

Tecnomanía

Tips para navegar seguro

Navegar por Internet puede ser tan seguro como se imagina, existen varias circunstancias que ponen en peligro la privacidad, información y hasta dinero. En este artículo presentamos algunos tips que pueden ayudar a prevenirlos.

Acoso por Internet

Se presenta por medio de amenazas para perseguir a otra persona por Internet, ya sea por correos electrónicos o por mensajes en línea. Para evitarlo se recomienda borrar las identificaciones (antecedentes) que se hayan creado en cuartos de charla y sistemas de mensajes instantáneos, cambiar direcciones de correo electrónico o, en caso de ser necesario, contactar al proveedor de servicio de Internet.

Contraseñas

Los passwords o “contraseñas” son tan importantes como la llave de su casa. Los ciberpiratas o hackers son ladrones de contraseñas, por lo que es importante que éstas sean difíciles de descifrar. Una contraseña simple puede ser descubierta mediante un programa especializado en menos de una hora; en cambio, una contraseña difícil puede tardar de 10 a 20 años en ser descubierta.

Toma en cuenta las siguientes recomendaciones:

- *No utilizar como contraseña algunas palabras que se encuentre en un diccionario, incluso en cualquier idioma.
- *No utilizar palabras al revés.
- *No usar una palabra que pueda ser asociada con información personal, dirección, teléfono, fecha de nacimiento, nombre de la mascota, pasatiempo o deporte favorito.
- *No utilizar letras o números consecutivos, por ejemplo “abcdefg” o “123456”.
- *Tratar que sea lo más simple a efecto de que se pueda recordar.
- *Utilizar una combinación de letras, números y caracteres especiales en orden aleatorio.
- *Utilizar por lo menos 6 caracteres. Cuantos más sean, más difícil serán de descifrar.

Puntos de acceso público

Muchas personas no tienen la posibilidad de ingresar a Internet desde una computadora propia, y lo hacen desde lugares o puntos de acceso público (café Internet, bibliotecas, librerías, aeropuertos, etcétera). En estas circunstancias también hay que tomar precauciones para cuidar la información personal y navegar de manera segura por la red.

Algunas recomendaciones:

- *Estar siempre alerta de las personas que se encuentren o estén sentadas cerca, ya que podrían ver la información personal de pantalla.

*Eliminar la memoria “temporal” del navegador antes de retirarse del lugar de la siguiente manera: desplegar el menú de herramientas, seleccionar opciones de Internet, dar un clic en “eliminar archivos” y “borrar historial”.

*Esto ayudará a minimizar el riesgo de que alguien tenga acceso a la información personal.

*Cerrar todas las páginas utilizadas antes de dejar el lugar.

*Nunca permitir a la computadora recordar contraseñas.

*Nunca ingresar información privada o importante mientras te encuentras en un sitio de acceso público.

Spam

Son los “correos electrónicos chatarra”, es decir, correos electrónicos no solicitados y enviados de manera masiva. El contenido de éstos se relaciona con publicidad de bienes y servicios; algunas compañías pagan por enviar publicidad y circulares. Varios usuarios pagan el servicio de Internet por horas y es obvio que invertirán más tiempo al abrir estos correos, que pueden llegar a saturar los buzones. Por lo general, el spam es retransmitido de forma indiscriminada, anónima, encubierta y repetitiva. Además, las personas que envían spam (spammers) utilizan direcciones electrónicas que fueron recolectadas o vendidas sin previo consentimiento del usuario.

Se recomienda tener las siguientes precauciones para evitar este tipo de correo:

*Nunca responder a un correo spam, de lo contrario se confirmaría la dirección y sería un objetivo idóneo para futuros correos.

*No utilizar la cuenta de correo normal o privada para suscripciones, listas de correo o publicidad. Se recomienda crear una cuenta especial para estos fines.

*Nunca comprar algo que se anuncie a través de correos spam.

*Utilizar un filtro especial para estos correos. Generalmente, los servicios de correo cuentan con tal opción.

*Reportar a las empresas spammers en los sitios denominados antispam.

*Revisar detenidamente las políticas de privacidad al momento de abrir una cuenta de correo.

*No abrir los archivos anexos a correos spam.

Spywarey “Caballos de Troya”

Debemos tener cuidado con los programas ejecutables (aquellos que puedes recibir a través de correos electrónicos y cuya terminación es “.exe”), ya que existen algunos que utilizan tu computadora y realizan conexiones automáticas a otros sitios, enviando tu información personal sin autorización y sin conocimiento de ello. Los programas “troyanos” permiten a un ciberpirata acceder a toda tu computadora y manejar la información personal. Es recomendable tomar precauciones, como revisar la configuración de cookies e instalar “barreras”. También existen programas para detectar a los espías y ciberpiratas.

http://www.profeco.gob.mx/html/ecomercio/ecomercio_conceptos.htm