

LA SEGURIDAD DEL USUARIO

Por: ZX80

Todos oímos casi a diario noticias sobre un nuevo virus que ha afectado miles de ordenadores en todo el mundo, ataques a telefonía móvil, hackers que se apoderan de ordenadores ajenos, robos de cuentas de e-mail, phishing... y la lista sigue creciendo.

La mayoría de las veces es culpa del propio usuario, y esto no sucedería si estuviera algo más informado sobre lo que es y lo que conlleva la seguridad. Precisamente de este echo se valen para conseguir sus logros. Este artículo intentará explicar básicamente los conceptos más usados y asegurar nuestros equipos al máximo. Constará de varias secciones:

- Protección del equipo frente al uso de personal no autorizado.
- Protección de ataques desde el exterior.
- Protección del malware (virus, troyanos, espías.)
- Actualizaciones de software y configuraciones por defecto.
- Protección referente a la web.
- Protección referente al e-mail.
- Seguridad en programas P2P.
- Protección ante nosotros mismos.
- Telefonía fija.
- Telefonía móvil.
- Consejos de última hora.

Protección del equipo frente al uso de personal no autorizado.

Normalmente nuestro ordenador solo lo utilizaremos nosotros, pero en el caso de que existan personas susceptibles de toquetear nuestras cosas (hermanos vengativos, compañeros de piso, padres estrictos, novio/a curioso/a...) el primer paso que debemos dar es proteger al cacharro con una contraseña nada más empezar y además evitar el arranque desde disquet o CD para evitarnos los trucos de escaqueo de dicha protección.

Esta protección se hace a través de BIOS, es decir, pulsando en la mayoría de ordenadores la tecla "SUPR." nada más encender el ordenador. De este modo entramos en el menú interno del Pc y en el apartado "*BIOS FEATURES SETUP*" o similar (dependiendo de marca de BIOS) y dentro de este menú seleccionar la opción "*SECURITY OPTION*", o en algunos casos "*PASSWORD CHECK*". Aquí podemos dejar 2 o 3 estados que son:

ALWAYS: Permite el uso de una contraseña justo después de haber arrancado, al mostrar la pantalla de comandos.

SETUP: Esta contraseña protege a la propia BIOS de acceder a ella, demandando que introduzcamos la contraseña correcta. Hay maneras de hacer que esta opción quede desactivada, pero es una opción a tener muy en cuenta y es la más utilizada.

DISABLED: Desactivamos toda contraseña de arranque.

¿Que contraseña elegir?

Las contraseñas a elegir en todos los casos (este y los que veremos en adelante) deben tener al menos 8 caracteres, alfanuméricos y alternando mayúsculas y minúsculas, siempre que el propio sistema lo permita, y huir de palabras que nos sean allegadas, como nuestro aniversario, nuestro nombre, el del perro....

Hay un manual al respecto en la dirección: <http://fentlinux.com/descargas/manuales/contraseñas.pdf>

Ruters y WIFI.

La conexión a internet no se produciría sin estos artefactos con luces que se encargan de gestionar el tráfico de datos de la red.

Es de vital importancia que estos aparatos estén correctamente configurados. En todos ellos (excepto en modems) se puede acceder dentro del ruter a través del navegador de internet, telnet o puerto serie, tecleando nuestra IP privada. Una vez dentro del ruter veremos una serie de menús en los que se nos da opción de activar un firewall, anular trafico de tipo ICMP o IGMP, bloquear rangos de IPs o IPs aisladas y también bloqueo de puertos.

Familiarizarse con esas opciones es vital para sacarle el máximo partido a nuestra seguridad. Muchos usuarios anulan los puertos relacionados con el P2P, otros bloquean el acceso a determinadas IPs que consideran peligrosas, otros andan en el silencio bloqueando el eco que se emite al recibir una petición. Entre la seguridad que ofrece el ruter y la seguridad del firewall en nuestro equipo tenemos más que suficiente para ahuyentar a los más osados atacantes.

Respecto al WIFI (Wireless Fidelity) o conexión inalámbrica, la cosa es más peliaguda, aunque no por ello más difícil.

En una red inalámbrica lo más importante es codificar al máximo la conexión mediante contraseña WEP (Wireles Equivalent Privacy). Se da así la opción de codificar a 32, 64 y 128 Ks y dentro de poco se podrá codificar a 256 Ks. Esto significa que cualquiera que esté rastreando redes no podrá conectarse porque el tráfico que detectará no le será conocido.

También deberemos esconder nuestro ESSID, es decir, nuestra identidad de red, ya que así evitamos un dato más que aporte pistas al atacante.

Luego tenemos el filtrado de MAC. Este bonito palabro no es más que una secuencia de números que identifica a cada tarjeta de red usada por los Pcs para la conexión. Si a nuestro ruter inalámbrico le damos solo una lista de nuestras MAC, evitaremos que otras MAC que no estén en la lista del ruter se puedan conectar.

Otra opción aconsejable es desactivar el Broadcasting, es decir, un envío a todos los Pcs cuando se hace un envío de datos, ya que así es fácil conectar a usuarios de diferentes redes o mediante sniffers, dar a conocer datos muy importantes.

Con estas medidas nos aseguramos de no tener cerca a ningún "chupoptero" aprovechándose de nuestra red.

Protección de ataques desde el exterior.

Actualmente es muy raro encontrar un ordenador que no tenga conexión a Internet (si es tu caso, sáltate este paso, aunque no está de más leerlo ;-)).

Es por eso que las infecciones y ataques actualmente son tan masivos, la red puede convertirse en un caldo de cultivo de víctimas objetivos de ataques de todo tipo, por eso lo mejor es protegerse ¿cómo?, pues mediante un *firewall*.

¿Eso que es lo que es ?, pues no es más que un programa que se encarga de permitir solo el uso de internet que nosotros le digamos, denegando todo lo demás.

Usando un símil, sería como un portero de discoteca. Si vas con bambas o camiseta no entras, si vas bien vestido te dejará pasar porque así se lo ha ordenado su jefe.

Hay varios tipos de firewall pero básicamente todos hacen la misma función. Suelen venir bastante bien configurados, pero no está de más echarle un ojo a las opciones por defecto.

Configúralo para que solo deje pasar lo que hemos pedido y lo que nos llegue sin haberlo pedido que no lo deje pasar. Y no está de más visitar de vez en cuando algún portal de seguridad para enterarnos de los puertos (entradas a la discoteca) que son susceptibles de ataques y decirle a nuestro portero que no deje pasar a nadie por esa puerta.

Algunos sitios para enterarnos de esto son:

<http://alerta-antivirus.red.es/portada/>

<http://seguridad.internautas.org/>

Los puertos más peligrosos:

Los puertos de un Pc son más de 65 mil, pero no os asustéis ya que solo unos pocos son perjudiciales.

En la siguiente lista pongo algunos de los puertos más usados y más peligrosos. No están todos los que son ni son todos los que están, pero anulando estos puertos en el firewall nos aseguramos en un 90% la seguridad de nuestro equipo (recordemos que la seguridad no es 100% óptima)

Lista de puertos de servidores:

- 20: Usado por servidores FTP en modo pasivo.
- 21: Usado por FTP para transferencia de ficheros.
- 22- SSH (Secure Shell) es un sistema de conexión cifrada entre Pcs.
- 23: Telnet, parecido al SSH pero sin cifrar, por lo que es muy inseguro.
- 25- SMTP o correo saliente, servidor de correo.
- 53: DNS, servidor de nombre de internet.
- 59: DCC, usado principalmente en programas de comunicación para transferir ficheros.
- 80: HTTP, para servidores web.
- 79: Finger Antigua fuente de información de usuarios en Internet y principal punto de ataque.
- 110: POP3, servidor para recepción de emails.

- 118: SQL, servidor de bases de datos.
- 143: El IMAP (Internet Message Access Protocol) es probablemente el puerto más escaneado después del 139 (NetBIOS). IMAP es un sistema relativamente nuevo, y dado que sus servidores no han tenido tiempo para madurar, este puerto abierto en tu sistema acapara gran atención para los intrusos.
- 194: IRC: servidor de chat.

Lista de puertos de sistema:

- 113: Servicio de Identificación/Autorización. Nunca debe estar abierto dado que es una fuente tremenda de escape de información.
- 135: RPC (Remote procedure call) Escritorio remoto de windows muy usado por los actuales virus.
- 137, 138 i 139: NETBIOS, ficheros compartidos de windows y usados por los más osados troyanos.
- 443: HTTPS, este puerto nos asegura transacciones por web cifradas. Muy usado para banca online, entre otros. Este puerto no debería estar abierto a menos que realmente lo estés utilizando para comercio seguro vía web.
- 445 Server Message Block. En Windows 2000, Microsoft añadió la posibilidad de ejecutar SMB directamente sobre TCP/IP sin la capa extra de NBT.
- 5000 El Universal Plug'n'Play es un protocolo de Microsoft para permitir a los PC's descubrir y controlar automáticamente un amplio rango de periféricos.

Lista de puertos de programas varios.

- 1080: Servicio de proxy.
- 4445: Chat.
- 4662: P2P (eMule, eDonkey...)
- 4672 UDP: P2P (eMule, eDonkey....)
- 5632: PcAnywhere: control remoto.
- 5900: VNC: control remoto.
- 6667, 6668, 6669 y 7000: Chat.
- 8080: Este puerto abierto puede permitir a otras personas utilizar tu ordenador para ocultar su IP real a los servidores web.
- 12345: Netbus: troyano de control remoto.
- 20001: Virus Millennium.
- 23456: Virus Evil FTP.
- 31337: Troyano Back Orifice de control remoto.
- 54320: Troyano Back Orifice 2000 de control remoto.
- 65000: Troyano Devil.

Para asegurarnos de que los puertos más importantes los tenemos cerrados podemos hacer uso de escaneadores on-line. Chequearán nuestro sistema y nos dirá los puertos "peligrosos" que tenemos abiertos y cerrados. Luego será tarea nuestra cerrar los que estuvieran abiertos.

Algunos programas de este tipos son:

<http://www.upseros.com/portscan.php>

<https://www.grc.com/x/ne.dll?bh0bkyd2>

Protección del malware (virus, troyanos, espías.).

Otro tema que preocupa mucho a los usuarios, el tema de los virus, troyanos y demás bichos raros que nos hacen la vida imposible. Hay que distinguir entre unos y otros, ya que aunque todos están dentro de la categoría del "*Malware*" no son lo mismo:

- **Virus:** Pues como su nombre indica, es un programa que se introduce en nuestro ordenador, y como si de un cuerpo se tratara, se pone "malo", dejando de hacer las funciones propias de ordenador, volviéndose lento, borrando información y sobre todo, contagiando a otros ordenadores.

- **Gusanos:** Se puede considerar un virus, aunque su propósito no es hacer daño a nuestro Pc, sino usarlo para su propio fin, que es expandirse por toda la red, por lo que no le interesa que el "anfitrión" (el Pc) se ponga malo (sería como la Tenia o Solitaria que habita en los intestinos de animales y humanos).

- **Troyanos:** Como pasó con el Caballo de Troya que usaron los Griegos para adentrarse en la ciudad de Troya, son programas de todo tipo, como animaciones cortas, programillas simples de texto o cualquier otra cosa que nos pueda llamar la atención y lo ejecutemos. Pero en verdad, aparte de dicho programa, va otro que se filtra en la máquina y que actúa en silencio, sin que el usuario sepa que está. Estos programas se usan para captar datos que luego se mandan por correo al creador del troyano, para abrir una puerta por donde poder entrar a nuestro Pc, recibir datos para almacenarlos...

Dentro de esta sección podemos mencionar las bombas lógicas, programas que están diseñados para que a cierta hora de cierto día empiecen a mandar información a una dirección. El ordenador infectado se le suele llamar Zombie y en conjunción con decenas o incluso centenares de Pcs igualmente infectados provocan DoS (denegación de servicio) a otros ordenadores más importantes para saturarlos y dejar vía libre a los atacantes.

- **Spyware o espías:** Estos programas se pueden considerar troyanos, ya que acompañan a otros programas de utilidad y actúan sin que nosotros sepamos que están, pero la intención de estos programas son los de ver a que webs accedemos para crear un perfil de usuario que se venderá a muy buen precio a empresas, ver si tenemos software original, etc...

Para este tipo de programas tenemos los antivirus, que se instalan en el ordenador y están a la escucha de todo lo que entra y lo revisa para verificar que está libre de "*bichos*". Pero no basta con instalarlo y listo, hay que actualizarlo sino a diario, si al menos una o dos veces a la semana, (muchos antivirus lo hacen automáticamente), ya que los virus, aparte de salir nuevos cada día, tienen la particularidad de mutar, convirtiéndose en otros, con capacidades que antes no tenían y la capacidad de esconderse de un antivirus que no está actualizado.

Hay que tener en cuenta que los antivirus también se infectan, por lo que un buen chequeo pasa por arrancar desde un sistema totalmente limpio y ajeno al sistema principal. Esto se hace con los disquets de arranque que el propio antivirus da opción a crear (y que la mayoría de usuarios no hace), incluso desde un arranque desde CD, en modo MS-DOS o distribución Live, y hacer el chequeo a conciencia desde ahí, tarde lo que tarde.

Para el mundo de los troyanos hay programas que los conocen y solo con un simple chequeo nos dirá si tenemos alguno. Además están a la escucha y en cuanto un programa que ejecutamos se desdobra, lo "encierra" evitando su funcionamiento y nos avisa.

Para el tema de los espías más de lo mismo. Existen programas limpiadores que chequean los programas instalados y eliminan dichos espías. Es bueno ir chequeando el sistema de vez en cuando.

Actualizaciones de software y configuraciones por defecto.

Al igual que pasa con los antivirus, los programas no basta con instalarlos y ya está, sobre todo los dedicados a nuestra seguridad. Van saliendo versiones cada cierto tiempo que implementan mejoras a nivel de estabilidad, seguridad y mejora de las propias opciones para las que fue diseñado el programa, por lo que conviene ir actualizando los programas a versiones más modernas y seguras.

¿Hay que actualizar siempre? Pues va a ser que no. Actualizar no siempre es sinónimo de mejoría. Muchas veces los programas se actualizan por un problema con algún tipo de hardware que nosotros no tenemos o implementan opciones que nosotros no usaremos nunca, por lo que en estos casos no es necesario actualizar. Otras veces se actualiza porque el programa, a algunos usuarios, les iba mal, pero si no fuera nuestro caso, no deberíamos tampoco de actualizarlo. En la web del programa suele venir una lista de mejoras de cada nueva versión, así sabremos si nos interesa cambiar o no.

En definitiva, es recomendable hacerlo cuando hayan problemas de seguridad o por mal funcionamiento del mismo.

Mención especial requiere la configuración que los programas traen por defecto. Para que sean lo más compatibles posible con la gran cantidad de usuarios, vienen preconfigurados con muchas opciones activas que los hacen algo inseguros. Por ejemplo, hay programas para navegar por internet que traen activadas opciones de carga de todo tipo de ficheros que lo demanden, o traen deshabilitadas opciones de bloqueo de publicidad o similares, que pueden ser aprovechadas por programadores de webs para la introducción de virus o troyanos en esas ventanas de publicidad.

No está de más echar una ojeada a los programas y configurarlos a nuestras necesidades para evitarnos sustos desagradables.

Protección referente a la web.

Cuando navegamos por internet, estamos mandando y recibiendo muchos datos. Estos datos que recibimos se traducen en ejecuciones de código para la traducción a un sistema que nosotros podamos entender, pero también esos datos nos envían peticiones de ejecución que nos pasan inadvertidas porque el navegador lo permite. Esto es muy inseguro, ya que la ejecución de código desconocido de cualquier web puede ser de tipo maligno, buscando el ansiado acceso a nuestro ordenador por parte de un atacante, virus, etc....

Es muy recomendable usar navegadores que NO permitan la ejecución de código sin nuestro permiso.

Asimismo es aconsejable por nuestra propia comodidad usar programas que eviten la apertura de ventanas adjuntas, usadas por los banners de publicidad, enlaces a múltiples webs "amigas", etc.

Existen muchos navegadores que son muy flexibles y permiten todas esas opciones y otras muy interesantes.

Tampoco es aconsejable marcar la opción "*Recordar contraseña*" que muchos sites nos dan a elegir, ya que estas contraseñas quedan almacenadas en nuestro Pc y se puede acceder a ellas y extraer de una manera relativamente fácil. También es bueno revisar y borrar todas las "*cookies*" que no necesitemos. Estas cookies

son archivos de texto con información de usuario que la web que la ha creado leerá siempre que nos conectemos, para que nos conozca (es el caso de foros, webs que requieren registro, etc).

Phishing.

¿Pescando?, pues es una buena traducción, ya que son muchos los que han sido "pescados" en este engaño.

Se trata de crear una web exactamente igual a la original, que suelen ser de temas bancarios, recargas de móvil, es decir, cualquier web que mueva dinero. De esta forma crearemos que estamos en nuestra web del banco y las transacciones que haremos quedarán en manos de los malos.

Si tu entras en, por ejemplo, "La Caixa.es", para hacer unos trámites, te pedirán todos los datos bancarios y tu se los darás, porque la web es tan fiel que no parece falsa. Una vez tengan todos tus datos dará un error de cualquier tipo como que el servidor está saturado, o que el servicio está desactivado por actualizaciones... como excusa para no realizar el trámite (ya que al ser imitación veríamos el fraude), de forma que tu transacción nunca se efectúa, pero en cambio ellos ya tienen tus datos y te pueden limpiar tu cuenta corriente.

Darse cuenta de esto es relativamente fácil, ya que la dirección web los delata. En el ejemplo de La Caixa la dirección sería <http://www.lacaixa.es> pero en cambio la web phishing sería del estilo <http://www.lacaixa.es.tk> por poner un ejemplo, cosa que nos haría sospechar.

Protección referente al e-mail.

Lo mismo que para el caso anterior sirven los consejos para el correo electrónico.

Los programas que ejecutan código a nuestras espaldas no son aconsejables, por lo que debemos cambiar a programas que no lo permitan, e incluso son recomendables los clientes de correo que permiten leer los correos en "*texto plano*", es decir, traducen a código ASCII los contenidos de los correos. Esto nos evita la ejecución de código maligno o los adjuntos de direcciones web de dudosa procedencia y que el usuario se empeña siempre en pulsar, aunque no las conozca.

Es aconsejable también activar filtros o instalar programas para evitar el correo basura o "*Spam*" que nos llenan la bandeja de entrada de correos que no hemos solicitado de diversos temas como casinos en línea, venta de productos, concursos que aparentemente hemos ganado, etc.

Nunca hemos de abrir correos del que no conozcamos su remitente o procedencia, y en general, borrar los correos que consideremos sospechosos aunque provengan de gente conocida. Si nos lo ha mandado algún amigo nos lo podrá volver a enviar si le decimos que lo borramos por error, aunque algunas veces nos dirán que no nos mandaron nada (Touché).

Hay que pensar que ni Microsoft, ni nuestro banco, ni empresas en general nos enviarán correos avisándonos de nada o pidiéndonos datos personales, así que eliminaremos inmediatamente dichos correos sin llegar a abrirlos porque pertenecen al phishing y sobre todo, no abrir ningún tipo de adjunto sin antes pasarlo por el antivirus.

Y para los más paranoicos, ¿que tal si ciframos los correos?. Existen programas como el PGP que traducen los correos a un galimatías ininteligible, así nos aseguramos de que si nos interceptan el correo no podrán entender nada de lo que pone, ya que solo el destinatario, con una contraseña adecuada, podrá leerlo.

Seguridad en programas P2P.

Los programas Peer to Peer (P2P) como eMule, Overnet, eDonkey... nos permiten encontrar material que está descatalogado y compartir nuestros archivos con los demás. Precisamente esta compartición es lo que hace que dichos programas sean algo inseguros. Hago referencia de nuevo al apartado de la configuración por defecto, ya que estos programas vienen preconfigurados por defecto para conexiones al puerto 4662 TCP y 4672 UDP. Cualquier atacante podrá lanzar un ataque a esos puertos y casi seguro que algún alma en pena encontrará para putearlo un poco.

Es recomendable pues elegir otros puertos, lo más elevado posible, para que se cansen de rastrear.

Este tipo de programas suelen dar mucha información de los usuarios que hay conectados y además suelen dejar un rastro muy evidente de nuestras conexiones, por lo que hay una llamada "*lista negra*" de Ips o direcciones de servidores que en verdad son robots que se dedican a recopilar datos nuestros. Esta lista va en un archivo normalmente llamado ipfilter.dat y que se deja en el directorio del programa que usemos y él solito se encarga de cargarlo y filtrar dichas IPs.

Otra opción consiste en socksificar las conexiones o anonimizarlas, pero no todos los programas soportan o traen esta opción. Parece ser que las próximas versiones traerán ocultación de datos personales, un logro en la seguridad, sin duda.

Protección ante nosotros mismos.

Como decía al principio de este artículo, los peores enemigos de la seguridad somos nosotros mismos. Por culpa de nuestra dejadez o desconocimiento se producen la mayoría de problemas relacionados con la seguridad.

Ante el desconocimiento, poco se puede hacer, aparte de leer y documentarse un poco de las novedades en el tema, pero ante la dejadez sí que hay muuuucho que podemos hacer para, al menos, minimizar los daños.

Vamos a ver algunas acciones que están en nuestra mano:

- **Orden:** Hay por ahí discos duros que parecen auténticos basureros. Debemos acostumbrarnos a tener todo ordenado para luego poder identificar a simple vista las carpetas que tenemos y el contenido en ellas. Lo normal es tener una carpeta o directorio donde pondremos nuestros archivos personales, ordenándolos en subdirectorios como fotos, textos, mp3, trabajos.... Esto nos servirá para el siguiente apartado, entre otras cosas.
- **Copias de respaldo secuenciales:** Es muy aconsejable ir haciendo periódicamente copias de nuestros datos personales, como agendas, textos, trabajos, fotos... previamente revisado mediante antivirus.
- **Copias de seguridad del sistema:** Es buena idea una vez recién instalado el sistema operativo, los drivers, los programas de uso diario y echa la configuración, crear una imagen del sistema, la cual nos permitirá restaurarla en pocos minutos en caso de tener problemas con el sistema, y nos evitamos así la pérdida de tiempo que se invierte en volver a dejarlo todo como estaba.
- **Uso correcto de contraseñas:** Como decíamos anteriormente, es mejor poner una contraseña larga y rara que una corta y allegada a nosotros, y por supuesto no usar la misma en todos los sitios porque si nos la

averiguan la probarán en todos los apartados y... Voilà.. acceso total.

No usar la misma contraseña que el nombre de cuenta o login, no guardarlas para recordarlas más tarde...

- **No seamos "Exeros":** Un exero es aquella persona que ejecuta todo programa que cae en sus manos. Evitemos la tentación de hacer "click" en ese programita que nos han dejado, enviado por mail, pirateado (ejem...). Pensemos en todo lo visto hasta ahora y decidamos entonces que hacemos (eliminación por procedencia dudosa, escaneo de malware en general...)
- **Evitemos en lo posible la comodidad que nos da un sistema:** Parece una contradicción, pero esa comodidad se consigue sacrificando la seguridad.

Telefonía fija.

Mucho se ha escrito sobre el tema y muy solucionado están los problemas que se derivan de la telefonía fija, pero aun así aun hay gente que se las idea para engañar al personal.

Hay un fraude que ni la propia telefónica sabe como parar. Se trata de una llamada recibida al domicilio en el que se dice ser un técnico de la telefónica haciendo funciones de revisión de la linea (nunca te llamarán por teléfono para chequear las lineas, lo harán sin avisar o mandarán un técnico debidamente identificado).

Bien, el supuesto técnico nos pregunta si el teléfono al que llama dispone de "marcación por tonos" y, si es así, pide a su interlocutor que marque el noventa, le dice que todo está en orden y se despide.

De esta forma nosotros mismos hemos convertido la línea de teléfono en emisora de todas las llamadas que se hagan desde el teléfono del que esa persona había telefoneado y, por tanto, las llamadas que el "técnico" haga nos serán cobradas a nosotros.

Otro timo es el de la oficina de Hacienda, INEM, ayuntamiento, etc. Recibimos una llamada de un número cualquiera de una supuesta oficina importante y nos dicen que tienen algo de interés para nosotros, pero que en ese momento les llaman por la otra línea, o tienen cualquier problema. Nos dan un teléfono para que llamemos en 5 minutos, número al que nosotros llamamos porque nos interesa y que al llamar nos dicen que esperemos un momento. El momento se convierte en minutos que estamos pagando nosotros a un teléfono de tarificación especial.

El tema de los Domos es otra de las cosas que nos hacen más cómoda la vida, pero a veces esa comodidad no es tan buena como creemos. Viendo quien llama podemos o no coger la llamada, pues ¿porque no anonimizamos la llamada?

Es tan simple como marcar el 067 antes del número a marcar y nuestro número no lo verá nadie. En el caso de los móviles, el código varía, siendo #31#

OJO: Esto no funciona con centralitas ni con la policía ;-)

Telefonía móvil.

Llegamos a un apartado que está también muy dejado por parte del usuario y que está dando mucho que hablar.

Están empezando a aparecer los primeros virus que se aprovechan de tecnologías como el Java o el Bluetooth

para producir el mayor daño posible, como borrado de la agenda, consumo de la batería, contagio a otros usuarios...

Los consejos aquí son más escasos, pero sirve más o menos todo lo visto hasta ahora: No fiarse de desconocidos, no abrir cosas de las que dudemos su procedencia, no dejarnos engañar con premios para que llamemos a ciertos números o para que nos conectemos a ciertas webs o descargemos ciertos programas...

Debemos dejar desactivado en todo momento las conexiones IR y Bluetooth y solo activarlo cuando vayamos a usarlo y, si el terminal lo permite, evitar conexiones externas, solo permitir las conexiones que nosotros demandemos.

Y no está de más ir visitando webs oficiales de seguridad en las que puntualmente nos informan sobre nuevos virus o engaños.

Y una noticia que cuando menos, impacta, es la creación por parte de la compañía F-Secure (creadora del famoso antivirus F-Prot) de un antivirus para móviles, llamado *F-Secure Mobile Antivirus*.

Como siempre, recomendable seguir la noticia y descargarlo cuando esté listo ;-)

Consejos de última hora.

Hay ciertas formas de actuar que no son aconsejables en absoluto, como por ejemplo:

- Mostrar mensajes descriptivos de errores: Esto lo que hace es abreviar un posible error de carga. Esta abreviación es para muchos de estos errores la misma, por lo que nunca sabremos exactamente por qué ha fallado.
- Esconder las extensiones de los programas: La peor opción que he podido ver. Si no vemos las extensiones de los archivos nos la pueden dar con queso. Es el caso de los conocidos "*falsos exe*", que son archivos escritos en Visual Basic pero que al tener 2 extensiones (programa.exe.vbs) solo mostrará la primera (programa.exe) y engañarnos de la naturaleza del archivo. La ejecución de este tipo de archivos es fatal.
- No mostrar archivos ocultos o del sistema: Visto todo lo anterior no es muy lógica esta opción, sabiendo que un malware intentará ocultarse para que no veamos su rastro.
- Ojo con los archivos de tamaño cero (0): Estos archivos son indicadores de algún tipo de malware (keyloggers normalmente), ya que está a la espera de llenarse con datos que probablemente enviará después a su creador.
Eso si, no todos los archivos de tamaño cero son malignos. Si algún programa "limpio" que hemos instalado en un sistema regularmente chequeado y sano nos pone un archivo de tamaño cero, probablemente será para su propio uso, pero no está de más desconfiar.

Espero que este documento sea de ayuda, al menos, para cambiar la forma de pensar de los usuarios y recordarles que en la red hay una fauna hambrienta de usuarios desprotegidos. Que no te pillen a ti ;-)

Fecha de creación: 8 Septiembre 2005

Liberada bajo licencia



<http://creativecommons.org/licenses/by-nc-sa/2.5/>