Como navegar de forma segura por Internet

Es fundamental tener en cuenta la importancia que tiene navegar por internet de forma segura. De esta manera el usuario incrementará notablemente los beneficios que obtiene de Internet.

¿Qué es navegar de forma segura por internet?

Navegar en forma segura por internet es adquirir ciertos hábitos y precauciones que reduzcan el riesgo de ser víctimas de fraudes y ataques para así lograr una navegación confiable por la web.

Para navegar por la web necesitamos un navegador web que nos permitirá simplemente recorrer la red de internet, comprar online o revisar nuestras cuentas bancarias, en todas estas acciones necesitamos un poco de sentido común y determinadas pautas para mantener todos nuestros dispositivos libres de virus y amenazas.

¿Por qué es importante navegar de forma segura?

Es importante navegar de forma segura porque hay muchos factores personales que entran en juego y que deben se cuidados. La privacidad personal en línea general, el secreto de nuestros datos como contraseñas y usuarios, los archivos importantes que tenemos alojados en los diferentes dispositivos y nuestros hábitos de navegación en internet pueden ser algunos de los factores que debemos proteger.

¿Cómo se puede navegar en Internet de forma segura?

Para **navegar por Internet en forma segura** hay que respetar la mayor cantidad de las siguientes recomendaciones:

Mantener actualizado el Software Antivirus

Sí o sí hay que tener un software antivirus correctamente instalado y actualizado en el dispositivo. También se recomienda adquirir las licencias anuales de los antivirus premium, ya que los mismos brindan una mayor y completa cobertura en la protección del dispositivo. Estas licencias en general tienen un costo anual bajo. Los antivirus Premium evitan que software malicioso se instale en nuestro Pc y que hackers espíen nuestros archivos y comportamientos o tomen control de nuestra cámara web.

Mantener actualizado el Sistema Operativo del PC

Todos los fabricantes de Sistemas Operativos ofrecen al mercado la versión original y luego paulatinamente van publicando actualizaciones para instalar. Hay que aceptarlas y llevar a cabo la actualización del sistema. Las mismas aportarán soluciones a problemas de seguridad encontrados y también generarán cambios y mejoras en la estética del software.

Mantener actualizado los Navegadores Web

La principal herramienta para navegar por Internet es el **Navegador Web**, el cual también es un software que tiene un desarrollo natural desde que es lanzado al mercado. Ante esta situación debemos ser conscientes del grado de actualización de los mismos. Algunos se actualizan automáticamente, pero siempre hay que chequear que tengamos la última versión instalada.
Como se aclaró en el punto anterior, las actualizaciones ofrecen parches a huecos de seguridad, como también, cambios en la estética y características.

Hay que utilizar una red Wi-Fi o LAN conocida para navegar por internet

Una **red conocida** es la de nuestro hogar, la de nuestro trabajo o la de algún familiar. Las redes desconocidas pueden ser las redes gratuitas de los bares, centros comerciales, hoteles o tiendas. En general, suelen ser muy poco seguras ya que todos

tienen acceso a ellas y allí es donde ciberdelincuentes navegan con nosotros en la misma red. Entonces, toda la información que se envía por estas las conexiones públicas pueden ser capturados fácilmente por estos hackers o ciberdelincuentes.
Si podemos evitar pedir contraseñas para acceder a estas redes, mucho mejor.

Generar contraseñas seguras y diferentes

Todos los sistemas que son utilizados por diferentes usuarios necesitan una contraseña para ingresar a trabajar. Ejemplo de ellos son el Correo Electrónico, los sistemas de Homebanking, las Redes Sociales, etc.
Lo que se recomienda es que **se utilicen contraseñas diferentes** para cada sistema, ya que si alguien descubre una, sólo podrá ingresar a un sistema y no a todos los sistemas con los que trabajamos.
También es fundamental que en el momento de la creación de la contraseña se elijan al menos **8 caracteres intercalando mayúsculas, minúsculas, números y caracteres especiales** como un signo de interrogación.

La generación correcta de contraseñas es clave en los hábitos para navegar en forma segura por Internet.

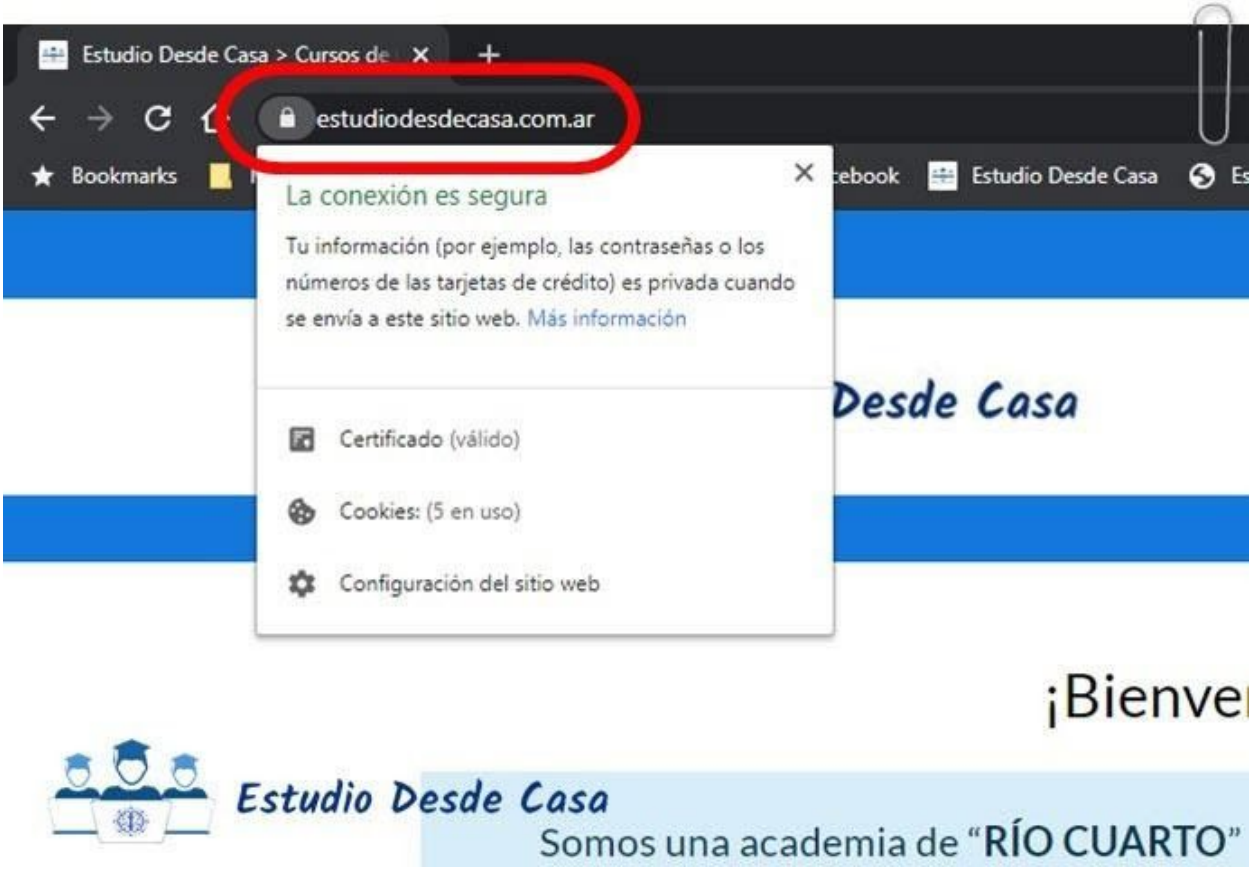
No te olvides nunca de cerrar sesión

Puede ser un poco tedioso pero internalizar el hábito de cerrar sesión en cada sistema que utilicemos no ahorrará muchos dolores de cabeza. Y mucho más aún, si la computadora es utilizada por varios usuarios esta conducta es obligatoria. Si dejamos

abiertas nuestros sistemas, el próximo navegante podrá ingresar a los mismos sin problemas.
Cabe aclarar, que algunos sistemas se auto cierran por inactividad como los sistemas de homebanking. Pero siempre luego de trabajar, es recomendable avisar que nos estamos retirando.

Hay que reconocer las páginas web que ofrecen navegación segura

Siempre cuando ingresamos a navegar por una web debemos chequear que nos ofrezca un sistema de navegación segura.



Saber detectar cuando un sitio web presta el servicio de sitio seguro incrementa la confianza para intercambiar información con el mismo.

¿Cómo identificar sitios seguros y no seguros?

Tenemos que observar arriba en la barra de dirección del navegador que su dirección web esté encabezada por un "Candado" o por un "Https".
Este nivel de seguridad nos indica que todos los datos que intercambiemos con ese sitio web viajarán por internet encriptados y si son interceptados por un hacker van a ser ilegibles para él.

¿Qué hacer cuando la conexión no es segura?

Si navegamos por un sitio no seguro sólo debemos tener cuidado de la información que proveemos. Se puede navegar con tranquilidad sin intercambiar información

sensible. En la actualidad, la navegación segura es un protocolo que todos los sitios serios buscan tener.

Nunca hay que proporcionar datos personales de acceso de nuestros sistemas

Ningún sistema serio pedirá a través de un formulario web o por correo electrónico nuestros datos personales de acceso como son nombres de usuario y contraseñas. Ya que esos datos son privados, son conocidos por los dueños del sistema y están guardados en sus bases de datos. Es como si Google nos pidiera que le recordemos la contraseña que usamos para ingresar a nuestro correo. Si Google no conociera esa contraseña no nos dejaría entrar directamente.
Evita el phishing o robo de identidad. Ingresa aquí a leer este artículo que te explica bien sobre este tema (https://estudiodesdecasa.com.ar/que-es-el-phishing/).

Hay que considerar la navegación en incognito

La navegación en incógnito es una modalidad de navegación que ofrecen casi todos los navegadores web actuales. En este modo de navegación, el navegador web no guarda ningún tipo de información sobre las páginas web visitadas. Eliminan las cookies y borran la memoria tras salir del navegador. No guardan las páginas visitadas en el historial ni muestran información de los archivos que se descargaron. Y tampoco guardan las contraseñas y ni permite el autocompletado de formularios.
Esta es una muy buena opción para no dejar rastros de que hemos navegado por alguna web en especial. También podemos utilizarla cuando usamos equipos de terceros.

¿Cómo abrir una ventana en modo incógnito?

Cuando necesitemos ingresar en modo incógnito a una página web, sobre el enlace a esa página hacemos Clic Derecho y luego Clic en la opción “Abrir el enlace en una ventana de incógnito”. Ante ésto, se abre una nueva ventana para navegar totalmente sin dejar rastros.

Utiliza dispositivos de confianza para operaciones confidenciales

Es recomendable utilizar dispositivos de confianza para realizar operaciones confidenciales. Estos dispositivos son los propios o de personas que sabemos que respetan las normas de seguridad mínimas. Los dispositivos peligrosos pueden tener instalados programas maliciosos que roben la información que introducimos. Por lo tanto, las computadoras públicas de Hoteles, bibliotecas o aeropuertos se deberían utilizar para navegación básica en la cual no se introduzca información sensible.

Realizar las compras online con precauciones

Al momento de realizar compras a través de Internet, asegúrate de que sea a través de sitios reconocidos para la compra y venta como por ejemplo Mercadolibre. También tienes que chequear que la url del sitio (la dirección web) coincida con la web donde crees estar y que su dirección empiece con https o el candado de navegación segura.

Hay que tener cuidado con los contactos desconocidos en las diferentes redes sociales

Las redes sociales son justamente lugares para intercambiar información con contactos desconocidos. Hay que tener mucho cuidado con la información sensible que intercambiemos con ellos. Nunca hay que proveer ese tipo de información como por ejemplo: nombres de usuario, contraseñas, direcciones, permisos especiales, etc. Ellos pueden utilizar esta información con fines maliciosos.

No publiques nada en internet que no te gustaría ver en un cartel inmenso con tu foto en él.

Nunca publiques nada en internet si no quieres que todo el mundo se entere. Publicar, justamente significa “hacer público”, por lo que es muy importante que analices minuciosamente lo que vas a publicar en la web y en las redes sociales. Tienes que cuidar tu identidad y la de tus seres queridos, ten mucho cuidado con las fotos y textos que publiques.
Si necesitas compartir información privada con tus contactos, existen muchas opciones de hacerlo en forma segura.

Sólo descargue software de sitios oficiales

Es muy común y necesario descargar e instalar software en nuestros dispositivos para realizar tareas puntuales. Ante ésto, siempre hay que chequear que el software provenga del sitio oficial del fabricante, ya que de no se así se corre el riesgo que el mismo esté infectado por códigos maliciosos que se introducirán en nuestro dispositivo.

Hay que tener precaución con los email recibidos y los enlaces sospechosos

Muchas veces vas a encontrar en tu bandeja de entrada emails de remitentes desconocidos. Los asuntos de estos correos generalmente llaman mucho la atención. Incluso se adaptan a nuestros gustos y preferencias. Cualquiera sea el caso, no hay que fiarse de ellos. **Nunca hay que hacer clic en los enlaces o documentos adjuntos de esos mensajes desconocidos**. Si hacemos clic en estos enlaces se nos cargará una página que seguramente nos solicitará el ingreso de datos personales privados, para así quedarse con ellos.
¡Nada es gratis! No se deje engañar con promociones sumamente atractivas.

Tampoco es recomendable responder a estos correos, ya que estaríamos facilitando datos personales importantes, como nuestra dirección de correo o nombre.
Lo más correcto en este caso es borrar estos correos sospechosos o abandonar los sitios webs que nos impongan estas acciones e ignorar los enlaces que tengan dudosa procedencia.

No des información de tu geolocalización en las redes sociales

Nunca des información de tu geolocalización en las redes sociales bajo ningún medio. Tampoco es recomendable publicar fotografías de tu geolocalización en vivo, cuando participas de viajes o estás en otras ciudades.
La información de dónde estás en tiempo real podrá ser tomada por ladrones o personas maliciosas y ser usada en tu contra.

Debes realizar limpieza de tu equipo periódicamente

Es muy recomendable realizar limpiezas de los dispositivos que usamos en forma periódica. Esta actividad se realiza con diferentes softwares especializados como por ejemplo los conocidos Ccleaner y AdwCleaner. En líneas generales, la limpieza consiste en eliminar residuos de la navegación por internet, archivos temporales, limpieza de cookies, del historial de navegación y fundamentalmente de códigos maliciosos que se puede haber instalado en nuestro dispositivo.
Literalmente, luego de la limpieza, se comienza a trabajar casi como si estuviéramos el dispositivo nuevo.