu correo sale por la misma IP que por la que sale, es decir, si el MX y el SPF son iguales, aunque es peor para la redundancia de seguridad, es mejor para aumentar el alcance de los correos, ya que alguno aún utiliza como comprobación el filtro de **Reverse MX Lookup**.
10. Y la más importante... no seas spammer y haz un uso correcto del correo electrónico.

El filtro antiphishing de GMail

Hace poco leía una noticia con el siguiente titular: "Gmail sigue mejorando: ahora es capaz de protegernos contra el phishing" y me dejaba sorprendido: *"¡Vaya!, ¿pero no habíamos quedado ya que Gmail era perfecto y que por eso había salido ya de beta?"*. La realidad tras el titular de la noticia es una cosa que me ha impactado por varios motivos que os paso a desgranar.

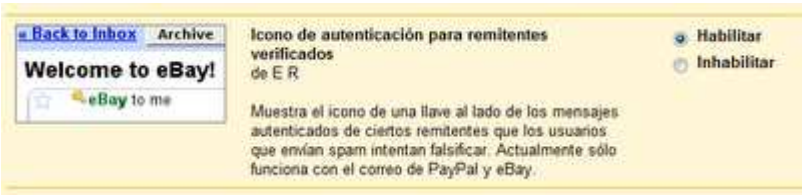
Eso sólo DKIM

Tan sólo y tan tanto. DKIM es una buena solución para garantizar la autenticidad del correo mediante una firma asociada a cada mensaje realizada por el servidor de correo saliente del dominio. El funcionamiento ya lo he explicado anteriormente. Cuando sale el correo por el servidor de correo saliente, este lo firma y añade una cabecera con el la firma y la clave que ha utilizado. El servidor que recibe el correo, en este caso Gmail, se va al DNS y busca la clave publica del servidor que firmo en el registro *nombredeclave._domainkey.remitentente.com*. Verifica que la firma está ok y listo.

Gmail ya hacía esto antes y mostraba un pequeño texto cuando se muestran los detalles que dice *"Firmado por"* si el mensaje viene por DKIM, pero no daba ninguna alerta visual al usuario fácil de ver. Sin embargo, se puede ver siempre la información en la cabecera SMTP.

Es sólo para Ebay y Paypal

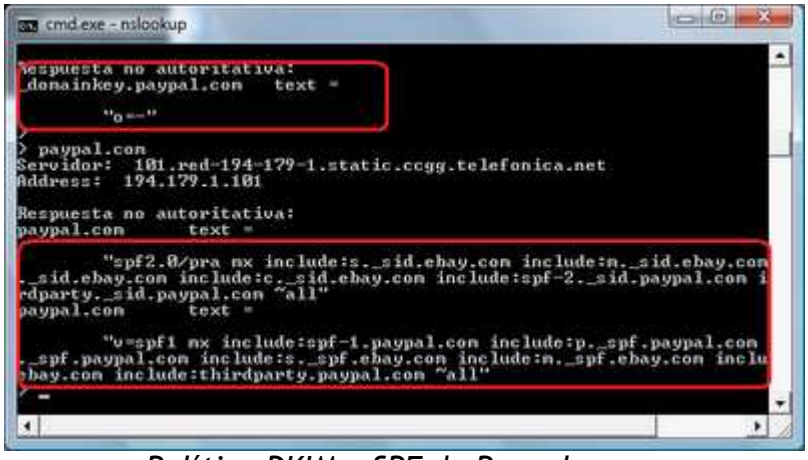
Según el anuncio es sólo para los mails que vienen de los dominios de Ebay y Paypal y cuando se activa esta protección en Configuración/Labs se especifica que la protección será sólo para ellos.



Configuración Antiphising

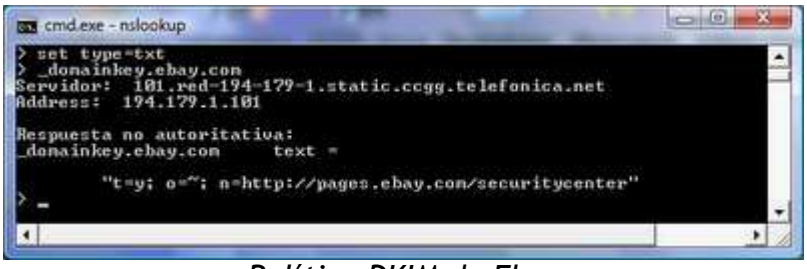
La gracia de DKIM está en que se debe comprobar la política en el DNS para saber que hay que hacer con los correos que no vienen firmados. En este caso concreto me llama más la atención porque:

- Paypal tiene política *Hardfail*, es decir, que todos los correos que vengan de un dominio paypal.com sin firmar con DKIM deben ser eliminados. Sin embargo, la política que tienen en el SPF es *Softfail*, lo que quiere decir es que no deben ser eliminados, y sólo se le debe advertir al usuario. Esto es totalmente incongruente.



Política DKIM y SPF de Paypal

- Ebay tiene política Softfail en DKIM y, además, está en modo test (t=y), con lo que los correos que no vengan firmados sólo deben ser marcados, pero deben entregarse al cliente.



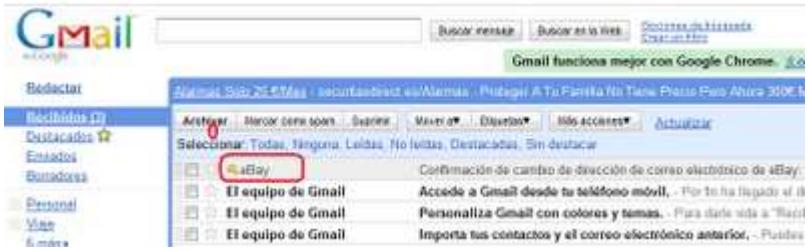
Política DKIM de Ebay

El icono

El resultado es "EL ICONO" que deberían llevar todos los correos firmados por DKIM no sólo los de Ebay y Paypal. Este icono es el mismo que pone Yahoo a todos los correos firmados (incluidos los de ebay y paypal) y que yo llevo pidiendo.

Icóno en correo firmado en Yahoo.com

El resultado es un iconito que de forma visual te advierte de que se ha comprobado la firma DKIM. La pregunta es ... ¿por qué sólo para Ebay y Paypal? Yahoo! es el creador de la idea y todos sus correos van firmados...¿por qué no avisar de la autenticidad de los correos que vienen firmados desde Yahoo! con un icono?

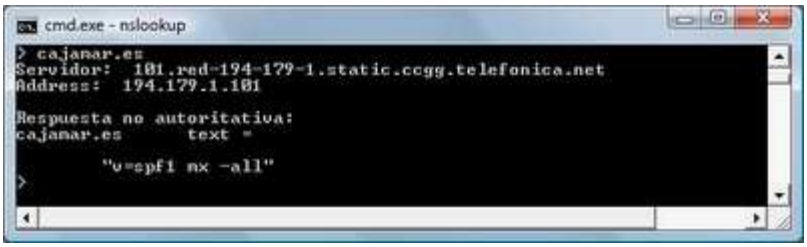


Correo firmado con dkim desde Ebay

¿Y el SPF?

¿Realmente se está tomando en serio Gmail la protección anti-phising? Yo creo que si lo está haciendo lo está haciendo mal. Cuando una organización utiliza el registro SPF para marcar los servidores autorizados para enviar correos Gmail debería hacer caso a la política.. y no lo hace.

Para esta prueba me he hecho un mail de phising suplantando al dominio Cajamar.es, que tiene creado un registro SPF con política Hardfail. Esto indica que si llega un correo que no venga de una de las IPs autorizadas, en este caso las de los registros MX, deberá ser eliminado.



Configuración SPF de cajamar.es

Sorprendentemete, a pesar de que se ve a la legua que es un correo de Phising (y con un poquito de Viagra) el mensaje llega a la Bandeja de Entrada sin ninguna alerta.

¿Es o no para bloquear este correo?

Conclusión

Mi conclusión es que Gmail debería seguir en beta unos añitos más...como el resto y que debería 1)Aplicar la polica SPF que marca el dominio del remitente 2) Mostrar el icono a todos los que vengan firmados y 3) Mostrar los iconos de alerta negativa y alerta positiva para los que cumplan y no cumplan las políticas SPF.