GUÍAS DE SEGURIDAD UJA

Seguridad en el correo electrónico

Servicio de Informática
Vicerrectorado de Universidad Digital
Universidad de Jaén

Edición: **diciembre 2020**

Contenidos

1. Introducción

Según recientes estadísticas, en el mundo existen más de 500 millones de usuarios de correo electrónico, lo que supone un enorme mercado para organizaciones y personas con fines maliciosos.

Todos hemos recibido alguna vez en la bandeja de entrada de nuestro cliente de correo electrónico mensajes cuyo contenido resulta sospechoso. En los peores casos, hemos aprendido a partir de la experiencia que abrir determinados mensajes de correo electrónico, abrir determinados ficheros adjuntos o hacer clic en enlaces incluidos en determinados mensajes pueden hacer que nuestro ordenador quede infectado por algún virus, gusano, troyano o cualquier otro tipo de malware, nuestras contraseñas pueden ser capturadas o podemos ser víctima de algún tipo de estafa en Internet, por citar tan solo algunas de las amenazas más habituales.

No se trata de ser alarmistas, pero la realidad es que en Internet existen todo tipo de trampas y artimañas diseñadas para obtener algún tipo de beneficio de los usuarios, y actualmente la mayor parte de esas amenazas llegan en forma de mensajes de correo electrónico.

En esta guía pretendemos identificar cuáles son esas amenazas y al mismo tiempo, ofrecer una completa lista de consejos y medidas a tener en cuenta para seguir haciendo uso de un sistema de comunicación tan habitual como es el correo electrónico, con las mayores garantías de seguridad.

2. Peligros más frecuentes asociados al correo electrónico

En la actualidad, las amenazas más habituales asociadas al uso del correo electrónico son las siguientes:

- **SPAM (correo basura)**: se calcula que más del 80 % de correos electrónicos enviados en todo el mundo actualmente son SPAM, y este porcentaje sigue creciendo.

- ***Phishing* (captura de credenciales)**: consiste en un método fraudulento de capturar información sensible, como nuestros números y claves de cuentas bancarias o de tarjetas de crédito. Se nos intenta engañar con mensajes que aparentan ser mensajes oficiales de entidades financieras o empresas de nuestra confianza.

- **Estafas de todo tipo**: donde se nos intenta vender productos falsos o inexistentes, se nos solicita dinero aludiendo a buenas causas, ofertas de trabajo inexistentes, y un largo etcétera.

- Correos con **ficheros adjuntos maliciosos (virus, gusanos, troyanos…)**. Actualmente es uno de los peligros más extendidos. Recibimos un mensaje (de un remitente no necesariamente desconocido ya que puede estar falsificado) con un fichero adjunto que nos invita a abrirlo. Dicho fichero contiene código malicioso que, si no disponemos de software antivirus o antimalware adecuado, infecta nuestro equipo, con consecuencias diversas. Muchos de estos ficheros

infectados a menudo utilizan la libreta de direcciones de nuestro cliente de correo para reenviarse a su vez a todos nuestros contactos.

- **Cadenas de mensajes falsos (hoaxes o bulos):** generalmente se trata de mensajes variados acerca de hechos o falsas alarmas de cualquier tipo, en los que se nos pide que reenviemos y difundamos el mensaje entre nuestros conocidos. El problema de las cadenas de mensajes falsos es el volumen de correos electrónicos que crea**.** Si una persona envía un mensaje a 10 personas y cada persona que le recibe envía el mensaje a otras 10, en poco tiempo se habrán enviado millones de mensajes de correo, con el coste asociado que esto tiene en cuando al tiempo de millones de personas leyendo el mensaje y el coste de los servidores de correo que tienen que recibir, guardar y enviar estos millones mensajes (y su posible caída de rendimiento y lentitud por la sobrecarga).

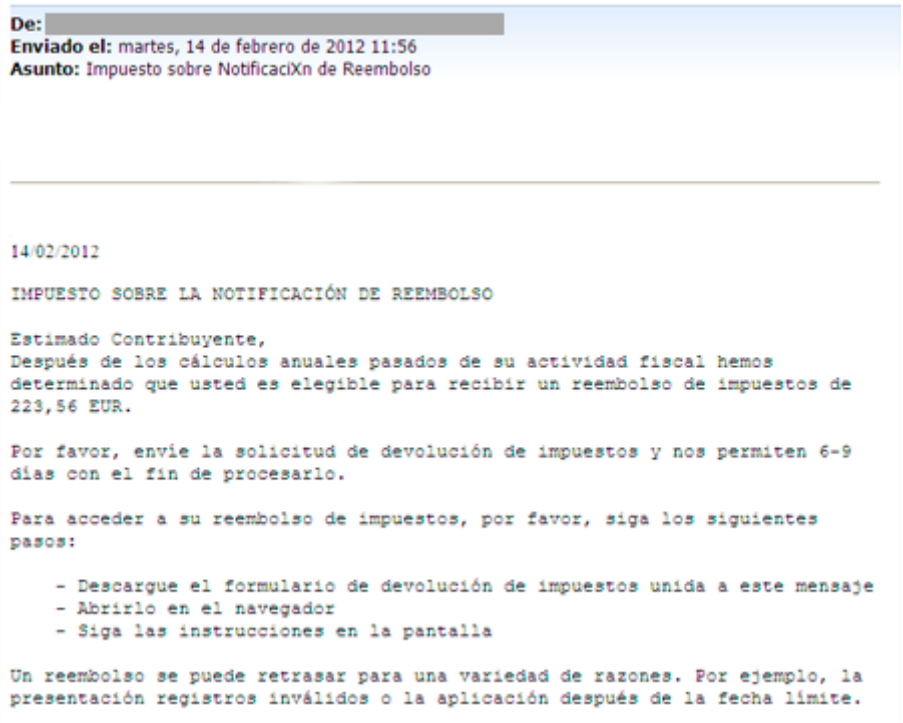
2.1. Email spoofing. Suplantación de identidad mediante correo electrónico

Dentro de los peligros citados anteriormente, uno de los más habituales en la actualidad es la suplantación de identidad mediante el correo electrónico (email spoofing), generalmente con la finalidad de captura de credenciales de usuario y/o infección mediante malware para permitir intrusiones en los sistemas informáticos de una organización.

A menudo nos llega un email de nuestro banco o de algún tipo de organismo (Correos, Agencia Tributaria, Seguridad Social, grandes cadenas de venta online…) pidiéndonos por favor que nos descarguemos un archivo o hagamos clic en un enlace. En todos estos casos tenemos motivos más que sobrados para sospechar, pues lo más probable es que se trate de un tipo de ataque de ingeniería social de tipo *phishing*, citado anteriormente.

Cada día se envían millones de correos fraudulentos por correo electrónico, y aunque la mayoría son detenidos por los filtros antispam, muchos terminan llegando a las bandejas de entrada de los usuarios. Existen varios elementos en los que podemos fijarnos para identificar este tipo de ataques. Uno de los más recomendables es **comprobar el remitente del correo**. Sin embargo, este no es un factor definitivo, ya que cada vez **hay más ataques de *phishing*, en los que el correo ha sido suplantado usando técnicas de email *spoofing*.**

El término *spoofing*, que en inglés significa falsificar o engañar, es una técnica de suplantación de identidad muy común, especialmente a través del correo electrónico, aunque existen otras modalidades.



De: [redacted]
Enviado el: martes, 14 de febrero de 2012 11:56
Asunto: Impuesto sobre NotificaciXn de Reembolso

14/02/2012

IMPUESTO SOBRE LA NOTIFICACIÓN DE REEMBOLSO

Estimado Contribuyente,
Después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 EUR.

Por favor, envíe la solicitud de devolución de impuestos y nos permiten 6-9 días con el fin de procesarlo.

Para acceder a su reembolso de impuestos, por favor, siga los siguientes pasos:

- Descargue el formulario de devolución de impuestos unida a este mensaje
- Abrirlo en el navegador
- Siga las instrucciones en la pantalla

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación registros inválidos o la aplicación después de la fecha límite.

El email *spoofing* se lleva a cabo mediante un correo electrónico fraudulento en el que **el atacante ha cambiado la dirección del remitente y el asunto para conseguir que parezca un mensaje legítimo**. Habitualmente, los ciberdelincuentes la llevan a cabo para realizar estafas y engañar a sus víctimas, con el objetivo de conseguir datos personales de los usuarios (contraseñas, números de tarjeta de crédito, cuentas bancarias, DNI, correos y otros datos personales) y obtener un beneficio económico.

También debemos tener en cuenta que existen dos perfiles a la hora de convertirnos en víctima de este ciberataque:

- **Víctima directa**: podemos estar recibiendo correos fraudulentos de una entidad o servicio al que han suplantado la identidad.
- **Víctima indirecta**: nosotros mismos podemos haber sido suplantados y un ciberdelincuente puede estar utilizando nuestro correo electrónico para engañar a nuestros contactos u otros usuarios. Además, es posible que ni sepamos que nos están suplantando, ya que no somos nosotros quienes recibimos el correo.

¿Cómo podemos identificarlo?

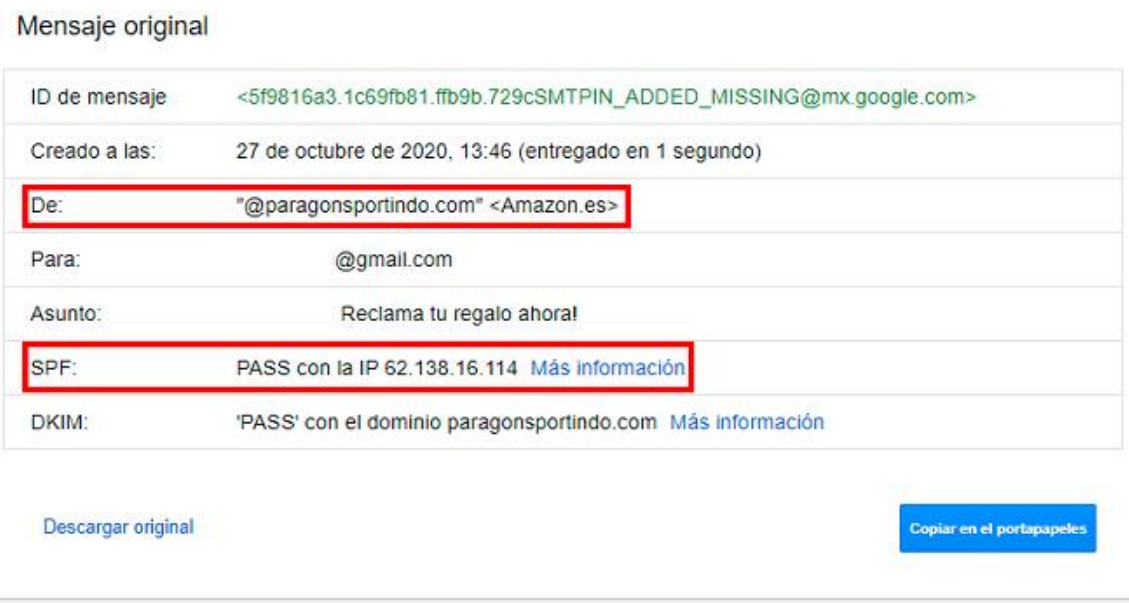
Existen diferentes pautas y elementos clave a la hora de saber si estamos siendo víctimas de un *email spoofing*. Lo más importante cuando tratamos de **identificar este tipo de correos fraudulentos** es ser pacientes y detenernos unos minutos, especialmente cuando nos enfrentamos a cientos de mensajes en nuestro día a día. Interpretando las cabeceras de los correos, podremos detectar información muy valiosa:

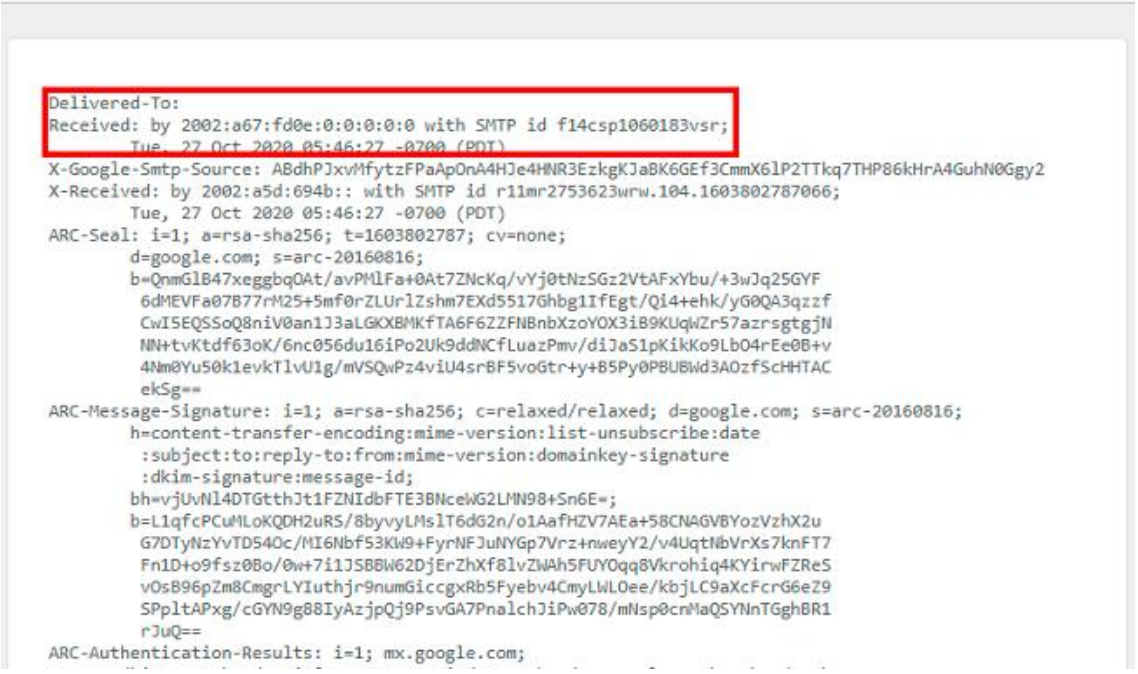
- Datos relativos al emisor y al receptor.
- Los servidores de correo intermedios por los que el mensaje ha pasado desde que se envió.
- El cliente del correo utilizado para enviar el email.

- Las fechas de envío y recepción.

Aunque esta información pueda permanecer oculta a simple vista, es posible visualizarla desde nuestro gestor de correos fácilmente. En el caso de GMail

1. Abriremos el correo a analizar.
2. Luego, haremos clic en el icono de los tres puntos y seleccionaremos **Ver origen del mensaje**:





```
Delivered-To:
Received: by 2002:a67:fd0e:0:0:0:0:0 with SMTP id f14csp1060183vsr;
        Tue, 27 Oct 2020 05:46:27 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJxvMfytzFPaApOnA4HJe4HNR3EzkgKJaBK6GEf3CmmX6lP2TTkq7THP86kHrA4GuhN0Ggy2
X-Received: by 2002:a5d:694b:: with SMTP id r11mr2753623wrw.104.1603802787066;
        Tue, 27 Oct 2020 05:46:27 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1603802787; cv=none;
        d=google.com; s=arc-20160816;
        b=QnmGlB47xeggbqOAt/avPMlFa+0At7ZNcKq/vYj0tNzSGz2VtAFxYbu/+3wJq25GYF
         6dMEVFa07B77rM25+5mf0rZLUrlZshm7EXd5517Ghbg1IfEgt/Qi4+ehk/yG0QA3qzzf
         CwI5EQSSoQ8niV0an1J3aLGKXBMKfTA6F6ZZFNBnbXzoYOX3iB9KUqWZr57azrsgtgjN
         NN+tvKtdf63oK/6nc056du16iPo2Uk9ddNCfLuazPmv/diJaS1pKikKo9LbO4rEe0B+v
         4Nm0Yu50k1evkTlvU1g/mVSQwPz4viU4srBF5voGtr+y+B5Py0PBUBWd3AOzfScHHTAC
         ekSg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-transfer-encoding:mime-version:list-unsubscribe:date
         :subject:to:reply-to:from:mime-version:domainkey-signature
         :dkim-signature:message-id;
        bh=vjUvNl4DTGtthJt1FZNIdbFTE3BNceWG2LMN98+Sn6E=;
        b=L1qfcPCuMLoKQDH2uRS/8byvyLMslT6dG2n/o1AafHZV7AEa+58CNAGVBYozVzhX2u
         G7DTyNzYvTD54Oc/MI6Nbf53KW9+FyrNFJuNYGp7Vrz+nweyY2/v4UqtNbVrXs7knFT7
         Fn1D+o9fsz0Bo/0w+7i1JSBBW62DjErZhXf8lvZWAh5FUYOqq8Vkrohiq4KYirwFZReS
         vOsB96pZm8CmgrLYIuthjr9numGiccgxRb5Fyebv4CmyLWLOee/kbjLC9aXcFcrG6eZ9
         SPpltAPxg/cGYN9g88IyAzjpQj9PsvGA7PnalchJiPw078/mNsp0cnMaQSYNnTGghBR1
         rJuQ==
ARC-Authentication-Results: i=1; mx.google.com;
```

3. Consejos para un uso seguro del correo electrónico

Existen numerosos consejos a seguir para usar el correo electrónico de forma segura, muchos de ellos de sentido común:

3.1. Consejos de carácter general

- **Usar diferentes cuentas de correo electrónico:** Un buen consejo práctico es mantener varias cuentas de correo electrónico para diferentes usos. Se recomienda usar dos o tres cuentas diferentes: una para el trabajo, otra para uso personal y una tercera para suscripciones y recepción de información. La cuenta de trabajo debe ser usada exclusivamente para temas relacionados con el trabajo. La segunda cuenta de correo electrónico debe ser usada para conversaciones con nuestros contactos personales, y la tercera cuenta de correo electrónico debe ser usada para ser expuesta en Internet, usándola para suscripciones a boletines de noticias y demás fuentes de información, sin problema de que nos la puedan capturar. Igualmente, si tenemos que proporcionar nuestra cuenta de correo electrónico en algún sitio de Internet, debemos usar esta tercera cuenta de correo electrónico. Probablemente, será en esta tercera cuenta donde recibiremos la mayor parte del SPAM o correo sospechoso, pero las demás las tendremos más protegidas.

- Si necesitas enviar datos importantes o sensibles a través de correo electrónico, en primer lugar, asegúrate de que los protocolos de envío (SMTP) y recepción (POP3/IMAP) de correo configurados en el cliente son seguros**. En el caso de las cuentas de correo de la UJA, se recomienda la configuración de estos protocolos seguros (cifrados) de correo: SMTPS (puerto 25 con TLS), POP3S (puerto 995 con SSL) e IMAPS (puerto 993 con SSL).** Puedes consultar las guías de configuración segura de correo en la siguiente dirección:

  https://www.ujaen.es/servicios/sinformatica/guias-practicas/correo-electronico

- **Usar la opción de copia oculta (BCC):** Cuando incluimos las direcciones de correo electrónico de una persona en el campo "BCC" ninguno de los receptores puede ver las direcciones de los otros receptores de correo electrónico, mientras que, si utilizamos "CC", si se verán los destinatarios.

  Cuando enviamos correo a un grupo diverso de personas sin usar el "BCC" ponemos en peligro la privacidad y la seguridad. Basta con que un *spammer* consiga todos los correos electrónicos e inmediatamente todos los destinatarios de nuestra lista serán bombardeados con SPAM o *phishing*. Además, muchos programas de correo electrónico están configurados por defecto para agregar de forma automática las nuevas direcciones de correo electrónico entrantes a la agenda. Esto significa que las personas del grupo receptor del mensaje habrán añadido inadvertidamente la lista entera a su libreta de direcciones, y como consecuencia, si el ordenador de alguno de esos usuarios está infectado con malware podrá estar enviando SPAM de forma silenciosa sin que éste lo sepa.

- **Ser prudente a la hora de contestar.** Aunque los clientes de correo suelen tener por defecto la opción de contestar sólo al remitente, a veces por error podemos seleccionar la opción de "Contestar a todos" e incluir a todos los que estaban en el correo electrónico original en la respuesta, con las consecuencias que ello

pueda tener.

- En muchos casos, el SPAM proviene del **reenvío de correo electrónico**. El reenviar correos puede ser una excelente vía para comunicarse con alguien sin tener que escribir algo muy extenso. Pero cuando un correo electrónico se reenvía, los receptores del correo son añadidos de forma automática al listado en el cuerpo del mensaje. Como la cadena permanece continuamente en movimiento, cada vez se añaden más y más receptores a la lista. Si ese correo finalmente llega a un *spammer* puede hacerse con una gran cantidad de direcciones de forma inmediata. Sólo se necesitan unos pocos segundos para borrar todas las direcciones de mail recibidas antes de reenviar una parte o la totalidad del correo, y ello puede evitar que, por nuestra culpa, nuestros contactos sean víctimas de SPAM o *phishing*.

3.2. Para evitar el correo electrónico fraudulento

- **Aprende a reconocer los fraudes por correo electrónico.** Los correos electrónicos no deseados usan una gran variedad de títulos atractivos para conseguir que el destinatario los abra. Muchos usuarios a menudo cometen el error de abrir estos correos electrónicos, abrir o ejecutar un adjunto malicioso o hacer clic en un link incluido en el propio mensaje. Ten especial cuidado en no abrirlos y elimine directamente aquellos correos en los que:

  - Nos informen de que hemos ganado en cualquier tipo de lotería o sorteo o que vamos a recibir cualquier tipo de premio.
  - Correos en los que nos informan de reyes o príncipes de Nigeria tratando de enviarnos una enorme cantidad de dinero.
  - Los detalles de ninguna cuenta bancaria en ningún caso necesitan ser reconfirmados inmediatamente.
  - Si nos informan de algún tipo de herencia sin reclamar.
  - Si nos indican que hemos ganado cualquier tipo de dispositivo electrónico o nos informan de alguna oferta sospechosa.
  - Cualquier otro tipo de correo que nos resulte altamente sospechoso y que provenga de remitentes que no conocemos.

- **Aprende a reconocer los ataques de *phishing* en los mensajes de correo electrónico.** Aunque seamos el usuario de correo electrónico más experimentado del mundo, antes o después acabaremos abriendo algún correo electrónico de *phishing*. En este punto, la clave para limitar el daño está en reconocer este tipo de mensajes.

  El *phishing* es un tipo de fraude en línea donde el remitente del correo electrónico Intenta engañarnos y nos solicita contraseñas personales o información relacionada con cuentas bancarias, por poner algunos ejemplos. El remitente generalmente roba el logo de un banco o empresa muy conocida y trata de diseñar un mensaje de correo electrónico para parecerse al que vendría del banco. Normalmente el correo electrónico de *phishing* nos invita a hacer clic en un enlace a fin de confirmar nuestra información o contraseña, pero también puede invitarnos a contestar al correo electrónico con nuestra información personal. Si proporcionamos información personal, el estafador usará la información para tratar de robar nuestra identidad y nuestro dinero.

  Las pistas que nos pueden hacer sospechar de un *phishing* incluyen:

- Un logotipo que parece distorsionado o de mala calidad.
- Mensajes que se refieran a nosotros como "estimado", "estimado cliente" o "estimado usuario" en lugar de incluir nuestro nombre real.
- Mensajes que nos adviertan que una cuenta nuestra se cerrará a menos que confirmemos nuestra información inmediatamente.
- Mensajes que vengan de una cuenta de correo similar, pero diferente a una que la compañía real que nos envía el correo usa normalmente.
- Mensajes que informan de "amenazas a la seguridad" y requieren que actuemos inmediatamente.

Si sospechamos que un correo electrónico es un intento de *phishing*, la mejor prevención es no abrir nunca dicho mensaje. Y en caso de abrirlo, nunca debemos contestar ni hacer clic en ningún enlace incluido en el mensaje. Además, **es muy conveniente márcalo como fraudulento** en nuestro cliente de correo o sistema de webmail, para que este aprenda y lo clasifique automáticamente en el futuro.

- Nunca envíes información sensible por correo electrónico y nunca proporciones información sensible a través de ningún enlace ni formulario que aparezca en el correo electrónico que has recibido. **Accede siempre directamente a la web que se indica, tecleando tu dirección en el navegador, así evitamos entrar en una dirección maliciosa a través de un enlace falsificado.**

- **Nunca proporciones tus contraseñas a nadie. ¡Son totalmente personales! Si se las proporcionas a terceros, las acciones que realicen las harán en tu propio nombre, suplantándote.**

3.3. Para evitar el malware a través de correo electrónico:

- **Nunca abras ningún mensaje ni fichero adjunto de un remitente que desconozcas o que te resulte sospechoso.** Elimina directamente este tipo de mensajes. Una buena práctica si no estamos seguros es contactar con la persona que lo envía, para ver si realmente lo ha enviado. Si al abrir un mensaje automáticamente nos aparece alguna ventana o se nos redirige a una página web donde se nos pide que instalemos algo, cierra la ventana automáticamente y elimina el mensaje de correo electrónico.

- Es importante mantener actualizado el **software antivirus/antimalware** y tenerlo configurado para que analice todos los correos electrónicos entrantes.

- Habilitar en el cliente de correo los **filtros de correo electrónico no deseado**. Estos filtros inicialmente necesitan algo de entrenamiento para diferenciar el SPAM del correo real y los usuarios deben tomarse el tiempo de marcar los mensajes que no han sido clasificados por el filtro de correo no deseado. No obstante, es algo totalmente recomendable, y en poco tiempo, la efectividad del filtro será cada vez mayor y veremos los resultados.

3.4. Otros consejos

- **No compartas la información de tu cuenta de correo con otros.** Todos lo hemos hecho: necesitamos una comprobación del correo urgente, llamamos a nuestra pareja o amigo y le pedimos verificar nuestro correo electrónico. Por supuesto, confiamos en estas personas, pero una vez la contraseña es conocida por alguien aparte de nosotros, nuestra cuenta no es tan segura como debería serlo. El problema real es que quizás nuestro amigo no use las mismas medidas de seguridad que nosotros. Él podría estar accediendo a tu correo electrónico mediante una conexión inalámbrica sin garantías de seguridad, quizás no tenga su antivirus actualizado, o podrías haber sido infectado con un *keylogger* (capturador de pulsaciones de teclado), que robe de forma automática su contraseña una vez que la escribe.

- **No uses contraseñas simples y fáciles de adivinar.**

- Las contraseñas que consisten de una palabra sencilla, un nombre, o una fecha son fácilmente adivinadas por los intrusos. Por lo tanto, cuando crea una contraseña que use números poco comunes y combinaciones de letras que no formen una palabra que se puedan encontrar en un diccionario. Una contraseña segura debe tener un mínimo de ocho caracteres, usando mayúsculas y minúsculas, números y caracteres especiales (%, &, $...).

- Como consejo adicional, es muy recomendable cambiar nuestras contraseñas (incluidas las del correo electrónico) de forma periódica, al menos una vez al año.

- **Cifra tus correos electrónicos importantes.** No importa cuántas precauciones tomes para minimizar las posibilidades de que tu correo sea controlado por intrusos, siempre debes asumir que alguna otra persona está mirando cualquier cosa que entre y salga de tu ordenador. Dada esta suposición, es importante que cifres tus correos para asegurarte de que, si alguien está controlando tu cuenta, al menos no pueden acceder lo que estás enviando. Consulta en la ayuda de tu cliente de correo electrónico la forma de cifrar el correo. Para ello, debes disponer de un certificado digital.

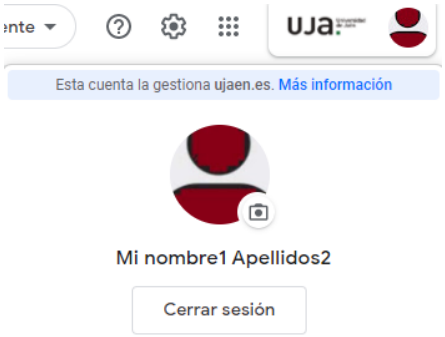
4. Consejos de seguridad en el uso del correo web (GMail)

A menudo, consultamos nuestro correo directamente en nuestro navegador, usando algún sistema de correo mediante web (webmail). En el caso de la UJA, el sistema de webmail está asociado a Google mediante su servicio Gmail, accesible desde la siguiente dirección:

https://mail.google.com/a/ujaen.es

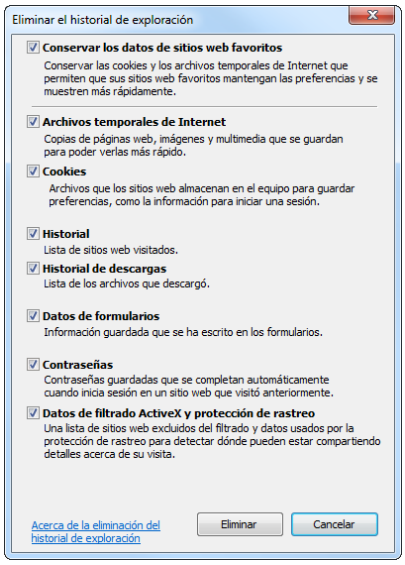
Estos son unos consejos de seguridad a tener en cuenta si usamos este sistema:

1. **Cierra siempre la sesión de Gmail, antes de cerrar la ventana del navegador.** Esto es una buena costumbre, y algo especialmente necesario cuando estás consultando tu correo electrónico en un sitio público, como una biblioteca o cibercafé. Para cerrar sesión en GMail, basta con pulsar el botón superior derecho y hacer clic en el enlace **Cerrar sesión**:

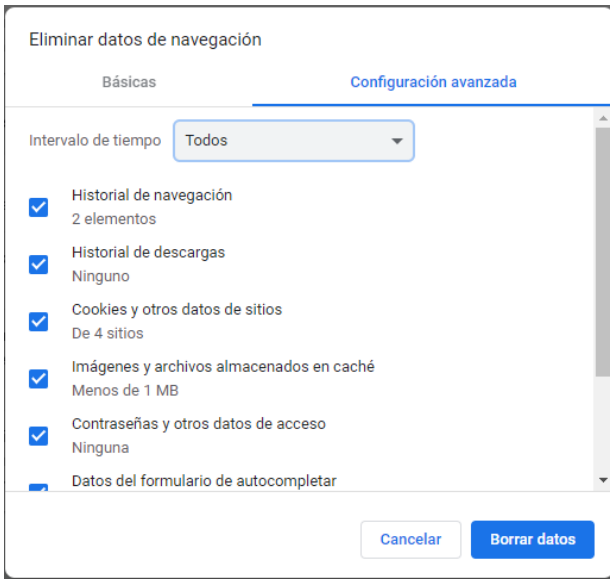


2. Cuando se consulta el correo de GMail en lugares públicos, es recomendable **utilizar la ventana de incógnito**. Si no lo has hecho, asegúrate de **borrar la caché del navegador, el historial y las contraseñas**. La mayor parte de los navegadores "recuerdan" de forma automática todas las páginas web que hemos visitado (historial), así como cualquier contraseña e información personal que hayamos tecleado con el objeto de ayudar a completar formularios similares en el futuro. Si esta información cae en malas manos, puede llevar a robos de identidad, robo bancario y robo de información usando nuestra cuenta de correo electrónico.

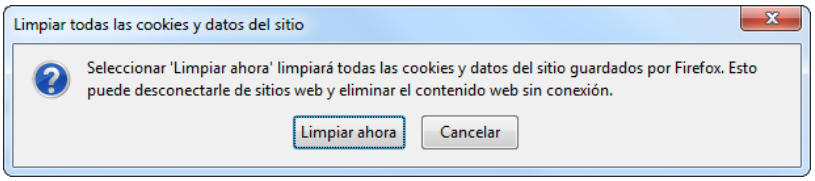
   En **Internet Explorer** esto se hace desde el menú **Herramientas > Opciones de Internet**, haciendo clic sobre **Eliminar**. Marcamos los elementos a eliminar, y pulsamos de nuevo el botón **Eliminar**:



En el caso de **Google Chrome**, es necesario entrar desde el menú principal a **Configuración > Privacidad y seguridad > Eliminar datos de navegación**. En la pestaña **Configuración Avanzada**, dentro de **Intervalo de tiempo** tenemos que seleccionar **Todos**, y asegurarnos que estén marcadas las casillas: **Cookies y otros datos de sitios, Contraseñas y otros datos de sitios**. Para mayor seguridad se recomienda marcar todas las casillas y hacer limpieza completa:



En el caso de **Mozilla Firefox,** desde el menú principal, hay que entrar en **Opciones > privacidad y seguridad**. Dentro del apartado Datos del sitio, pulsamos en "**Limpiar todos los datos**". Pulsando **Limpiar ahora** en la siguiente ventana se realizará la limpieza.



5. Seguridad en el correo electrónico de la UJA

5.1. Sistema anti-SPAM centralizado

La Universidad de Jaén dispone de un sistema anti-SPAM para atenuar el aumento de las amenazas a la seguridad contenidas en el correo, tales como SPAM, *phishing*, virus, etc... Este sistema incorpora una serie de filtros centralizados que se aplican en el siguiente orden:

- **Filtro de reputación**: rechaza la conexión de mensajes entrantes cuando la reputación de los servidores de correo de origen no sea buena. Esta reputación se monitoriza diariamente por miles de sensores repartidos por todo el mundo.
- **Filtro antivirus**: elimina o pone en cuarentena todos los mensajes que contienen virus.
- **Filtro de contenidos**: analiza el contenido del mensaje, tratando de detectar cualquier tipo de SPAM. Si se considera que un mensaje es un correo basura se marca, añadiendo en el asunto el texto: [POSIBLESPAM]. El usuario seguirá recibiendo todos los mensajes, pero con este sistema podrá definir filtros en su lector de correo para moverlos a una carpeta y, posteriormente, revisarlos o borrarlos, si lo cree conveniente. Esto permite controlar la bandeja de entrada (Inbox), impidiendo que el correo basura se mezcle con el resto de mensajes.

5.2. Filtros de correo no deseado en GMail

Gmail incluye filtros de correo no deseado que ayudan a proteger nuestra cuenta de las amenazas más habituales (SPAM, *phishing*…). Podemos ir alimentando y entrenando estos filtros a partir de los correos que recibimos en nuestra bandeja de entrada de Gmail.

Cuantos más mensajes marquemos como spam, más eficaz será la clasificación automática de spam de Gmail. Para ello, simplemente tenemos que seleccionar uno o varios mensajes y hacer clic en **Marcar como spam** .

Si en algún momento marcamos un correo incorrectamente, podemos quitarle la etiqueta de spam. Para ello, dentro de Gmail en el lateral izquierdo, haremos clic en **Más** y en la carpeta **Spam**. Abrimos el correo marcado incorrectamente y en la parte superior, haremos clic en **No es spam**.

Para impedir que un tipo de mensajes se coloque en Spam en el futuro, una de las formas de evitarlo es añadir el remitente a nuestros contactos.

6. Referencias en Internet

- Universidad de Jaén: Guías prácticas relacionadas con el correo electrónico
  https://www.ujaen.es/servicios/sinformatica/guias-practicas/correo-electronico
- Medidas de seguridad en el correo de Google
  http://support.google.com/accounts/bin/answer.py?hl=es&answer=46526
- Decálogo de seguridad para el correo electrónico
  http://www.baquia.com/blogs/seguridad/posts/2012-10-09-decalogo-de-seguridad-para-el-correo-electronico
- Instituto Nacional de Ciberseguridad (INCIBE)
  https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-correo-electronico.pdf
- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/
- CCN-CERT
  https://www.ccn-cert.cni.es/
- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica
  https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html