# CONSEJOS DE SEGURIDAD EN INTERNET

Cuando sales de casa, tomas algunos recaudos para protegerte de asaltos y otros peligros existentes en las calles. En internet, es igualmente importante poner en práctica algunos procedimientos de seguridad, ya que **los ataques, el espionaje y el robo de archivos y contraseñas son sólo algunos de los problemas** que las personas pueden tener en la red de redes. Para ayudarte a lidiar con esto presentamos a continuación **quince consejos importantes para que puedas mantener tu seguridad en internet y en tu computadora.**

## Siempre haz click en "Cerrar Sesión" o su equivalente.


Al acceder a tu casilla de correo electrónico, tu cuenta en tu red social, tu home banking o cualquier otro servicio que solicite que ingreses un nombre de usuario y una contraseña, **siempre haz click en el botón o link denominado "Salir", "Desconectar", "Cerrar Sesion"** o alguno similar, para salir del sitio web con seguridad. Puede parecer obvio, pero mucha gente simplemente sale del sitio web cerrando la ventana del navegador o entrando a otra dirección. Esto es riesgoso, pues el sitio web no recibió la orden de cerrar el acceso, y **alguien puede abrir el navegador y tener acceso a la información de tu cuenta.**

## Crea contraseñas difíciles de ser descubiertas.

No utilices contraseñas fáciles de ser descubiertas, como el nombre de hijos o parejas, fechas de cumpleaños, patente del auto, etc. **Trata de usar secuencias que mezclen letras, números y caracteres especiales (como "%&()/").** Además, no uses como contraseña una combinación que tenga menos de 6 caracteres. Lo más importante: no guardes tus contraseñas en archivos de Word o de cualquier otro programa. Si necesitas guardar una contraseña en papel (en casos extremos), destrúyelo después de memorizar la secuencia. Además de eso, **evita usar la misma contraseña para varios sitios web.** Haz click y aprende **cómo crear contraseñas seguras**

## Cambia tu contraseña periódicamente.

Además de crear contraseñas difíciles de ser descifradas, **es esencial cambiarlas periódicamente, cada tres meses por lo menos.** Ya que si alguien consigue descubrir la contraseña de tu e-mail, por ejemplo, podrá leer tus mensajes sin que lo sepas, sólo para espiarte. Al cambiar tu contraseña, el espía ya no podrá acceder a tu información personal.

## Usa navegadores diferentes

Si eres usuario de Windows, tal vez tengas el hábito de utilizar el navegador Internet Explorer. El problema es que existe una infinidad de plagas digitales (spywares, virus, etc.) que exploran problemas de seguridad de ese navegador. Por esto, **una acción importante es utilizar navegadores como Chrome o Firefox,** pues aunque éstos también puedan ser atacados por plagas, sucede con una frecuencia menor que para el Internet Explorer.

Haz click para **adentrarte en el mundo de los navegadores de internet**.

## Cuidado con las descargas

Si usas **programas para descargar archivos, como Emule o Ares,** o sueles descargar archivos de sitios webs de descargas, estate alerta a cada cosa que bajes. **Al finalizar una descarga, verifica si el archivo no posee algo extraño,** por ejemplo, más de una extensión (como "programa.mp3.exe"), tamaño muy pequeño o información de descripción sospechosa, pues **muchos virus y plagas pasan por archivos de audio o vídeo para engañar al usuario.** Además de esto, siempre examina el archivo que descargaste con un antivirus.

También ten cuidado de **aquellas webs que te soliciten la instalación de un programa para continuar la navegación,** o para acceder a algún servicio. Desconfía también de las ofertas de programas milagrosos, capaces de doblar la velocidad de tu computadora o de mejorar la performance.

## Cuidado al usar Windows Live Messenger, Google Talk, AIM, Yahoo! Messenger y otros.

Es común **encontrar virus que rondan por los servicios de mensajes instantáneos**, tales como el Windows Live Messenger, Yahoo! Messenger, entre otros. Esas plagas son capaces, durante una

conversación con un contacto, de emitir mensajes automáticos que contienen links que acceden directamente a virus u otros programas maliciosos. En esta situación, **es natural que el interlocutor que recibió el mensaje crea que su contacto es quien lo envió y acepte el envío.**

Si durante una conversación **recibes un link que no estabas esperando,** pregúntale al contacto si fue él quien lo envió. Si él no fue, no hagas clic sobre ese link y dile a ese contacto que **su computadora puede estar infectada con un virus.**

## Cuidado con los e-mails falsos

Tal vez hayas recibido en algún momento un e-mail que informa sobre una deuda con una empresa de telefonía, o que afirma que uno de tus documentos no es legal. **O un mensaje que te ofrece premios, o tarjetas virtuales de amor.** Te intimaron a una audiencia judicial?

Es probable que **se trate de un spam, o sea, un e-mail falso. Si el mensaje presenta un texto con errores ortográficos y gramaticales, hace ofertas tentadoras o tiene un link diferente del indicado** (para verificar el link verdadero, basta pasar el mouse por encima de él, pero sin hacer clic y mirar en la barra de abajo a que dirección apunta realmente), desconfía inmediatamente. Ante la duda, entra en contacto con la empresa cuyo nombre aparece en el e-mail.

## Evita sitios webs de contenido dudoso

Muchos sitios webs contienen en sus páginas scripts capaces de buscar fallas del navegador de internet, principalmente Internet Explorer. Por eso, **evita navegar en sitios webs pornográficos, de contenido hacker o que tengan cualquier contenido dudoso.**

## Cuidado con los adjuntos en un e-mail.

Este es uno de los problemas más comunes. El e-mail es una de las principales formas de diseminación de virus. **Ten cuidado al recibir mensajes que te piden abrir un archivo adjunto, principalmente si el e-mail proviene de alguien que no conoces.** Para aumentar tu seguridad, puedes chequear el archivo adjunto con un antivirus, inclusive si esperabas recibir ese archivo.

## Actualiza tu antivirus y tu antispyware

Mucha gente piensa que con sólo **instalar un antivirus**, su computadora estará protegida, pero no es suficiente. **Es necesario chequear que se mantenga actualizado, de lo contrario, el antivirus no podrá reconocer la existencia de nuevos virus.** Además de eso, utiliza a menudo un antispyware para quitar archivos y programas maliciosos de su computadora. **Una buena opción es Spybot.** Lo mismo que el antivirus, el antispyware también debe ser actualizado para poder reconocer nuevas plagas.

En ambos casos, verifica en el manual del software o en el sitio web del creador cómo chequear que se realizan las actualizaciones.

## Cuidado al realizar compras en internet o al usar sitios webs de bancos.

Hacer compras a través de internet es una gran comodidad, pero **sólo hazlo en aquellos sitios de vendedores reconocidos.** Si estás interesado en un producto que se ofrece en un sitio web desconocido, haz una búsqueda en internet para descubrir si alguien tuvo problemas con esa empresa.
Aquí encontrarás **consejos para comprar seguro en Internet**

Al acceder a tu cuenta bancaria a través de internet también ten cuidado. Evita hacerlo en computadoras públicas, **verifica siempre si la dirección del link es realmente la del sitio web del banco y sigue todas las normas de seguridad recomendadas por el banco.** *JAMAS ingrese a un sitio web de Home Banking desde un link de un e-mail*. Siempre accede escribiendo la dirección en el navegador. Una de las reglas de seguridad de todos los bancos es no enviarte un link de acceso al sitio web de la entidad en un mail.

## Actualiza tu sistema operativo

Windows es el sistema operativo más utilizado en el mundo, y cuando se descubre un fallo de seguridad, una serie de plagas digitales son desarrolladas para explorarlos. Por eso, **configura tu Windows para que se actualice automáticamente.**

Si es usuario de otro sistema operativo, como Mac OS o alguna distribución Linux, este consejo también es válido. **Los fallos de seguridad existen en cualquier sistema operativo,** por eso es importante aplicar las actualizaciones puestas a disposición por los creadores.

## Actualiza también los programas

También es importante **mantener tus programas actualizados.** Mucha gente piensa que las versiones nuevas sólo añaden funcionalidades operativas, pero la verdad es que también se realizan correcciones para fallos de seguridad. Por eso, **siempre utiliza la última versión de tus programas, especialmente los que acceden a internet** (navegadores de internet, clientes de e-mail, etc.). Muchas aplicaciones cuentan con una funcionalidad que actualiza el programa automáticamente o alerta por lanzamientos de nuevas versiones. Es un bueno activar esa funcionalidad.

## No reveles información importante sobre tu persona.

En las redes sociales como Facebook, Google+ o Twitter, o en las salas de chat, fotologs o cualquier sitio donde **un desconocido puede acceder a información personal de otras personas,** evita dar detalles de la escuela o la facultad en la que estudias, del lugar donde trabajas y principalmente del lugar en el que vives. **Evita también poner a disposición de extraños, datos o fotos que brinden cualquier detalle relevante sobre tu persona,** por ejemplo, fotos en las que aparezca la fachada de su casa o la patente de tu automóvil. Nunca publiques tu número de teléfono a través de estos medios, tampoco informes el lugar en el que estará en las próximas horas, o el lugar que frecuentas. Si estos datos están dirigidos a tus amigos, envíalos de manera personal, pues toda y cualquier información relevante sobre ti, puede ser usada indebidamente por personas con malas intenciones.

## Cuidado al registrarte

Muchos sitios webs exigen que te registres para usar algunos de sus servicios, pero esto puede ser una trampa. Por ejemplo, **si un sitio web pide tu número de tarjeta de crédito sin ser una página de ventas, las posibilidades de que se trate de un engaño o una estafa son grandes.** Además, tu información personal puede ser entregada (vendida) a empresas que venden, por ejemplo, productos por teléfono. O peor aún, su e-mail puede ser agregado a listas de SPAMs.

Por eso, antes de registrarte en un sitio web **haz una búsqueda en internet para verificar si esta dirección está involucrada con alguna actividad ilegal.** Evalúa también si es estrictamente necesario registrarse.

## Para finalizar

A pesar de que protegerse en el "mundo virtual" puede ser un poco trabajoso, es muy importante para evitar trastornos mayores. **La mayor parte de los engaños puede ser evitada si el usuario está atento,** por eso es recomendable tener presente cada uno de los consejos mencionados en este artículo.