Guía de recomendaciones para una navegación segura en Internet

SEGURIDAD DE LA INFORMACIÓN

División de Transformación Digital

Abril 2020

Introducción.

La navegación en Internet se ha vuelto una actividad cotidiana; acceder a la cuenta bancaria, enviar documentación utilizando el "webmail"[1], o comprar todo tipo de productos en tiendas online son acciones que realizamos de forma habitual. Sin embargo, esta actividad ofrece muchas "oportunidades" a los ciberdelincuentes, quienes han puesto internet en su "punto de mira".

Para estar protegidos es necesario que conozcamos los peligros más importantes a los que estamos expuestos al navegar por internet, así como las medidas que podemos adoptar para reducir estos riesgos.

Esta guía pretende, por un lado, orientar y concienciar al usuario sobre las técnicas más utilizadas por los cibercriminales y, por otro, divulgar y ofrecer un conjunto de pautas básicas para hacer que nuestra navegación por Internet sea más segura.

EMASESA está firmemente comprometida con la creación de una sociedad digital más segura. Con esta finalidad, el presente documento se ha adaptado a partir de la correspondiente guía interna con objeto de que pueda ser utilizado pública y libremente por cualquier persona u organización interesada.

[1] Correo electrónico online

Principales peligros cuando navegamos por internet.

Entre las diferentes amenazas a los que nos podemos ver expuestos cuando navegamos por Internet, se encuentran las siguientes:

Instalación de software malicioso sin nuestro conocimiento; puede ser de muy diverso tipo, como por ejemplo:

- **Ransomware;** cifra la información que tenemos almacenada en el ordenador y reclama un pago económico a cambio de su restablecimiento[2].
- **Adware y/o spyware;** abre constantemente ventanas emergentes de publicidad no deseada y, en muchos casos, realiza un seguimiento de nuestros hábitos de navegación.
- **Secuestradores del navegador** (browser hijackers); permiten al ciberdelincuente tomar el control remoto de nuestro navegador y utilizarlo con fines maliciosos. Suele agregar varios "favoritos" a la lista de marcadores del navegador y cambiar la página de inicio e incluso algunas claves del registro.
- **Capturadores de pulsaciones** (keyloggers); registra todo lo que tecleamos y lo envían a los ciberdelincuentes (por ejemplo, las contraseñas de sitios sensibles como el banco o el correo electrónico).
- **Barras de utilidades** (toolbars); son barras de botones y complementos que se añaden a nuestro navegador, generalmente durante la instalación de otro software gratuito, y que en muchos casos esconden malware.
- **Troyanos, gusanos, etc.;** otros tipos de malware, en general.

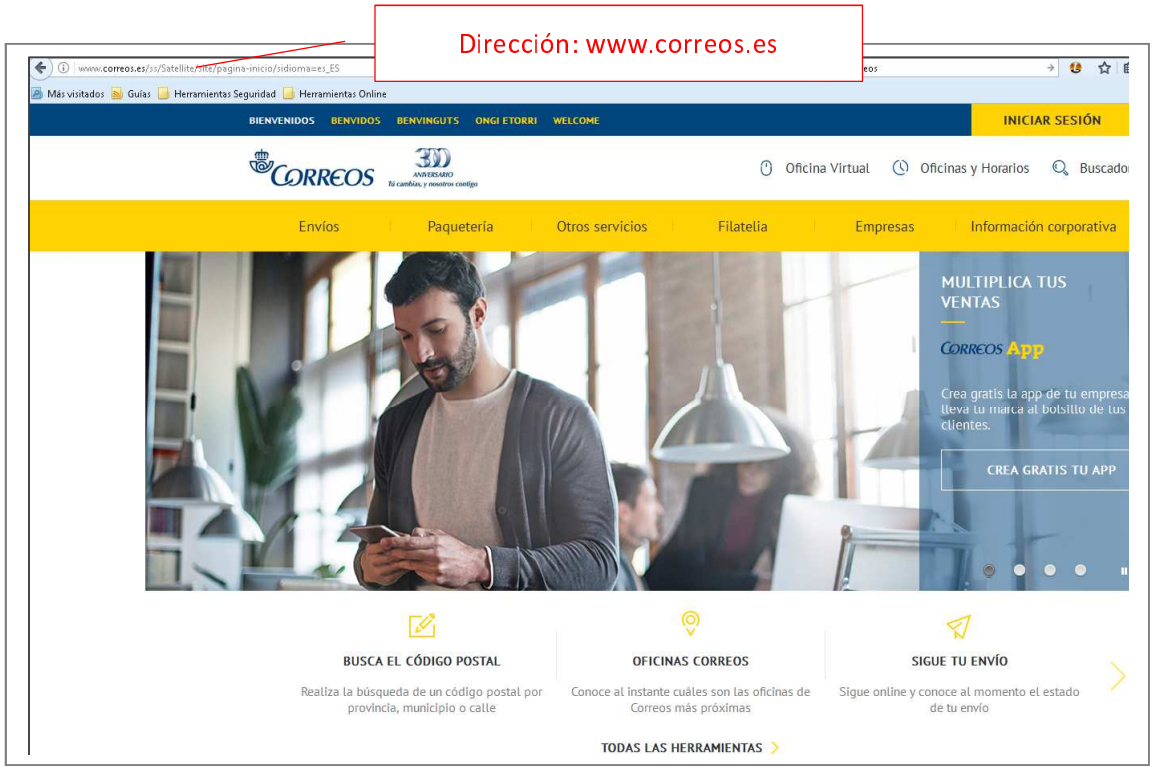
Ataques de suplantación; haciendo creer al usuario que está visitando una página fiable cuando, en realidad, se trata de una página diseñada por un ciberdelincuente con fines maliciosos, por ejemplo para robar información confidencial o distribuir malware.

[2] Actualmente es uno de los tipos de malware más dañinos y extendidos.

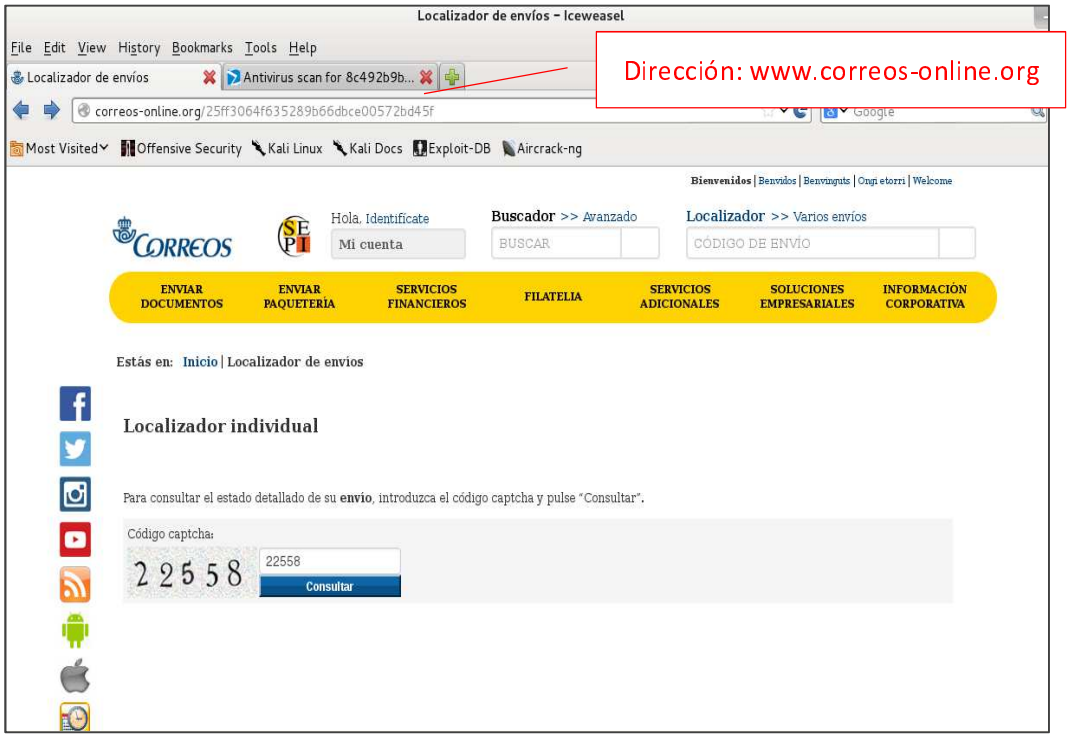
Ataques contra vulnerabilidades; aprovechando fallos de seguridad de los sistemas operativos y/o aplicaciones instaladas, como el propio navegador, con objeto de robar información sensible o descargar algún tipo de malware.

Robo de identidad; una vez los ciberdelincuentes disponen de la información de una persona (a través de alguno de los ataques anteriores), pueden utilizarla para suplantarla (por ejemplo, acceder a su cuenta bancaria) o cometer actos ilícitos en su nombre.

Acceso a información falsa o inexacta; ya que, como bien es sabido, no todo lo que se publica en internet es cierto.



Página REAL de Correos y Telégrafos (Dirección real)



Página FALSA de Correos y Telégrafos (Dirección falsa)

Recomendaciones para un uso seguro de la web

Recomendaciones generales

- **Nunca accedas a enlaces sospechosos**. Uno de los medios más utilizados para redirigir a las víctimas a sitios maliciosos son los **enlaces o hipervínculos**. Evitar hacer "click" en éstos previene el acceso a páginas web potencialmente capaces de infectar al usuario. Los enlaces pueden estar incluidos en un correo electrónico, una ventana de chat o incluso en un mensaje en una red social. Debemos analizar si nos resultan sospechosos, como por ejemplo una invitación a ver una foto que nos llega en un idioma extranjero, o un mensaje de un remitente que desconocemos.... En estos casos, no debemos acceder.

- **No accedas a sitios web de dudosa reputación**, tales como páginas de software ilegal (warez), generadores de números de serie (keygens), etc. A través de técnicas de "ingeniería social", muchos sitios web suelen "promocionarse" con información que pueden llamar la atención del usuario, como descuentos en la compra de productos (o incluso ofertas gratuitas), primicias o materiales exclusivos de noticias de actualidad, material multimedia o para adultos, etc. Es recomendable que estemos atentos a estos mensajes y evitemos acceder a páginas web con estas características.

- Se prudente con los **resultados que ofrecen los buscadores web** ya que a través de técnicas denominadas "Black Hat SEO", los ciberdelincuentes suelen posicionar sus sitios web maliciosos entre los primeros lugares en los resultados de los buscadores, especialmente en los casos de búsquedas de palabras clave muy utilizadas por el público (como temas de actualidad, noticias curiosas, venta de productos baratos, etc.).

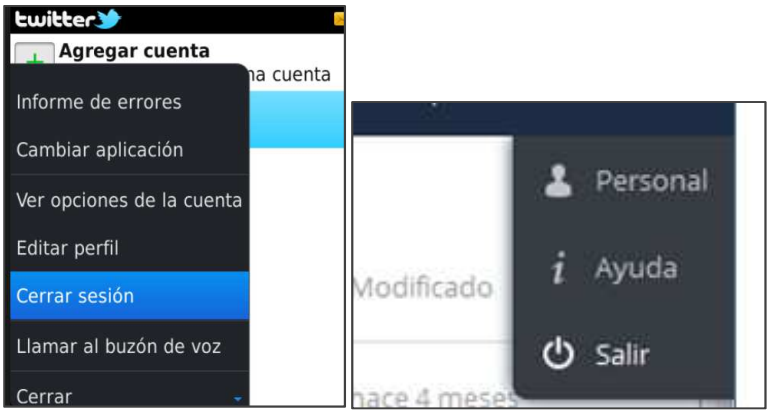
Envío de información sensible

- Utiliza "**conexiones seguras**" siempre que vayas a transmitir datos sensibles, como tu contraseña, acceder a información bancaria o realizar una compra por internet. Comprueba que la dirección web de la página a la que accedes comienza por **HTTPS**[3], pero ten en cuenta que esta es una **condición necesaria, pero no suficiente**; existen multitud de páginas HTTPS que han sido creadas por los cibercriminales para sus acciones malintencionadas.

- **Evita realizar transacciones comerciales** (compras online, acceso al banco...) o enviar información sensible **si estás utilizando un ordenador de un lugar público** (cibercafés, estaciones o aeropuertos, etc.). Igualmente, no realices transacciones comerciales estando conectado a redes públicas (habitualmente redes WiFi pública), incluso con tus propios dispositivos (ordenador, Tablet, Smartphone...).

[3] Tienes aclaraciones adicionales en el apartado "Algunas dudas frecuentes"

- **Cierra tu sesión** cuando finalices una actividad en una página web a la que hayas accedido con tus credenciales (usuario y contraseña). Según la página, el botón para cerrar sesión puede estar identificado de forma diferente ("Cerrar sesión", "Salir", etc.).



Cierre de sesión; el botón puede tener diferentes identificaciones (Cerras sesión, salir...)

Descarga de aplicaciones y archivos

- **No realices descargas de aplicaciones** desde **páginas que no sean las oficiales.**

- **Verifica todos los archivos que descargues desde internet** con un antivirus o aplicación de seguridad.

- **Ten especial precaución con la instalación de complementos extras para el navegador**, tales como barras de utilidades (Toolbars), sin verificar previamente su autenticidad. Instálalas solo si las conoces realmente y necesita usarlas. Muchas aplicaciones de software libre (Freeware) incluyen durante la instalación la posibilidad de instalar utilidades extra y barras de herramientas. Procura no instalar ninguna de estas aplicaciones extra, ya que muchas de ellas contienen malware o adware y ponen en peligro la seguridad del navegador y tu privacidad.

Ejemplo; barras de herramientas

Revisa periódicamente las aplicaciones instaladas en tu ordenador y elimina cualquier aplicación de tipo ToolBar (barra de herramientas) que resulte sospechosa o que no recuerdes haber instalado[4].

Atención a las opciones de instalación premarcadas

Uso de contraseñas en internet

[4] Tienes aclaraciones adicionales en el apartado "Algunas dudas frecuentes"

Una **contraseña segura es tu primera línea de defensa** contra los ciberdelincuentes. Por eso es necesario seguir ciertas pautas a la hora de elegir y gestionar nuestra contraseña en los servicios de internet a los que accedemos:

- **No reveles tu contraseña** a nadie.

- **Cambia tus contraseñas periódicamente y utiliza contraseñas robustas**. No dejes las contraseñas guardadas en un archivo de texto en el disco duro de tu equipo ni anotadas en un papel. Es recomendable el uso de gestores de contraseñas[5].

- **No utilices las mismas credenciales para sitios y servicios web distintos**. Si utilizas siempre las mismas credenciales y alguien las descubre, podrá usarlas para entrar también en tus cuentas de los demás sitios. Utiliza una contraseña diferente para cada servicio web.

- **Crea contraseñas que te resulten fáciles de recordar pero difíciles de adivinar** a los demás[6].

- **Ten precaución con las contraseñas que guardes en el navegador.** En general, debes evitar guardar por defecto cualquier información sensible en el navegador, como las contraseñas, ya que esta información puede ser fácilmente robada a través de aplicaciones maliciosas o virus. Nunca aceptes esta opción en un ordenador público o de uso compartido (cibercafé, etc.).

Precaución con el uso de la opción "Recordar contraseña"

[5] Consulta qué es un gestor de contraseñas en "Algunas dudas frecuentes"
[6] Tienes algunos consejos en el apartado "Algunas dudas frecuentes"

Protege tu privacidad en la red

Nunca facilites datos personales si no es estrictamente obligatorio y, en todo caso, hazlo únicamente si estás completamente seguro sobre quién los va a recibir.

No incluyas información sobre tus gustos, aficiones o preferencias en ninguna web si no quieres verte bombardeado de información comercial y publicidad relacionada con los datos registrados.

No rellenes la información que no sea obligatoria en los formularios de las páginas que requieran registro.

Evita publicar información sensible y confidencial que pueda ser usada por terceros con fines maliciosos. También es conveniente evitar la publicación de imágenes, incluido el etiquetado, propias y/o de terceros. En éste último caso, hazlo siempre con su consentimiento.

Cuando realices compras o accedas a la página de tu banco hazlo siempre desde un lugar de confianza, y nunca desde un punto de acceso público (WiFi libre, cibercafé, etc.).

Seguridad en las Redes Sociales

Lee las políticas de uso y privacidad de los diferentes servicios antes de utilizarlos, sobre todo, lo relacionado con la política de privacidad y la propiedad última de los que se publica en la red social.

Piensa antes de publicar, no sea que luego te arrepientas. Valora que información deseas revelar y controla quién puede acceder a ella. No olvides que "**lo que se sube a internet, se queda en internet**" aunque lo borres.

- **Controla tu lista de contactos**, y antes de agregar a alguien asegúrate que es de confianza.

- **No respondas a las solicitudes de desconocidos**, ya que pueden contener malware o formar parte de actividades delictivas o maliciosas. Las redes sociales contienen las mismas aplicaciones que utilizan los atacantes para propagar los virus (correo, mensajería, navegación, etc.). Mantén las mismas recomendaciones.

- Utiliza **contraseñas seguras** (robustas) para que no suplanten tu identidad.

Algunas dudas frecuentes

¿Qué significa "conexión segura"?

Normalmente, cuando navegamos por internet lo hacemos utilizando el **protocolo HTTP**; simplemente establece unas reglas sobre cómo se va a comunicar nuestro ordenador (el cliente) con una página web (el servidor). En este caso, los datos se transfieren en texto legible, por lo que si alguien intercepta la comunicación puede ver, o incluso modificar, la información (por ejemplo, si estuviéramos accediendo a nuestro banco).

Para mitigar este problema se utiliza el **protocolo HTTPS**, donde la "S" del final indica que es un protocolo HTTP, pero "seguro". Lo que hace HTTPS es **cifrar** la comunicación entre nuestro equipo y el servidor web de forma que, aunque fuera interceptada por alguien, no sería capaz de entenderla. Este proceso se realiza mediante algoritmos matemáticos bastante complejos.

Protocolo inseguro

Protocolo seguro

Sin embargo, hay que señalar que, aunque es una condición necesaria para que una página sea segura, **no es suficiente ya que los cibercriminales, hoy en día, también pueden crear páginas que utilicen HTTPS**.

¿Qué es el Cybersquatting y cómo podemos protegernos?

Resolved (9) Available (367) Errors (1)

Domain	IP Address / A record
www.masesa.com	104.17.197.60
www.emassa.com	23.20.239.12
www.emases.com	50.63.202.12
www.emase.sa.com	141.8.226.34
www.emasea.com	37.60.253.182
www.emaesa.com	50.63.202.35
www.em.asesa.com	195.235.35.111
www.emsesa.com	160.153.40.9

Dominios existentes, similares a www.emasesa.com

El **Cybersquatting**, también conocido como **"apropiación de dominios"** o **"ciberocupación"** ("squat" significa "apropiarse, ocupar"), se refiere al **registro** por parte de **cibercriminales** de un determinado **dominio muy similar a otro legítimo**, con objeto de utilizarlo **para fines fraudulentos**. Por ejemplo, es habitual crear una web falsa suplantando a la de un dominio legítimo, para robar credenciales o descargar malware si un usuario accede a la web.

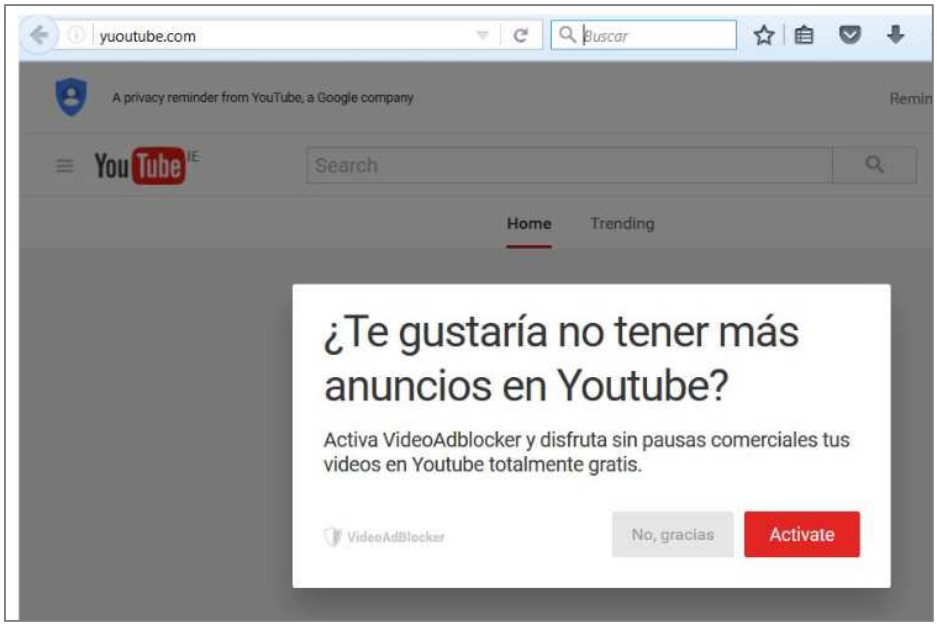
Existen diferentes métodos utilizados por los cibercriminales para aprovecharse de esta "apropiación de dominios". Estos son dos de los más habituales.

- El **Typosquatting**; no tiene una definición concreta en castellano, pero podríamos definirlo como el hecho de que un usuario abra una página diferente a la que se pensaba visitar al **teclear por equivocación** una dirección web. En este caso, los cibercriminales registran dominios similares al legítimo basándose en las faltas ortográficas o errores de escritura comunes de los usuarios al escribir.

- El ataque mediante **dominios homográficos**; consiste en enviar enlaces en correos electrónicos o aplicaciones de mensajería (WhatsApp, Telegram, SMS, etc.) que incluyan **direcciones que se lean de forma muy parecida a los originales**, pero realmente sean distintos, simplemente **cambiando alguna letra o carácter** para que el usuario no se percate de esta diferencia. Como ejemplo, fíjate en estas tres direcciones:

- www.ema**S**esa.com
- www.emasesa.com
- www.**e**masesa.com

No son iguales; hay caracteres diferentes, aunque a simple vista son muy parecidos. Cada una de las direcciones anteriores te llevaría a un domino diferente, pero sólo una es la legítima de EMASESA. En una lectura rápida ¿te hubieras percatado del engaño?



Página web falsa ("yuoutube" en lugar de "youtube")

Estos consejos pueden resultarte útiles, para **protegerte contra el Cybersquatting**:

- **Al escribir la dirección URL en el navegador, asegúrate de que lo haces correctamente**; cualquier error ortográfico pueden dirigirte a un sitio web "ciberocupado" que sea malicioso.

- Al **recibir un enlace** en un correo o aplicación de mensajería (WhatsApp, Telegram, SMS, etc.), **y estás seguro de que el remitente es de confianza**, es **preferible escribirlo** (correctamente) en el navegador antes que "clicar" sobre el enlace, pero si lo haces,

asegúrate bien de que la dirección que aparece en el navegador es la correcta revisándola detenidamente (está bien escrita, es la correcta y no aparecen caracteres "extraños").

- **No introduzcas información personal ni datos sensibles en una página web a no ser que estés absolutamente seguro de su legitimidad**.

¿Cómo puedo crear una contraseña robusta y fácilmente recordable?

Para crear una contraseña segura utiliza un mínimo de 9 caracteres, e incluye mayúsculas, minúsculas, números y caracteres especiales (@,#,$,...). Partiendo de estos criterios, un par de mecanismos sencillos para generar una contraseña robusta son:

1. Por ejemplo, imagínate y recuerda una frase como "Terminé de estudiar en el colegio en 2004" y usa las iniciales de cada palabra de este modo: "Tdeeece2004". Cuanto más largas sean, mejor, así resultarán más difíciles de descubrir.

2. Otra buena opción, complementaria a la anteriores, sería cambiar algunas letras minúsculas por mayúsculas y escribir un número o un carácter especial en vez de una letra o viceversa, por ejemplo:

    - Empezar y acabar con mayúsculas.
    - Poner una "n" en vez de una "ñ".
    - Cambiar una "e" por un "3".
    - Cambiar la letra "a" por un "@".
    - Cambiar la letra "o" por un "0".

    Aplicando estas reglas sencillas, la palabra, "compañeros" podría transformarse en la contraseña "C0mp@n3r0S".

Si quieres saber si tu contraseña es segura, puedes comprobarla en la siguiente dirección:

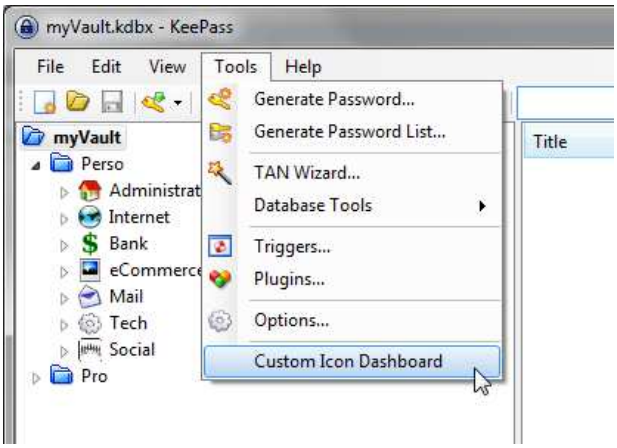
https://password.kaspersky.com/es/

¿Qué es un gestor de contraseñas?

Es necesario tener una contraseña diferente en cada servicio web al que accedamos (Banco, Facebook, Gmail, etc.). Para evitar tener que apuntarlas o memorizarlas, se puede utilizar un tipo de software que permite gestionarlas, esto es, un **gestor de contraseñas.** Se trata de una **aplicación que almacena todas tus contraseñas en un único archivo cifrado, al cual sólo se puede acceder si conoces una contraseña "maestra"**. La aplicación es capaz de generar y proponerte contraseñas robustas según los criterios que establezcas (número de caracteres, uso de caracteres especiales, números, etc.). Una vez generas la contraseña, puedes guardarla en la aplicación indicando los detalles de a qué servicio corresponde (banco, Facebook, etc.). De esta forma, puedes tener todas las contraseñas bien organizadas y correctamente protegidas siempre, claro está, que tu contraseña "maestra" que es la única que deberás recordar, sea suficientemente robusta.

Dispones de numerosas soluciones, tanto en aplicaciones de escritorio como aplicaciones online que puedes utilizar en tu ámbito personal. Una aplicación gratuíta y muy útil es "Keepass", disponible en esta dirección:

https://keepass.info/



Aspecto del gestor de contraseñas Keepass

¿Puedo infectar mi equipo si simplemente navego por internet?

Desgraciadamente **la respuesta a esta pregunta es afirmativa**. Los atacantes son capaces de aprovecharse de un fallo de seguridad (vulnerabilidad) y tomar el control de un ordenador, simplemente por haber abierto una página infectada. Esta técnica se conoce como "Drive-by download". Para minimizar este riesgo **es importante que los navegadores que uses estén debidamente actualizados**, al igual que sus complementos y plugins.

Para proteger tu equipo de casa, debes mantener el navegador al día. Te recomendamos que configures la opción de "actualizaciones automáticas". Esta funcionalidad viene incorporada en los principales navegadores. Aquí tienes un resumen de la forma de hacerlo.

Navegador	Cómo actualizar
Internet Explorer	En Windows, el navegador se actualiza a través del mismo mecanismo del sistema operativo:activando las actualizaciones automáticas. Ante grandes actualizaciones, como el paso de Internet Explorer 6 a Internet Explorer 7, es necesario confirmar el proceso (recomendado).
Firefox	Se actualiza de forma automática por defecto. Al ejecutarlo, busca actualizaciones, no sólo del navegador, sino de todos los accesorios (complementos o plugins) instalados. Lo descarga y pide permiso para reiniciarlo. Para forzar actualización: Actualizar Mozilla Firefox
Chrome	Se actualiza de forma automática por defecto. Al ejecutarlo, busca actualizaciones, no sólo del navegador, sino de todos los accesorios (complementos o plugins) instalados. Para forzar actualización: Actualizar Google Chrome

Configuración actualización en los principales navegadores

¿Por qué al acceder a algunas páginas web aparece un aviso de que la página no es segura?

Cuando el navegador se conecta a una "página segura" (como hemos visto, la URL empieza por "https://"), debe comprobar que:

- La página es auténtica; esto lo realiza validando el certificado digital.
- El cifrado de la comunicación es lo suficientemente fuerte como para que no pueda ser descifrado.

Página segura; la URL empieza por "https"

NOTA
El proceso de validación de un certificado digital es, de forma resumida, el siguiente:

Para que el certificado digital sea válido tiene que estar emitido por una "entidad de confianza". La identidad de esta "entidad de confianza" es un dato que aparece en el propio certificado. Así, cuando el navegador "recibe" el certificado digital del servidor, "pregunta" a la "entidad de confianza" que aparece en el mismo, si realmente ha emitido el certificado, si se corresponde efectivamente con la página a la que estamos queriendo acceder y si sigue siendo válido.

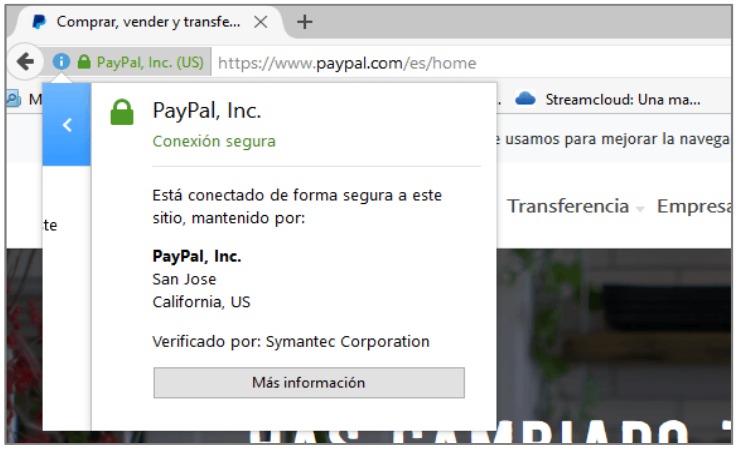
Por hacer un símil sería algo así como pedir un DNI (sería el certificado digital) para identificar a una persona que nos da su nombre y apellido. Con ese DNI preguntaríamos a la Policía (sería la "entidad de confianza") si ese es válido y si realmente se corresponde con quien la persona dice ser.

En caso de que el certificado no cumpla con alguna de las condiciones indicadas, al intentar acceder a la página aparecerá un mensaje de advertencia similar al siguiente:

Aviso por certificado digital no confiable

En estos casos, **debemos estar muy seguros** de lo que hacemos antes de acceder a la página utilizando la opción *"O puede añadir una excepción"*.

Un ejemplo certificado de seguridad válido sería el que se muestra en la siguiente imagen:



Ejemplo certificado digital válido (candado cerrado)

¿Cómo puedo analizar si un fichero tiene algún virus?

Como ya hemos indicado, es necesario verificar todos los archivos que descargues desde internet con un antivirus o aplicación de seguridad. Para ello, existen varias herramientas online gratuitas como por ejemplo **VirusTotal.** El enlace a esta web es:

https://www.virustotal.com/es/

Página web de Virustotal

Otra alternativa la puedes encontrar en el siguiente enlace

https://www.hybrid-analysis.com/

Página web de Hybrid-Analysis

¿Cómo puedo revisar periódicamente mi PC?

A nivel doméstico te aconsejamos que tengas un **antivirus convenientemente actualizado y que revises tu equipo periódicamente con algún antivirus específico.** Para ello te recomendamos las aplicaciones gratuitas Spybot Search and Destroy y Malware Bytes, mediante las cuales puedes analizar periódica y fácilmente tu equipo en busca de amenazas.

¿Cómo puedo comprobar si una página web es segura?

Para comprobar la seguridad de una página web puedes alguno de los servicios gratuitos disponibles en internet. Te recomendamos:

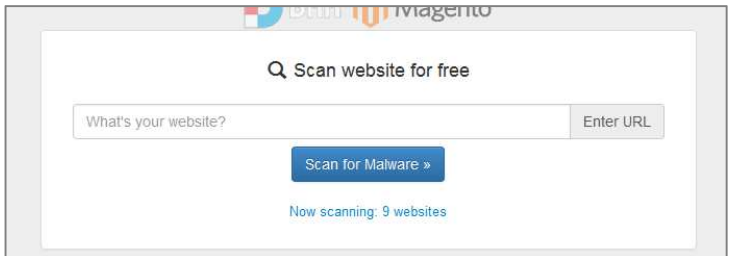
Virustotal

https://www.virustotal.com/es/

Página web de Virustotal

Quttera

https://www.quttera.com/



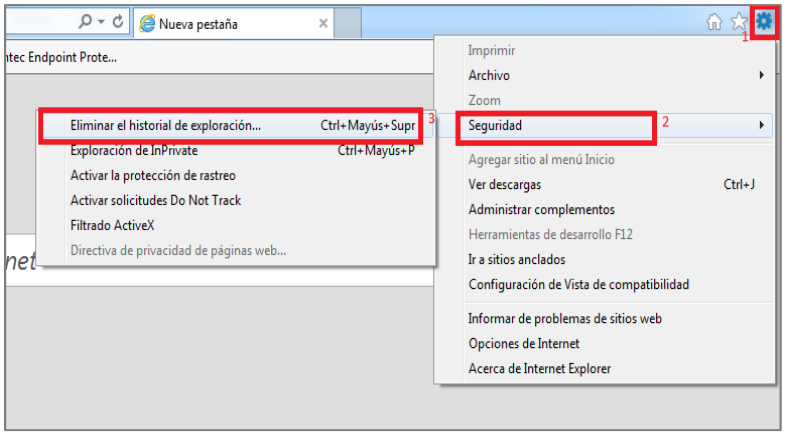
Página web de Quttera

¿Qué es y cómo puedo eliminar mi historial de navegación?

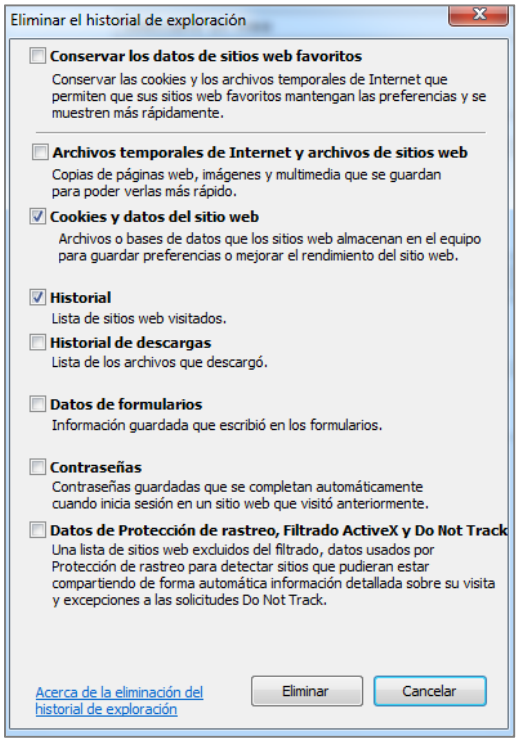
El **historial de navegación es un registro de todas las páginas que visitamos en Internet con nuestro navegador**. Esto puede resultar práctico en muchas ocasiones para encontrar más fácilmente las páginas que estuvimos visitando en días anteriores, pero también tiene su parte negativa: permite a cualquier persona que tenga acceso a nuestro ordenador saber qué es lo que hemos estado haciendo en internet. Es especialmente aconsejable borrar el historial de navegación si utilizamos un ordenador compartido (por

ejemplo, en un cibercafé). El procedimiento para **borrar el historial** depende del navegador:

Internet Explorer: En este caso hay que acceder al icono de configuración y hacer clic en "seguridad". Después de esto, tan solo hay que acceder a "Eliminar el historial de exploración y seleccionar los datos que desees borrar. Finalmente se selecciona "eliminar" y listo.

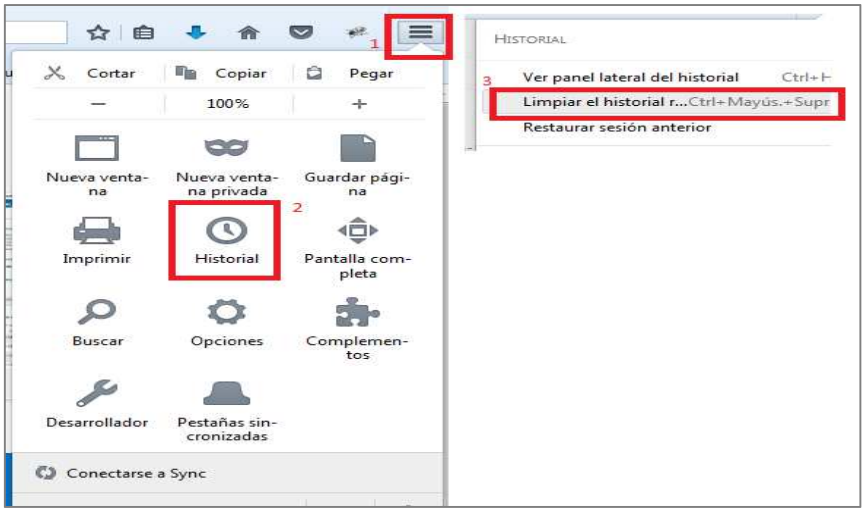


Eliminar historial navegación IE



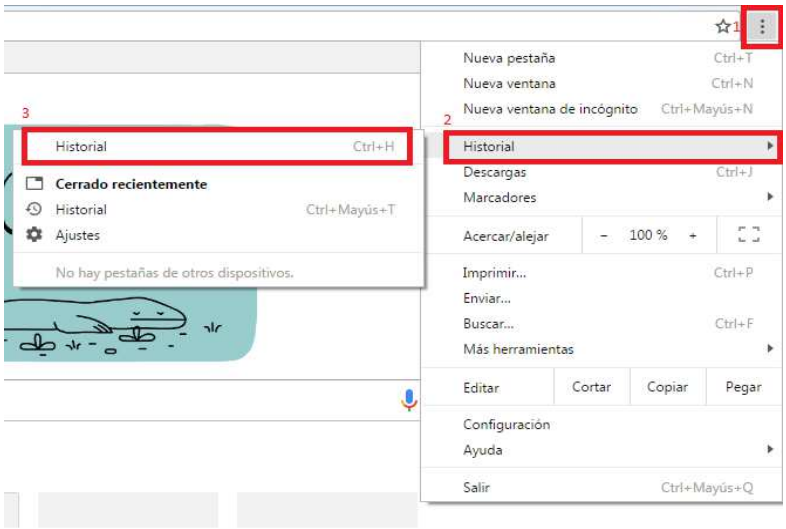
Opciones de eliminación en IE

Mozilla Firefox: tienes que acceder al menú y acceder a "historial". Luego tan solo hay que pulsar sobre "limpiar el historial reciente", donde podrás seleccionar el intervalo de tiempo y los elementos que quieras borrar.



Eliminar historial Firefox

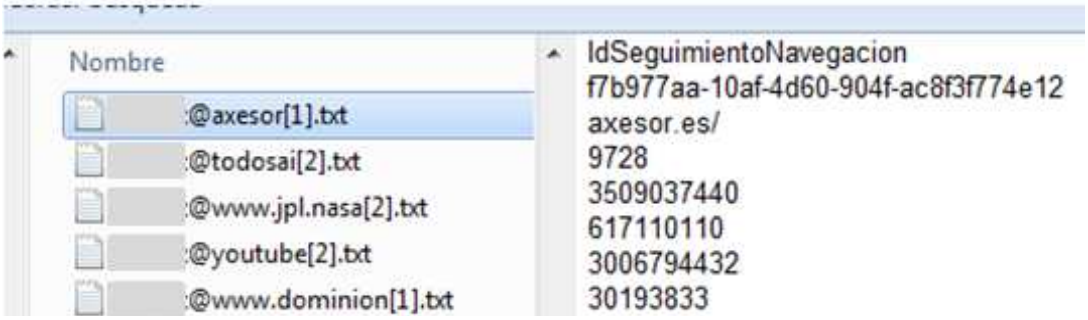
Google Chrome: debes hacer es acceder al menú de Chrome, pulsando en el icono en la esquina superior derecha. Una vez abierto, accede al apartado de "historial" y una vez dentro, encontrarás una opción llamada "Borrar datos de navegación". Una vez hecho esto, aparecerá un cuadro donde podrás determinar las fechas concretas que quieres eliminar, o si quieres eliminarlo todo.



Eliminar historial Chrome

En muchas ocasiones cuando accedo a una página aparece un aviso de "Aceptar Cookies" ¿qué significa?

Las cookies son pequeños ficheros de texto que un servidor web envía a nuestro navegador cuando accedemos a una página web. Estos ficheros se guardan localmente en nuestro equipo.



Ejemplo contenido de una cookie

En general, almacenan nuestras preferencias cuando navegamos por una página web, por ejemplo, productos añadidos al "carrito de la compra", idioma seleccionado, credenciales de acceso, etc. Su objetivo, en principio, es facilitarnos la navegación.

Sin embargo, existen también cookies publicitarias, que almacenan información sobre los lugares que hemos visitado y que permiten que se nos ofrezca una publicidad acorde a lo que nos interesa. En algunos casos estas cookies son tan intrusivas que llegan incluso al espionaje informático.

Ante esta situación se publicó la conocida como "Ley de Cookies", que obliga a los propietarios de las páginas web a informar a los usuarios de las cookies que utilizan y sus características a través de la "Política de Cookies", y solicitar su autorización.

Ejemplo aviso "aceptación de cookies"

Además de la posible intromisión en nuestra intimidad, las cookies pueden sobrecargar el navegador a medida que van aumentando en número, por lo que es una práctica aconsejable eliminarlas de forma periódica. Para borrarlas, hay que ir a la configuración del navegador y borrar todo el historial de navegación (explicado en el apartado "¿Cómo puedo eliminar mi historial de navegación?"), con la inclusión de todas las cookies.