SDIGITALES

- Sistemas
- Software a Medida
- Soporte Corporativo
- Consultoría Informática

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

Conceptos importantes para su Seguridad

Lamentablemente, es cada vez mayor la cantidad de problemas generados por virus y malwares que tenemos que atender. Hemos recuperados discos, archivos borrados, particiones, documentos dañados, con el consiguiente costo y pérdida de tiempo. Peor aún, las infecciones se repiten, en muchos casos, por la modalidad de uso que se hace de Internet.

La mejor forma de prevenir este tipo de inconvenientes es teniendo todos los cuidados pertinentes al utilizar Internet. A continuación, les enumero los ítems que debe tener en cuenta para evitar problemas:

- No instale absolutamente ningún programa (desde internet) sin estar completamente seguro que es inofensivo. Busque en Google o consúltenos ante cualquier duda. Desconfié de programas gratuitos que se les ofrecen solos, a través de alguna ventana popup. Lo mismo puede decirse de juegos gratis, fondos de pantalla, protectores de pantalla, etc.
- Los programas P2P (Ares, Emule, etc.) en este momento son considerados todos INSEGUROS. Particularmente, en las PC's con Ares siempre se encuentran infecciones graves.
- No confíe plenamente en su antivirus. Por más actualizado que esté, seguirá siendo vulnerable a virus nuevos, o escondidos dentro de aplicaciones consideradas seguras.
- No confíe en antivirus gratuitos. Normalmente, no son demasiado efectivos. Gaste unos pesos, pero compre una solución segura. Se recomienda la línea de antivirus ESET.
- No instale barras de botones (toolbars), aun cuando las sugiera algún programa o página confiable. Habitualmente, si no contienen malware o virus, afectan a su navegador, haciéndolo mas lento. Por lo general, recaban información acerca de sus preferencias de navegación.
- Utilice algún navegador seguro, con bloqueador de Popups (Recomiendo el Maxthon o Firefox). Evite Google Chrome, dado que por su distribución viral es muy posible que tenga algún tipo de fin oculto (robo de información o monitoreo de navegación).
- Si algún sitio no es seguro, no insista en entrar. Las consecuencias siempre van a ser graves.
- Descargue archivos de sitios seguros. Si en esos sitios reciben comentarios de usuarios, espere a que los comentarios sean favorables antes de descargar algo. Evite aquellos sitios que sugieren “Downloaders” (programas que asisten a la instalación)
- Evite agregar contactos desconocidos a los mensajeros electrónicos.
- No envíe por correo electrónico cadenas, ni las continúe. En caso de hacerlo, por fuerza mayor, borre todas las direcciones de correo que contenga el mail, y coloque todos los destinatarios como CCO (Copia de Correo Oculta).
- Al enviar emails con archivos adjuntos, que en el cuerpo del correo quede bien claro que es lo que manda. De la misma manera, no abra archivos adjuntos si no tiene bien claro cuál es el contenido.
- Si envía fotos o documentos, asegúrese que tengan un tamaño adecuado, y que estén en un formato tal que el destinatario pueda abrirlo. El tamaño excesivo puede causar sobrecarga en los servidores de correo, y hasta puede ser bloqueada su cuenta.
- Nunca abra los links que se le envían por correo electrónico o mensajero sin estar completamente seguro del destino. Hay muchos virus y malware que entran en la PC por esa vía.
- Nunca envíe información confidencial, contraseñas, números de tarjeta de crédito u otros datos importantes por email o mensajero electrónico. Menos aún, por Hotmail. Gmail o servicios de correo gratuitos. Tampoco rellene formularios, ya sea por mail o web, donde se le solicite información de este tipo, salvo que esté completamente seguro del sitio o destinatario.

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

- Preferentemente, use correo POP3 de algún proveedor seguro. Descárguelo en su equipo, con algún cliente de correo (se sugiere Mozilla Thunderbird).
- Si utiliza el correo para fines comerciales, no dude reservar su propio dominio, y contratar un hosting seguro y confiable. De esa manera, pasará a ser propietario de sus cuentas de correo, tendrá pleno control sobre las mismas, y no dependerá de 3º o servicios gratuitos (que habitualmente imponen sus propias condiciones, arbirtrarias).
- Con respecto a las redes sociales, no envíe invitaciones masivas, ni acepte las que le indican. Muchas veces los correos de invitación son falsos, y apuntan a direcciones de descarga de virus o malware. Úselas con mucha precaución. Detrás de las redes sociales normalmente se esconden usuarios mal intencionados que distribuyen distinto tipo de malware a través de juegos y videos. En este aspecto, no es conveniente el acceso a estas redes desde equipos que sean usados con fines laborales. Esto se aplica particularmente a Facebook, dado que hemos encontrado muchísimos problemas en equipos que acceden con frecuencia a esta red.
- En caso de duda sobre alguna invitación a red social, o sobre el contenido de algún archivo adjunto, confírmelo con el contacto que lo envía, por email u otra vía, antes de aceptar el archivo o invitación.
- Evite el uso de Facebook en todos aquellos equipos que puedan almacenar información importante, o que estén conectados a alguna red en la que haya equipos con tal información. Dada la baja seguridad que posee, es normal que se infiltren, a través de Facebook, o sus aplicaciones, virus y malwares. El principal objetivo de estos es ROBAR INFORMACION. Normalmente, roban contraseñas de cuentas de correo y cuentas de home banking, y utilizan las direcciones de correo almacenadas en el equipo para distribuir SPAM (Correo basura)
- Busque información sobre Nettiquete, léala, y respétela.
- Consúltenos, por mail ante cualquier duda. Es más rápido y seguro preguntar qué desinfectar o recuperar (y obviamente, mucho más económico)

Rendimiento y Seguridad en los equipos

Últimamente, he visto una gran cantidad de equipos con problemas de rendimiento y seguridad causados por instalación de software inadecuado, o mal uso de las características de Windows. Esto se agrava muchísimo en el caso que el equipo corra algún sistema de gestión de información, sea accedido por documentos o programas a través de red, o almacene información importante. Por eso le recomiendo tener las siguientes precauciones:

- Instale siempre en su sistema una copia original de Windows. Evite las “distribuciones” modificadas, dado que siempre traen problemas.
- No instale software para alterar el aspecto de Windows, ni las herramientas del sistema del mismo (TaskSwitch, Vistamizer, etc.)
- Mantenga siempre actualizados los drivers del equipo.
- Mantenga su Windows siempre actualizado, con los parches de rendimiento y seguridad que indica Microsoft.
- **No almacene carpetas con documentos o archivos en el escritorio. Todos eso debe hacerse en la carpeta Mis Documentos, o en otra carpeta creada para tal fin, pero fuera del Escritorio**.
- Mantenga el estilo visual estándar del Windows. No use temas, ni protectores de pantalla, ni fotos de fondo de pantalla. En particular, algunas fotos, por su tamaño, pueden reducir muchísimo la velocidad del equipo. Tampoco instale programas para alterar el aspecto visual (por ejemplo, algunos que le dan el aspecto de Windows Vista o Windows 7 al XP)

Pueyrredón 935 - (2630) Firmat
Tel. 03465-420494
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar

- No instale programas adicionales para Messenger, Outlook, Facebook, u otras redes sociales. Habitualmente, contiene spyware, o consumen muchos recursos, enlenteciendo el equipo. (Por ejemplo, Messenger Plus, SweetIM, IncrediblMail, etc.).
- No instale Ares ni cualquier otro programa P2P. Normalmente, tienen troyanos, o problemas de seguridad graves que pueden afectar a su máquina.
- No instale, ni lo permita, barras de botones en el navegador de Internet. Habitualmente, contienen spyware. Verifique con frecuencia, y desinstale los que accidentalmente puedan haberse instalado.
- Evite instalar juegos on-line o que accedan a internet. Muchos contienen código malicioso, y son muy peligrosos.
- Realice con frecuencia un respaldo de sus datos, en Pendrive u otro medio extraíble.
- Realice mantenimientos periódicos a su equipo.
- Mantenga su Windows, y su software, permanentemente actualizado.
- No utilice versiones Beta de programas. Suelen generar problemas.