CCOO Federación Servicios

NAVEGANT SEGURS

NAVEGANT SEGURS

Uns quants consells per a navegar segur i no perdre l'ordinador en l'intent

VISITANOS SI QUIERES ESTAR INFORMADO

SECCIÓN SINDICAL FRATERNIDAD MUPRESPA

El primer, és protegir amb contrasenya el

propi sistema operatiu i la BIOS si és possible. Ara per ara, quan XP campa a pler

entre els PC dels usuaris, això és més senzill, però en sistemes

tan populars (i encara usats) com Windows 98 o Em, resulta virtualment

impossible. També és necessari recordar que si no es posseeixen drets d'administrador

sobre la màquina, molt millor, així serà més complicat accedir per

error als punts més crítics del sistema.

Actualitzar el sistema.

Visitar

windowsupdate.com,
la pàgina que

automàticament entra en el nostre sistema, ho revisa, i ens diu què seria

convenient actualitzar, és recomanable cada cert temps. Està lluny de ser

la solució ideal, perquè resulta una violació de la intimitat i, la major part

de les vegades, els pegats no funcionen bé o desestabilitzen el sistema per complet

però, per a la majoria, és millor això que gens. Parchejar una

vulnerabilitat soluciona problemes de seguretat dels quals s'aprofiten els

virus, i això pot evitar que entrin nous, independentment de l'antivirus

actualitzat. Windows XP ve de sèrie amb el sistema d'actualitzacions

automàtiques. Jo recomano desactivar-lo, visitar la pàgina esmentada i elegir

manualment els pegats que ens afectin. I no només el sistema operatiu.

Actualitzar qualsevol programari pot evitar problemes de seguretat.

Elegir
bones
contrasenyes.

El nostre correu, el nostre sistema, les pàgines

que requereixen registre... solem usar les mateixes contrasenyes per a tot, i això

és un greu problema de seguretat. Devem canviar les nostres contrasenyes cada

tres mesos, evitar apuntar-les en papers, per descomptat no donar-se-les a ningú i

intentar imaginar claus complicades que combinin lletres i nombres. Gens

del nombre de telèfon, data de naixença...

Desactivar els serveis que no s'usin.

És necessari investigar un poc el nostre

sistema, i detenir tots els serveis que no estiguem usant. En alguns

sistemes pot estar activat el servidor de FTP, IIS... etc. Informar-se sobre

els serveis que presta l'ordinador i detenir-los, evita tenir els ports

oberts, que poden suposar potencials problemes de seguretat.

Evitar Internet Explorer i Outlook Express.

Van tenir la seva oportunitat, però aquests dos

programes ja han demostrat amb escreix que no són necessaris i cometen

massa errors de seguretat. Existeixen alternatives molt millors, més

funcionals, segures, i que consumeixen menys recursos. És molt important evitar

aquests dos programes a tota costa.

No fiar-se de res ni ningú.

Ni dels arxius que ens arriben per correu,

ni dels correus en si. No es deu executar gens la procedència dels quals resulti

remotament sospitosa, i menys encara de les pàgines que prometen grans

guanys o trucs que ningú coneix per a poder *hackear correus. NO existeixen les

fórmules màgiques, i és trista observar com molts dels neòfits en Internet,

el primer que busquen són les instruccions per a accedir a correus aliens.

Aviat acaben a pàgines que prometen una fórmula infalible en el qual, enviant

la teva pròpia contrasenya, es pot aconseguir qualsevol altra. Aquests ingenus pensen

que, encara havent-se incorporat tan tard al carro d'Internet, acaben de

descobrir poc menys que El Daurat i es llancen a les mans de persones sense

escrúpols, enviant-los els seus pròpies claus a l'espera de rebre les quals

realment desitgen robar.

També és molt comuna descarregar cracks,

pensant que sempre són útils. Es podria dir que un terç d'aquests

programes vénen amb algun regal intern, units amb sistemes de control

remot, o trojans que deixen la porta del teu ordinador oberta.

Antivirus i
Tallafocs
actualitzat.

L'antivirus és una mica que tot el món

instal·la, però que crea una falsa sensació de seguretat més preocupant que la

seguretat en si. Molts, a l'empara de la seva antivirus, executen el que els ve en

gana, sentint-se protegits, i obliden que els ports, els serveis oberts,

tot just són detectats per aquests programes (que l'hi recordin als infectats

per Blaster). Un firewall en condicions és el que completa a l'antivirus,

però també és necessari actualitzar-lo , no amb noves definicions de virus,

sinó observant atentament les seves regles i comprovant que realment està

complint el seu treball.

Xifrar la informació.

Existeixen programes que permeten xifrar les

dades importants, bé sigui convertint-les en un executable protegit amb

contrasenya, bé sigui dedicant una partició completa. Això resulta molt còmode.

Quan s'arrenca el sistema, es munta la partició després d'introduir una

contrasenya, així podem recuperar o guardar les dades. Quan decidim,

vam desmuntar el sistema i les dades queden xifrats. Així ningú pot llegir

les nostres dades i ens permet treballar amb ells de forma còmoda.

La missatgeria instantània.

És molt senzill enganyar a algú. Mentre es

té una conversa múltiple, canviant el nick per un d'algú en la pròpia conversa, no es pot saber exactament qui és qui. L'única forma d'identificar inequívocament a la persona amb la qual es parla és observant l'adreça de correu que apareix en la part superior de la finestra de la conversa, però si la conversa és múltiple, apareixeran diverses adreces de correu i resulta complicat associar adequadament cada direcció a la seva nick. Aquest senzill truc pot fer que algú que no és qui diu ser, enviï un arxiu, s'accepti i executi en el nostre sistema qualsevol virus, troja o cuc.

Còpies de seguretat.

Avui en dia tots els sistemes més o menys actuals vénen equipats amb una regrabadora de cd. Usem-la para una mica més que exercitar el nostre dret a la còpia privada d'obres musicals, emmagatzemant els nostres arxius importants, guardant una imatge del disc dur, per a poder lamentar menys les desgràcies que tard o d'hora, sempre ocorren i deixen inoperatiu el sistema. Mes val prevenir que guarir, i si el sistema operatiu es nega a funcionar o el disc dur és físicament danyat, sempre serà més fàcil acudir a la còpia de seguretat que buscar la hipotètica forma de recuperar el perdut.