10 COSAS QUE NO DEBES HACER CON EL COMPUTADOR DE LA EMPRESA.

Abrir archivos o links sin precaución

No abras inmediatamente los archivos que recibes, ni sigas ciegamente los enlaces que te piden realizar acciones, así parezca que son conocidos los que te los envían, se más desconfiado si es algo que no te esperabas. Existe una técnica llamada suplantación de identidad (phishing), utilizada por muchos virus informáticos para distribuirse e infectar otros equipos, también es utilizada por estafadores cibernéticos haciéndose pasar por instituciones gubernamentales, bancarias o policiales que pudieran impresionarte. Ten presente que según las últimas encuestas el 70% de los ataques cibernéticos son a través del correo electrónico.

Usar contraseñas fáciles o que todos en la oficina las conozcan

El nombre del usuario y la contraseña en la red corporativa es algo privado, cámbialas con frecuencia. La mejor manera de proteger los documentos que usas a diario y por ende el trabajo realizado es colocándolos en un sitio seguro donde solo tú tengas acceso y tener respaldos. Son frecuentes los casos donde las personas pierden su información y no saben que paso, en ocasiones la información se encuentra en otro sitio porque alguien sin querer la movió de lugar, a veces nunca se encuentra; lo cual indica que alguien la borro quizás por error. También puede suceder que otras personas usen tu computador mientras no estás, teniendo acceso a información sensible cono sueldos y salarios, balances, correos electrónicos, etc.

Dejarte engañar por desconocidos

Cuidado con enlaces y archivos de desconocidos, no creas en todo lo que ves o lees en internet. Al realizar descargas de programas o documentos, antes de abrirlos, analízalos con un antivirus. Las instituciones gubernamentales como el Seniat, IVSS ni los bancos solicitan actualización de datos por correo electrónico o telefónicamente. Estas son técnicas utilizadas por personas inescrupulosas y es conocida con el nombre de ingeniería social.

Usar los pendrives sin cautela

El pendrive es ahora casi que un accesorio personal, de hecho varias marcas los han fusionado con sus productos, pulseras, relojes, dijes, etc. Por lo tanto es común que estos sean introducidos de computador en computador y a veces en sitios muy concurridos, como lo son los cibercafés y los laboratorios de computación de las instituciones de estudio, que a su vez son fuente de innumerables mutaciones de virus. Antes de abrir los archivos de tu pendrive revísalo con un antivirus.

Usar redes P2P

Las redes compañero a compañero (Peer to Peer), como Ares, Shareaza, e-mule y otras son medios utilizados por los criminales cibernéticos para infectar computadores. También los archivos que se descargan a través de ellas, películas, música, fotografías y programas pueden terminar llenando el disco duro de tu equipo o del servidor de la empresa. Es común encontrar en las empresas que un 80% del volumen de la información está compuesto por videos, fotografías personales y música descargada por el personal. Por otro lado si se hace común el uso de estas redes en la empresa la velocidad del Internet puede verse afectada notablemente.

Escuchar música en línea o mirar videos en línea

La música es muy agradable para muchas personas y gustan de realizar sus labores disfrutando de ella, los videos; por otro lado, ocupan dos de tus sentidos (Vista y oído), lo cual impide que realices tus labores. Que tu superior te encuentre viendo videos, es igual a que te encuentre leyendo el periódico. La situación se agrava cuando ese comportamiento lleva por el piso la velocidad del Internet, tu puedes estar en tu oficina disfrutando de tus videos en línea y en el departamento de administración en el piso de arriba la licenciada esta halándose los cabellos porque el archivo de la nómina no pasa al banco. Recuerda que este comportamiento puede estar siendo registrado.

Ser imprudente en la web

Toda navegación deja huella, siempre te pueden descubrir. Es importante que sepas que por ley los sistemas informáticos en el trabajo son solo para propósitos laborales y que todos los mensajes y archivos son propiedad de la compañía, además nadie tiene el derecho de esperar que sus comunicaciones o uso de los sistemas informáticos de la empresa sean privados. Tal como en el pasado se utilizaban mecanismos para controlar las llamadas telefónicas del personal, actualmente tu empresa puede tener mecanismos que le permitan determinar que páginas visitas y en que horario lo haces. Tampoco debes olvidar que en Internet hay peligros y que ir por caminos inadecuados puede traer virus o software espías a tu equipo y a la red corporativa.

Instalar programas innecesarios

Muchos programas durante su proceso de instalación, modifican las configuraciones del computador. Esto puede originar desde un molesto mensaje en pantalla, hasta que tu equipo quede fuera de la red. Programas para conectar tu celular, bonitos salvapantallas o programas gratuitos bajados de Internet son causantes de grandes problemas en los equipos de las organizaciones. Muchos programas supuestamente “Gratuitos” contienen software espía (Spyware), que pueden desde inundar tu correo electrónico con marketing hasta robar la contraseña que usas en tu banco, además de poner tu equipo extremadamente lento. Lo mejor antes de instalar programas es consultar con el profesional de tecnologías de información que asiste a tu empresa.

Divulgar datos personales o de conocidos

Al usar computadoras, no entregues informaciones personales, como número de tarjeta de crédito, nombre de usuario y contraseña de servicios y cosas por el estilo, ya sea por Messenger, correo o cualquier otro medio de comunicación online. Mantén dichas informaciones en sigilo en esos ambientes, a no ser que sea extremamente necesario. Tampoco divulgues información de hermanos ni amigos, ten en cuenta que con quien contactes puede o no ser verdaderamente quien te ha dicho que es.

Modificar la configuración de tu equipo

Quizás seas una persona con conocimientos avanzados en el uso de computadoras, eso suele suceder con frecuencia en tiempos actuales ya que mucha gente comenzó a usar pc´s a temprana edad. Sin embargo debes entender que tu equipo es solo la punta del iceberg, está conectado a una red que tiene muchos y sofisticados dispositivos que ofrecen diversos servicios a todas las personas que la usan, sin querer pudieras hasta provocar la caída de toda la red corporativa. Si te incomoda tu equipo es mejor consultar con el profesional que asiste a tu empresa.

MasterSoft de Venezuela, c.a.
Sistemas, Computación y Electrónica
RIF: J-30237543-6

Telfs: +58 251 2553121 - 2548305
Website: www.mastersoftweb.com
e-mail: contacto@mastersoftweb.com