10 Tips de seguridad informática

1- **Cuidado con los adjuntos en tu correo**

Si no lo conoces, no lo abras. Con esa lógica de pensamiento, tendrías que quedarte a salvo durante mucho tiempo de los correos electrónicos de direcciones extrañas o que tienen archivos adjuntos como .pps, .zip, .exe, etc. Es mejor validar la procedencia de éstos.

2- **Actualiza el antivirus de tu sistema periódicamente**

Más reciente, más resistente. Pues es tan simple como pensar "si yo uso una aplicación que está desactualizada hace tres meses, llevo tres meses de vulnerabilidades no resueltas encima".

3- **Crea mejores contraseñas y cámbialas cada mes**

Más dificultad, menos previsibilidad. Un primer y obligado lugar es en tu campo de texto: "**introduzca una nueva contraseña**". Es que apelar a la misma contraseña de años para todos los servicios a los que estás suscrito es realmente un riesgo, pues si te descubren una; descubren todo.

4- **Usa antivirus y aplicaciones anti-malware**

No queremos héroes: usa Antivirus. El antivirus puede poner lento el equipo y utiliza recursos del sistema que te podrían dar algún dolor de cabeza. Pero, sopesando los riesgos, un antivirus activo es siempre más efectivo y seguro que un ordenador sin él.

5- **Acostumbra a cerrar las sesiones al terminar**

Una ventana de entrada es también una ventana de salida. El ser humano es curioso por naturaleza, y en cuanto ve algo que no es suyo puesto a su disposición, lo más probable es que, al menos por curiosidad, haga uso de ese regalo del devenir. Esto suele pasar en los cibercafés, en las oficinas de trabajo y en todos los sitios donde los ordenadores se comparten.

6- **Evita operaciones privadas en redes públicas**

Compartir la conexión, pero no los datos. Uno de los asuntos más complicados para muchos turistas es encontrarse de vacaciones y tener que realizar movimientos bancarios desde la red abierta de su hotel o desde algunas de las redes abiertas del lugar. Esto significa comodidad, pero también posibilidades para que el sniffing cobre forma y nos asalten las cuentas bancarias, sociales, de correo, etc. en un abrir y cerrar de ojos. Por eso, lo mejor es usar medios alternativos como servidores VPN o, más accesibles, extensiones como Blacksheep, acceder sólo a sitios con protocolo HTTPS y tener el firewall al máximo de atención.

7- **Verificar que esté activo el Firewall de tu sistema**

La Gran Muralla China no se construyó para decoración. Esta frase debería ser una invitación a que nos cuidemos más sin poner tantos caprichos a la hora de ser un poco cercenados en nuestra comodidad.

10 Tips de seguridad informática

8- **Evita software con recurrentes asociaciones a afecciones**

CanciónMuyLinda.exe no es un MP3: Debido a la cantidad de estafas que existen en relación a los servicios web, aplicaciones y lo que se les ocurra, tener una idea clara de qué programas no contribuyen a que tu ordenador sea un refugio de virus y malware. No puedes descargar software a tu equipo corporativo.

9- **Desconéctate de internet cuando no la necesites**

Menor grado de exposición, menor tasa de infección: Hay excepciones por montones, pero la mayor cantidad de infecciones se dan cuando los ordenadores están conectados a la red, pues los spywares y malware realizan sus acciones comunicándose con servidores o remitiendo información utilizando puertos abiertos en tu conexión. Por lo que si quieres bajar la tasa de posibilidades de infección y utilizas el ordenador mucho tiempo sin necesidad de una conexión a la red (juegos, diseño, escritura, etc) o si te vas a ir a dormir o si directamente vas a estar ausente, desconectando internet te evitas que algo pase en tu sistema sin apagar el ordenador. Simple, pero 100% efectivo.

10- **Realiza copias de seguridad (guardando los archivos abiertos cada 10 min y archivando el correo electrónico)**

Más vale prevenir que curar: En el caso de darse una situación donde pierdes datos por falta de políticas de seguridad en tu ordenador, por no llevar a cabo algo de todo lo que hemos contado arriba, la situación más común es la desesperación. Pero si serán importantes los backups o copias de seguridad, que cuando todos estarían inundándose en llanto, quien hizo la tarea y respaldó sus datos se lo tomará como una experiencia más.

Bonus: Educa a quienes comparten el ordenador contigo

Cuantos más sepan, menos se equivocan: Este punto tiene por objetivo dejar en claro que si bien puedes ser un paranoico de la seguridad del ordenador, cuando a este lo tenga en sus manos un inexperto, pocos de tus recursos cumplirán su función y el ordenador tendrá muchas posibilidades de infectarse. Para evitar esto, sobre todo para los que tienen un ordenador familiar o lo comparten en su trabajo, lo mejor es educar a quienes tengan contacto con ordenadores en general. Tanto los que comparten el tuyo como con tu entorno. Enseñándoles este artículo, contándoles tu propia experiencia, recomendándole software de seguridad e instruyéndolos en el arte de estar atento a la peligrosidad que existe cada vez que conectamos el cable de red al ordenador.

Cuidar nuestros sistemas es una obligación que los usuarios tenemos que asumir cuando los creadores del software o del sistema operativo han cometido errores, por lo que en última instancia la seguridad depende de nosotros.

Funte: http://www.abc.es