

10 pasos para mantenerte seguro en Internet



No podemos estresar lo suficiente la importancia de que protejas tus equipos de cómputo, gadgets y otros aparatos en donde tu información personal es administrada y almacenada, pues los delincuentes cibernéticos están al acecho en todo momento en la red (y la red es global y de alcances ilimitados). Protegerse de robos, ataques morales y personales, además de proteger a nuestros seres queridos es de gran importancia y seriedad.

¿Sabías que junio es considerado el mes de la Seguridad en Internet? Ya que este tema es muy importante debido a su implicaciones y a que es Jueves de Tecnología, te damos algunos pasos para asegurar que tu experiencia e Internet como principiante o incluso como experto, sea lo más segura posible.

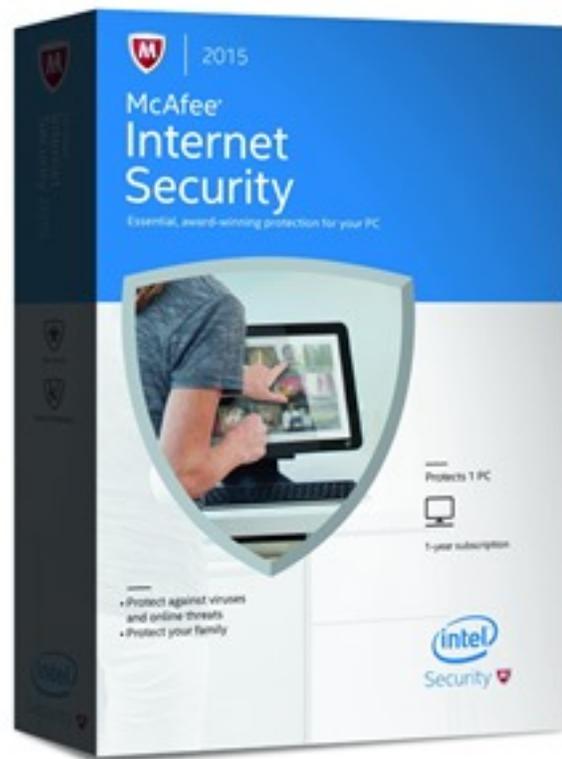


La seguridad es para todos. Todos aquellos que naveguen por la red, sea cual sea su edad, tienen que conocer las normas

básicas sobre la seguridad en Internet.

El lugar de la computadora importa. En un hogar con niños, se recomienda que lo coloque en una zona familiar con mucho movimiento para que pueda monitorearse el uso del Internet. Igualmente, deberás cuidar conectarte a una red privada en lugar de pública, así reducirás el riesgo de que tu conexión se interfiera.

Utiliza un antivirus o software de seguridad. Asegúrate de contar con uno con control parental o un software específico diseñado para proteger a los niños online, uno de seguridad para edificios y viviendas, particulares, para empresas, de seguridad wi-fi, que proteja el ordenador frente a virus, hackers y spyware, y que también filtre el contenido, las imágenes y los sitios



Web ofensivos, dependiendo de tus necesidades de seguridad. Como estudiante UDLAP, te ofrecemos un antivirus gratuito de McAfee. Consulta la información [aquí](#).

Comprueba. Asegúrate de que tu equipo dispone de las tres protecciones básicas siguientes: software antivirus, antispyware y un firewall. Además, éstas deberían complementarse con una protección antiphishing, para mayor tranquilidad, pues cada minuto se detectan 1.4 sitios nuevos de phishing.

*No olvides actualizar este software con regularidad.



Establece límites. Define los límites de tu uso de la red, ya sea si vives solo o acompañado. Es necesario establecer las áreas prohibidas y los sitios Web, foros y salas de chat que se pueden visitar y los que no, además de los archivos que pueden descargar; de este modo te será fácil bloquearlos en el explorador de tu elección para no preocuparte de abrirlos accidentalmente y descargar un programa malicioso.

Si tu computadora es utilizada por varias personas, te recomendamos tener distintas cuentas de usuario personalizadas para evitar problemas de seguridad. Asigna privilegios, sitios bloqueados, descargas permitidas y otras configuraciones a cada cuenta dependiendo de los usuarios para asegurarte de que tu equipo esté mejor protegido.

Es mejor bloquear el contenido malicioso antes de aparezca. Explora estas opciones para el software que utilizas.

Acuerda normas de seguridad generales para tu computadora, ya sea personal o compartida. Debes asegurarte de que:

- Los nombres de usuario no deben revelar la identidad real de la persona y no deben resultar provocativos (en tus dispositivos o cuentas de redes sociales, correo electrónico, etc.).
- Las contraseñas deben mantenerse en secreto. Consulta más información [aquí](#).
- Ajusta las condiciones de seguridad de tus navegadores.
- No debe darse información que pueda revelar la verdadera identidad de la persona.

- No deben colocarse en Internet fotografías ofensivas o inapropiadas que puedan revelar la identidad real de la persona (por ejemplo, el nombre de tu empresa o escuela en una camiseta) y si deseas hacerlo, asegúrate de que sólo las compartirás con familiares y amigos de confianza.
- No compartir información personal con extraños o desconocidos que se hayan conocido en la red y no quedar en persona con ellos.
- No abrir nunca archivos adjuntos procedentes de desconocidos.
- Recordar que la descarga gratuita de juegos, música, barras de herramientas animadas o de otros elementos puede exponer a tu equipo a programas malintencionados u otro software no deseado. Además en algunos casos, es un delito.
- Ten cuidado con tus búsquedas en Internet. La búsqueda segura significa tener suficientes elementos para protegerte mientras haces búsquedas en Internet. Recuerda que las páginas que protegen tu información de manera cifrada utilizan URLs que inician con “https://”. Toma en cuenta que en la red hay más de 700,000 sitios maliciosos.

*Ten siempre presente estas reglas al usar tu computadora. Si es necesario, anótalas y

colócalas cerca del ordenador para que todos puedan recordarlas.



Comprométete. Para que te mantengas seguro al navegar en Internet es importante que te comprometas a evitar los peligros conocidos e identificados que puedes tener al navegar, de esta forma podrás identificar el motivo por el cual tu

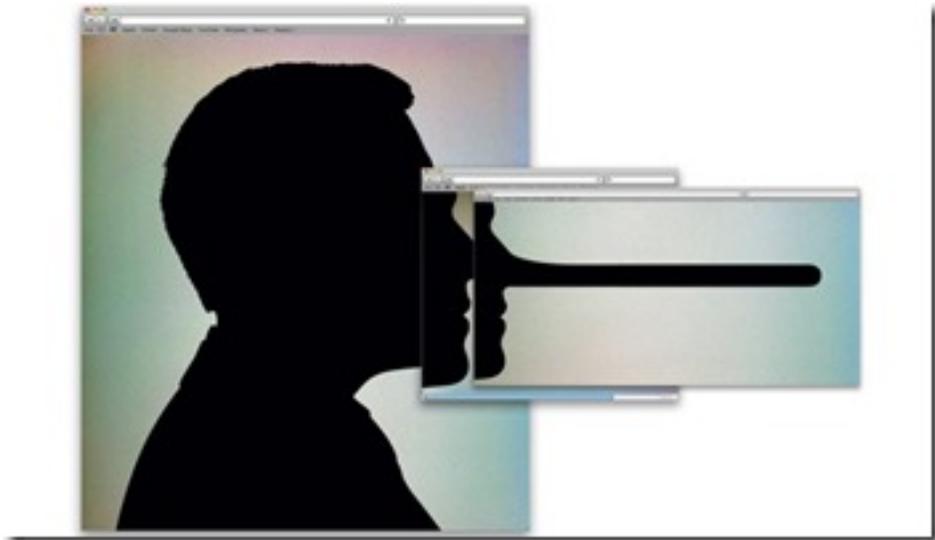
seguridad haya sido vulnerada. Si compartes tu ordenador con menores, es necesario que les reiteres que deben avisarle a un adulto en caso de que sientan que se encuentran en medio de una situación sospechosa en Internet (comunicación con un extraño, etc.).

Tómate tu tiempo. Dedicar el tiempo necesario a aprender el funcionamiento de los controles de tu equipo y utilizar las opciones para filtrar y bloquear material inadecuado. No

olvides tomar en cuenta que las amenazas pueden llegar desde algún hardware externo o gadget conectado a tu computadora (X-box, Play Station, Smartphone, tablet...); asegúrate también de mantenerlos seguros, o en caso de que aplique, activa restricciones de seguridad para menores en estos aparatos.

Utiliza además, un software que proteja tus dispositivos y su información del malware y los robos, mejorando así tu experiencia móvil con las funciones de búsqueda segura, búsqueda remota, bloqueo y borrado de historiales.

En Internet, mentir es más fácil. Toma en cuenta que mentir y fingir ser otra persona en redes sociales es mucho más fácil y peligroso si no conoces personalmente



a las personas con quienes tienes contacto en estos medios. Procura no comentar tu información básica y financiera con ellos.

Crea contraseñas a prueba de ataques. Para que una contraseña sea difícil de “descifrar” te recomendamos [estos pasos](#).

Mantente informado. El conocimiento es poder y cuanto más sepas, más seguro estarás. Actualízate constantemente sobre temas de seguridad en Internet y las novedades en softwares y técnicas de protección.

Recuerda que el Internet nos ofrece muchas cosas buenas y malas, todo dependerá de cómo lo uses para evitar ser víctima de crímenes electrónicos que pudieran afectarte en el mundo real.

Finalmente, para navegar seguro en Internet sigue las cuatro reglas de seguridad en cualquier situación: Sospecha, extrema precauciones, verifica los datos y utiliza protección específica.

¿Te sirvió esta información para tus actividades en la universidad, tu casa o empleo?
Déjanos saber lo que te gustaría conocer para facilitar tu vida universitaria y personal con ayuda de la tecnología.

*Con información de MaAfee.

Hasta el próximo jueves.