Soluciones Digitales

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

Pueyrredón 935 - (2630) Firmat
Tel.: 03465-420494 // Whatsapp: +54 9 3465 522230
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar
telegram: @aesantarelli skype: sdigitales

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.

En los últimos meses, los ataques con virus encriptadores (o ranson), agravan muchísimo la situación, dado que se presentan en gran cantidad de variantes, y normalmente desactivan los antivirus antes de actuar.

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:

- Sea desconfiado. No brinde información innecesaria en sitios web. Verifique que el sitio corresponda con su dominio o dirección.
- No instale absolutamente ningún programa (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. Solo descargue software de sitios confiables, seleccionando, preferencialmente, la página del desarrollador del programa a un sitio de shareware. 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), como Softonic.
- 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 complementos al navegador, aun cuando las sugiera algún programa o página confiable. Habitualmente, si no contienen malware o virus, afectan a su navegador, haciéndolo más lento. Por lo general, recaban información acerca de sus preferencias de navegación.
- Utilice algún navegador seguro, con bloqueador de ads, ventanas emergentes, y rastreo (Recomiendo Opera o Vivaldi). Evite Google Chrome, dado su alto grado de peligrosidad, generado por la posibilidad de instalación de complementos, y la gran cantidad de vulnerabilidades que tiene. El mismo problema de los complementos lo presentan Internet Explorer y Mozilla Firefox.
- Si algún sitio no es seguro, no insista en entrar. Las consecuencias siempre van a ser graves.
- Cuando un sitio sea de uso habitual (AFIP, Bancos, etc.), guarde su dirección en los Favoritos del Navegador, y acceda siempre al sitio a través de ese enlace. Evite la búsqueda de la dirección de estos sitios en buscadores, dado que muchas veces ocurre que los primeros resultados de las búsquedas dirigen la navegación a páginas inseguras, falsas, para robar la información de los usuarios.
- No envíe por correo electrónico cadenas, ni las continúe.
- En caso de necesitar enviar mails a varios contactos, coloque todos los destinatarios como CCO (Copia de Correo Oculta).
- En caso de necesitar reenviar un email que ya fue enviado a varios contactos, borre todas las direcciones de correos de los otros usuarios que han recibido el mail.

Pueyrredón 935 - (2630) Firmat
Tel.: 03465-420494 // Whatsapp: +54 9 3465 522230
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar
telegram: @aesantarelli skype: sdigitales

- 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.
- Evite el uso de webmails. Muchas veces, sus vulnerabilidades y bajo nivel de seguridad, sumado a las posibles vulnerabilidades de los navegadores (como ocurre en Google Chrome), pueden causar infecciones graves y perdida de información. Preferentemente, descargue sus correos a través de un cliente de correos (como Mozilla Thunderbird)
- 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.
- 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, arbitrarias).
- 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 con malas intenciones que distribuyen distinto tipo de malware a través de juegos, aplicaciones 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. Desconfíe de todo lo que vea en redes sociales.
- Recuerde que todo lo que publique en una red social es público (incluso, lo que se marca como privado, puede ser accedido o usado para perfilarlo)
- 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)
- Evite el uso de páginas con contenido activo para escuchar música. Muchas de estas páginas contienen código malicioso, que puede descargar virus o instalar complementos en su navegador. Además, consumen muchos recursos, tanto del equipo, como ancho de banda de la conexión a Internet. Particularmente, evite el escuchar música reproduciendo canales de video (como youtube), por el gran consumo de datos.
- Busque información sobre Nettiquete, léala, y respétela.
- Consúlteme, por mail ante cualquier duda. Es más rápido y seguro preguntar qué desinfectar o recuperar (y obviamente, mucho más económico)

Pueyrredón 935 - (2630) Firmat
Tel.: 03465-420494 // Whatsapp: +54 9 3465 522230
Web: http://www.sdigitales.com.ar
Email: informacion@sdigitales.com.ar
telegram: @aesantarelli skype: sdigitales

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.
- Instale una versión de Windows adecuada para su equipo. No actualice a una versión superior, solo porque el “técnico” se lo recomienda, o por seguir una publicidad. Es el camino más rápido a gastar U$S 600 en un nuevo equipo. (Habitualmente, este es el objetivo final del que hace la recomendación)
- Nunca permita que le formateen el equipo, sin la certeza de la necesidad absoluta.
- 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**. Esto afecta tanto la seguridad como el rendimiento y estabilidad de Windows. A su vez, la agrupación de documentos facilita su respaldo.
- 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
- 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, complementos o barras de botones en el navegador de Internet. Habitualmente, contienen spyware. Verifique con frecuencia, y desinstale los que accidentalmente puedan haberse instalado.
- Realice regularmente 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.