

Correo Electrónico no solicitado (Spam).

Identificación y procedimientos a seguir.

¿Quién no ha encontrado alguna vez en su buzón de correo electrónico mensajes publicitarios donde dicen regalar algo, o ganar mucho dinero; y peor aún ¿quién no ha recibido en su buzón este tipo de mensajes aparentemente procedentes de algún compañero de trabajo? o enviados desde una dirección desconocida.

El correo basura está continuamente creciendo, y disminuye la funcionalidad y credibilidad del correo electrónico como aplicación.

El correo basura o no solicitado (spam, uce ...) es uno de los múltiples resultados de la inseguridad y fragilidad del correo electrónico en Internet.

El correo electrónico clásico es un canal inseguro y fácilmente manipulable.

Los protocolos de correo electrónico utilizados por la mayor parte de los usuarios no pueden garantizar la autenticación del emisor ni la confidencialidad del contenido.

Pero esto no es obstáculo para considerar la manipulación y falsificación de mensajes como una acción ilegal y punible.

Es necesario perseguir este tipo de actividades y una de las tareas prioritarias por parte de las instituciones que ofrecen el servicio, es informar de ello a los usuarios.

Esta información deberá facilitarse a través de las Políticas de Uso propias de cada institución

Prácticamente todas las partes de un mensaje de correo (cabeceras y trazas) son falsificables pero siempre quedan rastros.

Antes de abordar el correo electrónico falsificado debemos hablar del correo electrónico válido que es aquel donde el remitente no intenta ocultar el origen del emisor del mensaje.

En primer lugar se verá la interpretación de la procedencia de un mensaje para descubrir posibles falsificaciones y a continuación veremos lo que se debe hacer con el correo electrónico no deseado.

La mejor forma de garantizar la procedencia e integridad de un mensaje es la utilización de PGP, actualmente integrado en casi todos los clientes de correo electrónico.

Interpretación de las cabeceras de los mensajes

La mayor parte de los usuarios sólo ven las clásicas cabeceras From: (Desde:), To:(Para:), Subject:(Asunto:) y Date:(Fecha:), casualmente las más fácilmente manipulables. Es recomendable echar un vistazo a esas otras cabeceras que no se suelen leer, sobre todo las que empiezan por "Received:".

Es importante descubrir quién originó el mensaje y la máquina que lo distribuyó para de esta forma identificar al emisor del mensaje.

El mecanismo del correo electrónico en Internet es sencillo, un mensaje de correo electrónico sale del programa del emisor, le encarga a un servidor de correo (servidor SMTP) -similar a un estafeta de correo postal- la distribución hacía el destino; el mensaje viaja por la red y llega al buzón del destinatario (login y palabra clave) el cual físicamente está en el servidor de co-

correo destino (servidor POP o IMAP). Durante el "viaje" desde el "Servidor SMTP" hasta el "Servidor de correo destino" puede haber servidores intermedios por donde circula el mensaje pero nunca menos de dos.

Cuando el mensaje pasa por un servidor de correo éste imprime una traza en la cabecera del mensaje (Received:) y queda archivada en un archivo de dicho servidor.

Es decir, los responsables del servicio de correo electrónico deben tener acceso a esta información y por lo tanto pueden facilitar mucho la labor de investigación. A un usuario le bastaría con interpretar la última traza impresa en la cabecera del mensaje cuando éste entra en su servidor.

Lo primero que debe hacerse para leer las cabeceras de un mensaje es habilitar la correspondiente opción en el programa de correo. Hay que fijarse exclusivamente en las líneas que empiezan por la palabra "Received:".

El orden de lectura va de abajo hacia arriba, es decir la primera cabecera "Received:" será la que ofrezca información del emisor y la última es la entrega en nuestro buzón.

Cada una de estas líneas ha sido impresa por el servidor de correo por donde ha pasado el mensaje.

Se verá un ejemplo, sin olvidar que el perfil de las cabeceras es similar, pero la información de las trazas "Received:" puede variar:

Ejemplo 1: Mensaje normal

From: "Fernando el Católico" f.catolico@upv.es
To: perico@rediris.es
Date: Tue, 11 Jan 2000 18:58:26 -0600 (Wed 01:58 MET)
Subject: Soy yo y no te engaño

Aparentemente viene de la dirección <f.catolico@upv.es> y es enviado a <perico@rediris.es>. Si desplegamos el resto de cabeceras veremos:

(2) Received: from vega.upv.es (vega.cc.upv.es [158.42.4.1]) by chico.rediris.es (8.9.3/8.9.3) with ESMTP id SAA05366 for <perico@rediris.es>; Tue, 11 Jan 2000 18:58:38 +0100 (MET)

(1) Received: from fons (enano.har.upv.es [158.42.108.72]) by vega.upv.es (8.8.4/8.8.5) with ESMTP id SAA12517; Tue, 11 Jan 2000 18:58:37 +0100 (MET)

La primera línea para interpretar es la (1) que indica que el mensaje ha sido emitido desde la máquina con dirección IP [158.42.108.72] que tiene asignado el nombre (resolución inversa en el DNS) "enano.har.upv.es", es decir es una máquina conectada a la red local del dominio upv.es.

El cliente de correo electrónico de este usuario utiliza la máquina "vega.upv.es" como servidor de correo saliente (servidor SMTP). Esta transacción se realizó el "11 Jan 2000 18:58:37 +0100 (MET)". Esta línea (1) ha sido añadida por el servidor de correo "vega.upv.es" por lo que podemos creer que sea correcta.

La cabecera (2) nos indica que el servidor "vega.upv.es" se ha conectado al servidor "chico.rediris.es" como paso final para depositarlo en el buzón <perico@rediris.es>. La transacción fue realizada el "11 Jan 2000 18:58:38 +0100 (MET)", es decir 1 segundo después.

Como conclusión podemos considerar que muy probablemente las cabeceras de este mensaje no hayan sido manipuladas y que el mensaje haya sido generado en el PC "enano.har.upv.es", pero no podemos garantizar que el mensaje sea de "Fernando el Católico" <f.catolico@upv.es>. Si las direcciones son de dominios de universidades españolas, como el del ejemplo UPV.ES, es muy probable que sean válidas.

Ejemplo 2: Mensaje falsificado

Este es un mensaje que se recibe en el buzón <perico@rediris.es> y las cabeceras clásicas son:

From: <perico@rediris.es>
To: "Fernando el Católico" <f.catolico@upv.es>
Date: Tue, 11 Jan 2000 18:58:26 -0600 (Wed 01:58 MET)
Subject: Soy yo y sí te engaño

Este mensaje se ha recibido en el buzón <perico@rediris.es> y aparentemente proviene de él mismo y va dirigido a: <f.catolico@upv.es>, todo un follón. Evidentemente nos hace sospechar y debemos investigar y desplegar las cabeceras y veremos algo así como:

(2) Received: from vega.upv.es (vega.cc.upv.es [158.42.4.1]) by chico.rediris.es (8.9.3/8.9.3) with ESMTP id SAA05366 for <perico@rediris.es>; Tue, 11 Jan 2000 18:58:38 +0100 (MET)

(1) Received: from fons (enano.har.upv.es [158.42.108.72]) by vega.upv.es (8.8.4/8.8.5) with ESMTP id SAA12517; Tue, 11 Jan 2000 18:58:37 +0100 (MET)

Vemos que la traza (2) dice "for <perico@rediris.es>" (no siempre existe) e indica que el mensaje iba encaminado a dicha dirección aunque el campo To: que solemos ver tenga el valor: [To:"Fernando el Católico" <f.catolico@upv.es>]. Unicamente podemos asegurar que dicho mensaje ha sido emitido desde el PC identificado con las siguientes coordenadas: enano.har.upv.es [158.42.108.72] y que es ahí donde se ha producido la falsificación.

Las cabeceras From: y To: que son las únicas que la gente suele visualizar, son falsificables aunque evidentemente hay que tener algunos conocimientos y motivo para hacerlo. No todo el mundo se dedica a hacer falsificaciones, pero sí hay que tener en cuenta que la posibilidad existe.

Estas falsificaciones son las que pudieran resultar más interesantes pero evidentemente hay muchas otras variaciones que requieren más habilidad en la falsificación. Se puede falsificar todo, desde las fechas de transmisión hasta la propia información de trazas "Received:" pero al final siempre queda una pista que nos permite identificar por lo menos el servidor de correo de donde salió el mensaje.

Todas las máquinas disponen de una dirección IP para transitar por Internet, y también deben de tener una entidad (empresa, organismo, etc.) que se responsabilice de las mismas.

El problema se produce cuando estas máquinas no tienen una dirección IP fija (accesos dial-up vía red telefónica básica) lo que imposibilita la labor de identificar al emisor, aún así siempre existe un responsable de direcciones IP (Proveedores de acceso a Internet).

Todas las máquinas deben tener un dueño y/o un responsable.

Este es un mensaje completo con las cabeceras desplegadas, lo que un programa de correo electrónico suele mostrar son los campos Date:, From:, To: y Subject:. Veamos quien envió el mensaje y a quien va dirigido.

Received: from hkbilib.hkbu.edu.hk (hkbilib.hkbu.edu.hk [158.182.30.1])
by chico.rediris.es (8.9.3/8.9.1) with ESMTP id JAA18473
for <heras@REDIRIS.ES>; Mon, 7 Feb 2000 09:50:31 +0100 (MET)
Received: by hkbilib.hkbu.edu.hk id QAA0000017827; Mon, 7 Feb 2000 16:50:41 +0800 (HKT)
Message-id: 200002070850.QAA0000017827@hkbilib.hkbu.edu.hk
Reply-to: srchzznngnz@mailexcite.com
Content-type: text

----[las cabeceras de abajo son las únicas que se suelen ver]----

From: srchzznngnz@mailexcite.com
Date: Mon, 7 Feb 2000 16:50:41 +0800 (HKT) (09:50 MET)
To: srchzznngnz@mailexcite.com
Subject: Submit Your Site or Home Page

Sería un mensaje dirigido a <heras@REDIRIS.ES> y enviado directamente desde la máquina (hkbilib.hkbu.edu.hk [158.182.30.1]). ¿Qué usuario lo envió? Eso sólo podrá conocerse consultando los ficheros donde se dejan las trazas de los correos y en teoría sólo están accesibles a los responsables de dicha máquina... ¡en Hong Kong!.

Otro ejemplo real un poco más complejo.

Received: from ainnet.ain.es ([193.146.125.2])
by chico.rediris.es (8.9.3/8.9.1) with SMTP id MAA18844
for <heras@rediris.es>; Wed, 9 Feb 2000 12:18:42 +0100 (MET)
Received: from xx (unverified [130.206.1.3]) by ainnet.ain.es (EMWAC SMTPRS 0.83) with SMTP id <B0000191785@ainnet.ain.es>; Wed, 09 Feb 2000 12:27:27 +0100
Received: from xxxxxx (xxxxxx [1.1.4.3])
by yyyyyyyyyy with ESMTP id JAA18473
Received: by xx.xx.xx id QAA0000017827; Mon, 7 Feb 2000 16:50:41 +0800 (HKT)
Message-id: <200002070850.QAA0000017827@xx.xx.xx>
Reply-to: srchzznngnz@mailexcite.com
Content-type: text

---[las cabeceras de abajo son las únicas que se suelen ver]---

From: xxxxx____@xxxxxx.com
To: xxxx____@xxxxxx.xx
Date: Mon, 25 Feb 1999 16:50:41

¿A quién va dirigido? ¿qué máquina es la emisora? ¿qué máquina distribuyó el mensaje? ¿en qué fecha fue emitido? ¿a quién deberías dirigirte para denunciar este mensaje? si respondes a este mensaje (Reply) ¿a qué dirección sería enviada?

Recomendaciones

La dirección de correo electrónico que nos ofrecen en nuestra institución (universidad, centro de investigación, etc.) debe ser utilizada con criterios y normas de uso perfectamente definidas para llevar a cabo nuestra labor profesional en dicha institución.

Ahora bien, podemos disponer de otra dirección privada para nuestras actividades personales (*@hotmail.com, *@yahoo.com etc.).

Lo más importante es que cada una de estas direcciones se utilicen usando unos parámetros (servidor SMTP, POP/IMAP, claves) diferentes ya que están implicados en ello una serie de recursos (máquinas, líneas de comunicación etc.) determinados. La dirección privada debe utilizarse con los servidores del correspondiente proveedor de Internet y la dirección institucional con los servidores apropiados. No se deben mezclar ambos entornos.

Pero además de realizar un correcto uso del correo electrónico y una vez que ya sabemos interpretar las cabeceras, se recomienda utilizar los servidores oficiales asociados a nuestra dirección de correo electrónico. Esta práctica aportará algo más de garantía a los receptores sobre la fiabilidad del emisor. Si bien hay que hacer hincapié de nuevo en que sólo el uso de técnicas de criptografía de clave pública/privada como es PGP garantizará al máximo la veracidad del emisor de un mensaje.

¿Qué hacer con los mensajes no deseados que recibimos?

Para enviar una queja acerca de un correo no deseado hay que saber a qué dirección enviarla, para ello basta con saber interpretar las cabeceras de los mensajes y disponer de alguna herramienta que nos ofrezca información de las direcciones de correo electrónico de los responsables.

La mayor parte de los usuarios al recibir estos mensajes no deseados los borran al ser esto lo más rápido, pero si se desea actuar de forma efectiva contra este tipo abusos, debemos hacer o evitar hacer lo siguiente:

No se debe:

- * Enviar ningún mensaje cuando se ofrezca la posibilidad de darse de baja de la "supuesta" lista o ponerse en contacto con el "supuesto" emisor. Pues aunque muchas de ellas son falsas, muchas otras son correctas y al responder lo único que generalmente se consigue es capturar la dirección de correo electrónico correcta para posteriores envíos de correo basura.
- * Enviar quejas a direcciones que no estemos seguros de que son las que realmente han distribuido el mensaje.
- * Tratar con violencia al spammer. Lo peor sería estereotipar a estas personas como terroristas pues les daría más fuerza.
- * Poner filtros en los programas de correo electrónico para borrar automáticamente el correo basura. Si no se sabe muy bien lo que se hace se pueden perder mensajes que no interesaba filtrar.
- * Distribuir el mensaje a otras personas o listas.

* Ignorarlos. Es necesario denunciarlo.

Sí se debe:

- * Investigar la dirección del emisor o del responsable de la máquina o del dominio que ha permitido la difusión de dicho mensaje.
- * Disponer de dos mensajes tipo en castellano y en inglés, que se utilicen como contenido de la denuncia o queja.
- * Si no se quiere hacer nada, mejor que borrarlo es enviárselo al responsable del servicio de correo electrónico de su organización para que sea él quien actúe. La dirección para enviar este tipo de incidentes dentro de tu institución (dominio) debe ser: `abuse@dominio.ar` y si no existe es necesario recordarle al `<postmaster@dominio.ar>` que lo cree.

Ahora bien ¿cómo localizar las direcciones a las que hay que enviar el mensaje de queja?. Lo más importante es identificar los dominios implicados en la distribución de este tipo de mensajes basura. La mayor parte del correo basura con contenido en castellano no suele utilizar técnicas de falsificación de trazas aunque sí de direcciones, lo que facilita mucho la labor.

Una vez localizados los dominios implicados en la distribución hay que localizar las direcciones de los responsables que por defecto suelen estar en:

- * `postmaster@dominio.xx`
- * `abuse@dominio.xx` donde xx es el top-domain correspondiente (.es, .com, etc.)

Existen varias herramientas (whois, iplookup, etc.) así como direcciones de páginas web que permiten localizar a los responsables de un dominio. En el caso de un dominio registrado bajo .es se puede consultar el siguiente URL: <http://www.nic.es/whois/>.

Pongamos un ejemplo:

```
Received: from m1smtpsp01.wanadoo.es (m1smtpisp01.wanadoo.es [62.36.220.21])
by chico.rediris.es (8.9.3/8.9.1) with ESMTP id HAA04592
for <perico@rediris.es>; Tue, 8 Feb 2000 07:20:11 +0100 (MET)
Received: from maria.ctv.es (maria.ctv.es [212.25.129.25])
by m1smtpsp01.wanadoo.es (8.9.3/8.9.3) with ESMTP id HAA00488;
Tue, 8 Feb 2000 07:19:01 +0100 (MET)
Received: from default (ctv21225132171.ctv.es [212.25.132.171])
by maria.ctv.es (8.9.3/8.9.1) with SMTP id HAA19285;
Tue, 8 Feb 2000 07:16:16 +0100 (MET)
Message-id: <200002080616.HAA19285@maria.ctv.es>
```

---[las cabeceras de abajo son las únicas que se suelen ver]---

```
Date: Tue, 8 Feb 2000 07:16:16 +0100 (MET)
From: jordi <tu@ctv.es>
To: Lista de destinatarios oculta <tu@ctv.es>
Subject:!!!!teletrabajo!!!!
```

Como se deduce de las cabeceras, este mensaje fue enviado al buzón `<perico@rediris.es>` que es la víctima, fue emitido desde una dirección del dominio "ctv.es" y por lo tanto utiliza el

servidor de ese dominio "maria.ctv.es" y para llegar al destinatario usa otro servidor de correo m1smtpisp01.wanadoo.es.

¿Cómo deberíamos actuar? En primer lugar no enviando nada a la dirección <tu@ctv.es> que se sospecha que está falsificada y a continuación buscando las direcciones de los responsables de los dominios ctv.es y wanadoo.es que serían: postmaster@ctv.es, abuse@ctv.es, abuse@wanadoo.es, postmaster@wanadoo.es además como son dominios ".es" las encontraremos en: <http://www.nic.es/whois> .

Hay diversos lugares en la red que facilitan mucho esta labor. Simplemente enviándoles el mensaje basura incluidas las trazas, localizan los dominios implicados y sus responsables y al final generan de forma automática el envío del mensaje con nuestra queja. Los hay accesibles por correo electrónico, como "abuse.net" o vía Web como "spamcop.net". De todas formas antes de usarlos, es importante saber lo que se hace para evitar enviar mensajes a personas que nada tienen que ver con nuestro problema.

Es aconsejable recordar: No usar el correo electrónico para las distribuciones masivas, independientemente del contenido, molesta a mucha gente y puede llegar a ser ilegal. No colocar en el campo "To:" de un mensaje decenas o cientos de direcciones para difundir algo que interesa, existen alternativas y los responsables del servicio de correo electrónico darán las mejores soluciones

ES COMÚN PREGUNTARSE ¿CÓMO HAN PODIDO CONOCER MI DIRECCIÓN DE CORREO ELECTRÓNICO? ¿EXISTE ALGÚN TIPO DE LEGISLACIÓN QUE NOS PROTEJA DEL CORREO NO DESEADO?, ¿QUÉ MÁS SE PUEDE HACER ADEMÁS DE ENVIAR NUESTRAS QUEJAS?.

Las empresas y gente que se dedica a hacer spam utiliza unas vías típicas para recolectar direcciones e-mail. Pueden hacerlo con diverso soft existente que se dedica a buscar en las news direcciones e-mail de los usuarios. Pueden hacerlo también buscando direcciones en páginas web.

También pueden comprar bases de datos de clientes a proveedores de internet, que normalmente se las venden (mucha gente que se ha dado de alta en un proveedor de internet y que nunca se ha conectado, ha observado como al usar el buzón al cabo de un mes o dos, ya tenía propaganda esperándole).

Una opción es escribir la dirección e-mail en alguna imagen gráfica de nuestra página web. Existen también algunos scripts Java que confunden a los robots de búsqueda,.

Si se tiene página web se está mas agobiado de propaganda que el resto de usuarios.

Es posible cambiar el típico por el siguiente Script de JAVA sustituyendo las palabras por los datos de e-mail:

```
<SCRIPT language="JavaScript">
<!--
var name = "minombre";
var domain = "midominio.com";
document.write('<a href=\'mailto:\' + name + \'@\' + domain + \'\'>');
document.write(name + \'@\' + domain + \'</a>');
// --></SCRIPT>
```

Por último, existen empresas especializadas que se dedican a "robar" datos privados de los usuarios por vías más sofisticadas. Estas son las más eficientes y peligrosas.

Utilizan sobre todo la navegación de los usuarios para robarles su dirección e-mail sin que lo sepan.

Cuando visitamos páginas web, en muchas estamos siendo redirigidos a diversas máquinas de esas empresas en donde nos es extraído el e-mail, la IP, nuestro nombre de usuario, etc...

Otras introducen cookies en nuestra PC, y al cabo del tiempo acaban dándoles un perfil de preferencias e intereses del usuario.

Ellas son la causa en definitiva de que a pesar de tomar las precauciones mencionadas anteriormente, sigamos recibiendo propaganda en nuestros buzones sin que le veamos explicación.

Esto sólo es evitable utilizando métodos de protección en la navegación, como software que evita estos redireccionamientos, la admisión de cookies, la programación JAVA, etc.

Si se prefiere usar programas para evitar el spam, es aconsejable utilizar aplicaciones como las siguientes:

E-Mail Remover 2.4 <http://home.pacific.net.sg/~thantom/eremove.htm>

Permite ver las cabeceras de los mensajes en el servidor antes de descargarlos, permitiendo su eliminación. Puede que no sea el mejor, pero tiene el aliciente de que es Freeware (gratuito).

SpamBuster 1.61 <http://www.contactplus.com/>

Se trata de una de los programas más conocidos de este género. Funciona con el tradicional sistema de filtros, bajando únicamente las cabeceras de los mensajes para evitar perder tiempo.

Sin embargo, como siempre, la mejor de las medidas es la prevención.

*Sólo hay que dar nuestra dirección E-mail a nuestros amigos y conocidos.

*No publicar nuestra dirección E-mail principal en las News o en páginas web.

*No rellenar formularios en los que se soliciten nuestros datos personales a menos que sea absolutamente necesario.