Barcelona Activa
Cibernàrium

Navega amb seguretat

Barcelonactiva

Ajuntament de Barcelona

Navega amb seguretat

1. **Còpies de seguretat**
2. **Les contrasenyes i la creació d'usuaris**
3. **Els virus**
4. **Els antivirus**
5. **Tipus d'antivirus**
6. **Com configurar el nostre navegador**
7. **El *Firewall* o tallafocs**
8. **Els *Spyware* o troians**
9. **L'*spam* i el correu electrònic**
10. **Bones pràctiques de seguretat**

La seguretat és conjunt de mètodes i mitjans de protecció que ens permeten viure en un ambient de confiança en la nostra comunitat, societat o país i mantenir-nos lliures de perills. De la mateixa manera que en la vida quotidiana procurem sentir-nos segurs, pel que fa a l'ordinador també és necessari recórrer a un conjunt de mètodes de protecció perquè tan l'ús que li donem com la navegació per Internet siguin el més segurs possible.

Regularment, les amenaces a la seguretat de l'ordinador i a la informació que conté, estan relacionades principalment amb l'incompliment de certes mesures de seguretat bàsiques com les següents:

- El mal ús de claus d'accés i contrasenyes com, per exemple, respondre "*sí*" quan ens pregunten si volem guardar la nostra contrasenya en un ordinador.
- No utilitzar les eines de seguretat que ens proporciona el sistema operatiu o els programes que ens permeten navegar per Internet.
- No tenir còpies de seguretat de la informació.
- No fer servir correctament un antivirus, un *antispyware* (anti-programes espia) o un *antispam* (anti-enviaments de correus no sol·licitats).

Parlem de seguretat però, de què hem de protegir al nostre ordinador?

- De la modificació, destrucció i obtenció d'informació que conté el nostre ordinador, provocada per terceres persones, virus, *spyware* (programes espia), entre d'altres (sobre els quals parlarem més endavant).
- De falles en processos, emmagatzematge o transmissió de la informació, que poden passar quan, per exemple, reenviem de forma accidental un missatge amb virus o quan obrim arxius adjunts a un correu electrònic sense verificar abans si té virus.

És important saber que aquests errors poden produir-se de forma accidental o intencionada. Per evitar-los, a continuació mostrarem una sèrie de mesures preventives que ens donaran tranquil·litat quan utilitzem el nostre ordinador i naveguem per Internet.

1. Còpies de seguretat

Les còpies de seguretat del sistema són, amb freqüència, l'únic mecanisme de recuperació que tenen els administradors per restaurar una màquina que per qualsevol motiu -no sempre s'ha de tractar d'un virus- ha perdut dades. Cal tenir còpies de seguretat tant dels programes instal·lats com dels arxius que hem anat guardant.

Hi ha múltiples suports on guardar les còpies de seguretat:

- **El disc dur.** És possible utilitzar una unitat de disc dur completa (o una partició, és a dir, una part del mateix) per realitzar còpies de seguretat. Es pot crear un sistema de fitxers sobre la unitat i copiar-hi els fitxers que ens interessi guardar (o recuperar). Sempre es recomana fer una còpia de seguretat de tot el disc dur. Per això disposem d'un assistent per còpia de seguretat o restauració en el sistema operatiu Windows. Només hem de seguir les instruccions que van donant els diferents quadres de diàleg, seleccionar les opcions de preferència i fer clic en "següent". El problema d'aquest sistema és que la còpia de

seguretat s'emmagatzema en el mateix ordinador i en cas que entrés un virus, aquest pot atacar també la còpia de seguretat.

- **El CD-ROM.** Avui dia, la majoria dels ordinadors disposen d'unitats gravadores de CD-ROM i DVD, amb una capacitat d'emmagatzematge de 650 MB en un CD-ROM i de 4.7 Gb en un DVD. Aquests addicionalment poden ser reescrivibles i utilitzar-se diversos cops.

- **El *Pen Drive* (o llapis USB o llapis de memòria).** És un petit dispositiu d'emmagatzematge USB de la grandària d'un clauer que pot ser de diferents capacitats.

- **Els *discos* externs: són unitats d'emmagatzematge** de gran capacitat que són la millor opció per mantenir grans quantitats d'informació emmagatzemada. És un disc dur transportable que es connecta amb USB 2.0, 3.0 o Bluetooth. Les seves capacitats van des dels 2 GB dels microdiscs a centenars de GB (Terabytes). Són compatibles amb tots els ordinadors actuals.

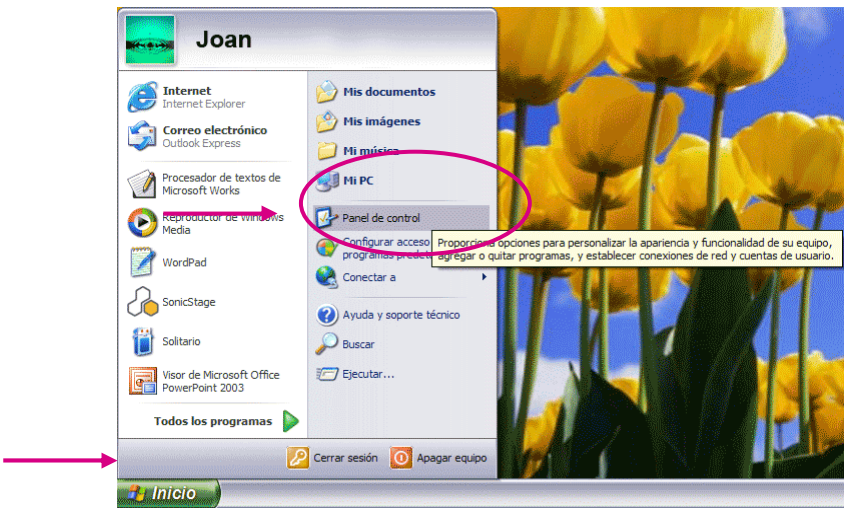
2. Les contrasenyes i la creació d'usuaris

Les **contrasenyes** són claus secretes i formen part de la nostra vida diària. Per exemple, quan obrim un compte bancari ens donen una llibreta o targeta, amb una contrasenya que ens permet retirar diners d'un caixer automàtic de manera segura.

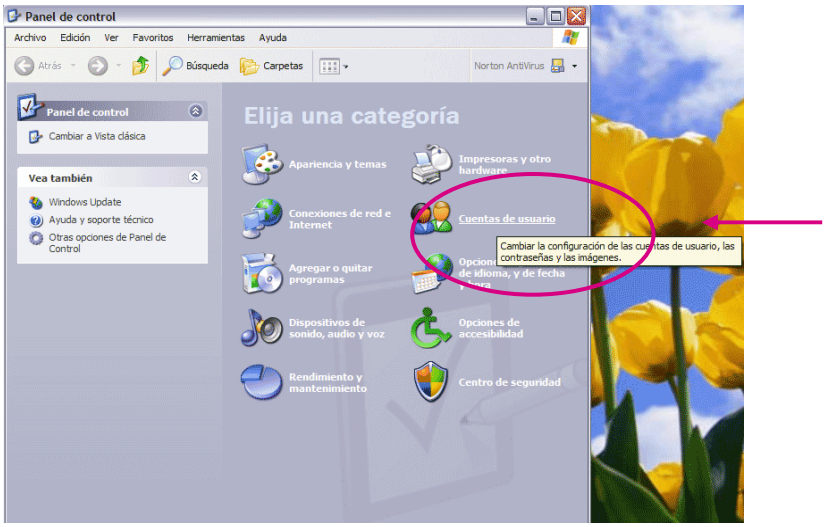
En el cas del nostre ordinador, una clau o contrasenya ens ajuda a controlar les persones que l'utilitzen, ja sigui a casa o a la feina. Però perquè la creació de contrasenyes realment tingui utilitat recomanem crear **comptes d'usuari** diferents. Així les diferents persones que utilitzen el mateix ordinador (com altres membres de la família o els companys de feina) entren amb la seva clau personal, disposen d'espai propi i poden treballar sense el risc d'esborrar o modificar informació important per al altres usuaris.

Per crear un compte d'usuari hem de fer el següent:

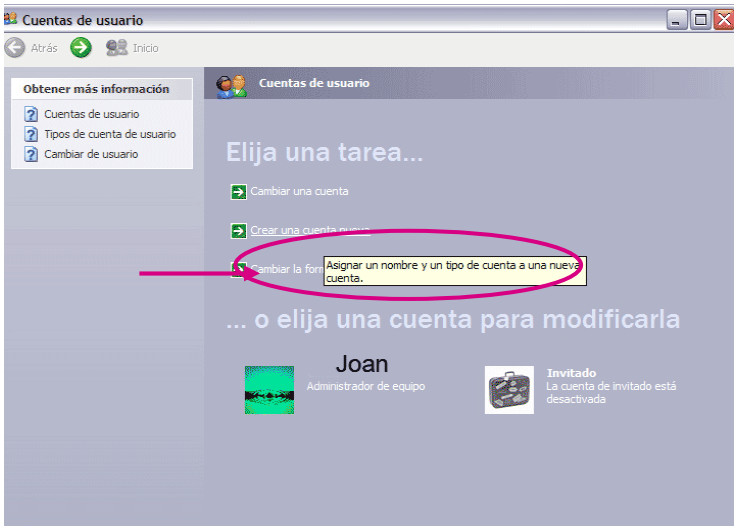
PAS 1. Anar a inici i fer clic al **panell de control**.



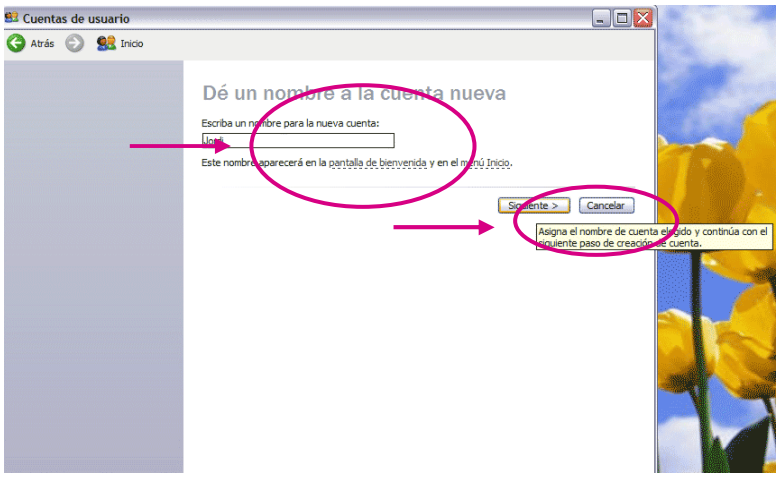
PAS 2. Anar a **comptes d'usuari** i fer clic.



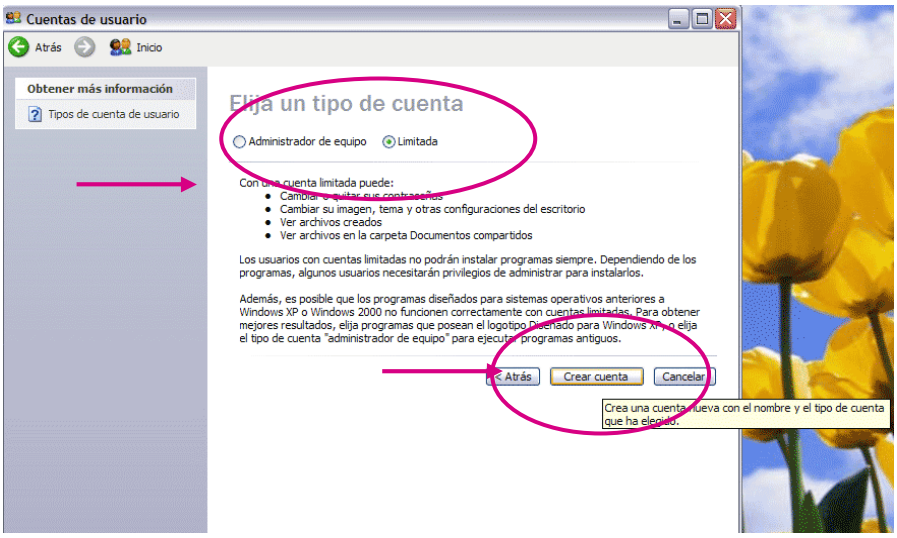
PAS 3. Fer clic a **crear un compte nou**



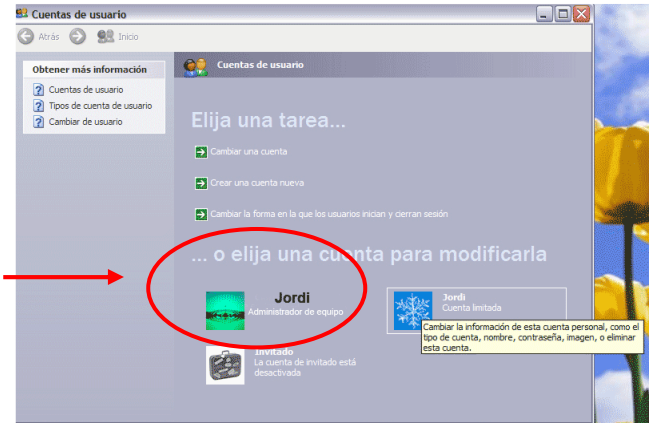
PAS 4. Escriure el nom d'usuari i fer clic en **següent**.



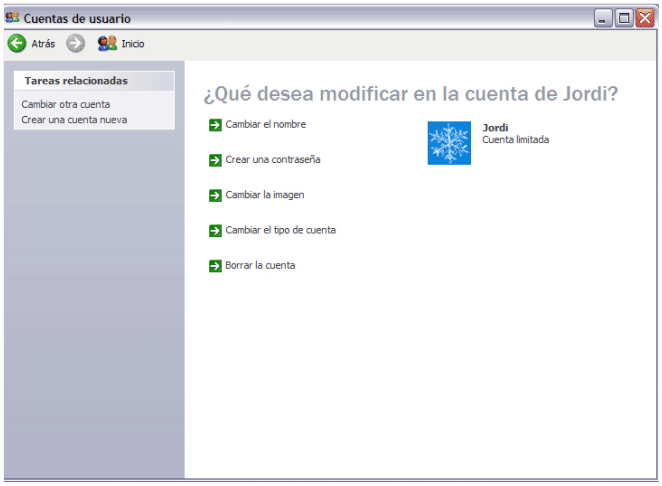
PAS 5. Triar el tipus de compte. Pot ser com a administrador, per tenir el control de l'ordinador o també podem obrir un compte limitat, per exemple, per als nostres fills. Una vegada que hem triat, hem de fer clic a **crear compte**.



PAS 6. S'obrirà una finestra on se'ns indicarà que el nou compte d'usuari ha estat creat. Si desitgem obrir la informació del nou compte, hem de fer clic en el nom de l'usuari, en aquest cas, en el nom de Jordi.



PAS 7. En aquesta secció podrem canviar el nom d'usuari, crear la contrasenya, canviar la icona que ens representa o simplement esborrar al nou usuari.



3. Els virus

Igual que els éssers humans, els ordinadors estan exposats a "malalties" provocades per virus que es poden contreure des d'un dispositiu d'emmagatzematge infectat, un correu electrònic, per haver baixat programes o simplement navegant indiscriminadament per la Xarxa. És important fer palès que els virus entren per l'intercanvi d'arxius, així que no només es transmeten per Internet, sinó també en fer servir unitats de disc externes: discos extraïbles, discos compactes, DVD de dades o disquets. Pensar a tenir el nostre ordinador aïllat, sense fer servir aquests mitjans –Internet i les unitats de disc- no seria pràctic; igual que tenir un cotxe sense rodes.

Tal com passa en el cos humà, els virus en els ordinadors no sempre es manifesten immediatament, sinó que "s'incuben" dintre del cos per un temps determinat fins que alguna cosa els activa: llavors apareixen els veritables problemes. Veiem algunes característiques dels virus:

- poden estar en unprograma d'ordinador.
- Poden autorreplicar-se.
- Intenten ocultar la seva presència fins al moment de l'activació.
- Produeixen efectes nocius en l'hoste, és a dir, en l'ordinador.

Principals tipus de virus

Els tipus de virus es poden definir segons diversos criteris: segons els danys que causa, els fitxers que infecten, les tècniques que utilitzen per infectar, el seu origen, etc. Alguns dels tipus de virus més coneguts són els següents:

a) **Virus resident**: Se'ls anomena d'aquesta manera perquè són virus que s'oculten de forma resident o permanent en la memòria RAM. Aquests virus controlen totes les operacions que realitza el sistema operatiu com l'execució de fitxers i programes. Poden romandre ocults per un temps abans d'atacar o de ser eliminats per antivirus. Exemples: *Randex, CMJ, Meve, MrKlunky.*

b) **Virus d'acció directa:** Aquests virus no romanen en la memòria sinó que es reprodueixen i actuen quan són executats. Busquen contagiar els arxius que estan en el seu mateix directori.

c) **Virus de sobreescriptura**: Són virus que destrueixen la informació continguda en els fitxers, escrivint damunt d'ella i provocant la seva inutilitat. Si això succeeix, l'única forma d'eliminar-lo és esborrant l'arxiu i perdent el seu contingut. Exemples: *Way, Trj.Reboot, Trivial.88.D* .

d) **Virus d'arrencada**: Aquests virus infecten els discos que contenen els fitxers. La seva principal característica és que infecten primerament el sector d'arrencada del disc. Només s'activarà el virus si s'engega aquest últim disc. Exemples: *Polyboot.B, AntiEXE*.

e) **Virus de Fitxer**: Són aquells que afecten programes o fitxers executables (fitxers d'extensions EXE i COM). Aquest és el tipus de virus que ens podem trobar més comunament.

Què fan els virus?

- La combinació de codi potencialment nociu, amb l'habilitat de reproduir-se -i fins i tot "evolucionar"- és el que fa als virus perillosos per als ordinadors. Quan un virus s'instal·la en una màquina, pot executar qualsevol instrucció que el seu autor hagi programat. L'activitat del virus pot iniciar-se en una data determinada, després que el programa infectat s'hagi utilitzat un determinat nombre de vegades o bé a l'atzar.
- Quan s'inicia la càrrega, la majoria dels virus són inofensius, i no fan més que mostrar missatges de diferents tipus.
- Hi ha altres virus més perillosos que poden destrossar arxius, desplaçar o sobreescriure el sector d'arrencada principal, esborrar els continguts del disc dur o, fins i tot, escriure sobre la BIOS[1] deixant l'ordinador inutilitzable.
- La majoria dels virus no esborren tots els arxius del disc dur, ja que si s'esborra tot el disc dur també s'esborrarà el virus.

1 Sistema d'entrada i sortida que permet carregar el sistema operatiu.

Algunes de les accions més evidents dels virus són:

- Fer que l'ordinador s'aturi.
- Esborrar arxius.
- Causar un comportament erràtic en la pantalla o monitor.
- Desplegar missatges.
- Desordenar dades en el disc dur.
- Augmentar la grandària dels arxius (en infectar-los).
- Reduir la memòria total.

Com reconèixer un Virus?

- Molts virus s'anuncien ells mateixos produint un so o mostrant un missatge en pantalla. Però també estan els que no donen cap senyal de la seva presència en l'ordinador (fins que causen el danys).
- Atès que els virus es comporten de maneres diverses, no existeix un signe comú que serveixi d'avís de la seva presència; no obstant això, les accions abans esmentades serveixen com a senyal de la presència d'un virus.

Per què hi ha gent que crea virus?

En realitat no està clar perquè hi ha programadors que es dediquen a crear i alliberar virus: en últim terme només ells ho saben. Es creu que alguns ho fan pel desafiament tecnològic de generar una amenaça única, no detectable. Uns altres ho fan només per vanitat: el creador espera que el virus es propagui de tal manera que el faci famós (la notorietat pública arriba quan les empreses antivirus han de dissenyar una solució específica per aquest virus).

Es poden trobar llistats dels virus actius en els llocs web dels fabricants de programes. Inclouen informació sobre les diferents tipologies, com tractar-los i quines eines existeixen per eliminar-los. Un parell d'exemples:

www.symantec.com/region/mx/avcenter/removal_tools.html

www.pandasoftware.es

- Trobem el virus "lladre de contrasenyes" que monitoritza les direccions web a les que hem accedit que continguin certes cadenes de text, pertanyents a entitats bancàries, i les redirigeix fins altres que les imiten, per enganyar a usuaris desprevinguts, que proporcionarien informació confidencial, per després enviar-la al seu autor. Aquest frau es denomina *phising* i està originant greus contratemps i pèrdues tant a usuaris com a entitats financeres.

- Els ***backdoor*** són un punt d'accés al control parcial d'un ordenador, que permet als pirates informàtics accedir de manera remota a l'ordinador afectat, per realitzar en ell, accions que comprometen la confidencialitat de l'usuari o dificulten el seu treball. Té un nivell alt de perillositat.

- Els **virus cuc** es propaguen mitjançant l'enviament massiu de correu electrònic a direccions que hi ha al sistema infectats. Les característiques dels missatges són variables, encara que l'assumpte del missatge sempre està en anglès o en un altre idioma. També poden propagar-se a través de xarxes d'intercanvi d'arxius (P2P: KaZaa, eMule). Alguns virus cuc (*worm*) intenten detenir programes de seguretat com tallafocs (*firewalls*) i antivirus; i també de monitorització, com l'Administrador de Tasques o l'Editor del Registre de Windows. També poden intentar obrir una porta pel darrera a l'ordinador infectat o actuant des de aplicacions com la de *Microsoft Outlook* en els equips infectats i recursos compartits a la xarxa. L'extensió d'aquest arxiu cuc pot ser *.com, *.cpl, *.exe, *scr.

- Els virus que infecten documents amb ***macros,*** com els de Microsoft Word o Excel (del paquet Office). A l'obrir el document infectat, el virus es copia fins a 50 documents que són enviats com a annexes en altres correus a través del programa de correu Microsoft Outlook (si es troba instal·lat a l'ordinador). El virus també pot infectar altres documents i enviar-ho per correu de forma inadvertida per l'usuari utilitzant la llibreta de direccions de l'usuari. Els receptors poden ser enganyats i obrir l'arxiu infectat, ja que el missatge amb el virus procedeix d'una direcció coneguda.

És important recordar que els virus no entraran en acció fins que no obrim el document adjuntat: el missatge de correu en si mateix és inofensiu. Els usuaris de productes Microsoft han d'estar actualitzats en les aplicacions que l'empresa desenvolupa regularment per contrarestar els virus que afecten als seus programes. És important utilitzar programes amb llicencia o programari lliure (com el gestor de correus de Thunderbird o el paquet de programes d'Open Office).

Què fer quan s'ha contret un Virus?

- En general s'ha de tenir activat el tallafocs i un antivirus que s'actualitzi, i passar-lo cada cert temps per evitar aquesta situació. Quan detectem un virus el primer que cal fer és contenir-lo perquè no es propagui per qualsevol lloc i així poder erradicar-lo.
- Si disposem d'un bon programa de protecció antivirus, podem suprimir el virus i recuperar l'ordinador. Qualsevol bon programa antivirus ens ajudarà a identificar el virus i a suprimir-lo del sistema.
- Si treballem en una xarxa local i sabem que estem infectats per un virus hem de sortir d'ella immediatament.
- Una vegada que hem contingut el virus, necessitarem desinfectar el nostre sistema, i després revisar totes les còpies d'arxius que s'han realitzat des de l'ordinador infectat, ja que aquestes possiblement també tinguin el virus. És recomanable passar per un antivirus aquestes unitats, o senzillament eliminar-les (si és que tenimuna còpia en l'ordinador o en un altre lloc).
- Per desinfectar el sistema, es tanquen totes les aplicacions i s'apaga l'ordinador de seguida. Aleshores, s'arrenca l'ordinador utilitzant el Disc de Recuperació del Sistema (*System Rescue Disk*). Aquest disc fou generat pel programa antivirus, el dia que es va instal·lar. S'utilitza l'antivirus d'aquest disc de recuperació per escanejar el seu sistema a la recerca de virus.
- Les definicions de virus del disc de recuperació poden estar desactualitzades, un cop s'hagi fet una primera revisió, i s'hagi netejat el sistema de virus coneguts, es reinicia el sistema operatiu i es pot optar per realitzar una nova revisió d'antivirus, amb

les definicions actualitzades.

- Si no s'han actualitzat els arxius de definició de virus recentment, cal fer-ho immediatament per estar protegit dels últims virus.
- Una cop que s'ha revisat el sistema, s'haurà d'assegurar que les còpies de seguretat i informació transferible no estiguin infectades. D'aquesta manera, s'assegurarà que l'ordinador no es tornarà a infectar-accidentalment. Igualment, s'han de verificar totes les unitats d'emmagatzematge d'informació.

4. Els antivirus

La gran proliferació de virus, cucs, troians i altres tipus de programari nociu poden afectar tant als sistemes connectats a xarxes de comunicació (Internet) com aquells que no estan connectats a xarxes externes, però disposen de dispositius de lectura de suports òptics o magnètics, capaços d'importar qualsevol tipus de virus (CDs, DVDs, disquets, llapis USB, etc.).

Els antivirus són programes que protegeixen l'ordinador de l'entrada de virus i troians. Són una mesura de precaució molt poderosa, ja que després de detectar la presència del virus, l'eliminen. S'ha de tenir en compte que, tant en la detecció de virus com en la reparació que l'antivirus pugui portar a terme, és molt important la informació que aquests programes tinguin sobre la definició dels virus més recents. En la mesura que disposin d'aquestes dades, podran reconèixer una major quantitat de virus.

En general, els virus guarden còpia de si mateixos en els sectors d'arrencada de disquets i discos durs, o bé en arxius executables o arxius de dades que continguin ***macros***.

Per protegir l'ordinador els antivirus utilitzen distintes tècniques:

- **Rastreig**: Quan un virus està plenament identificat, és possible dissenyar un programa que detecti qualsevol arxiu o sector d'arrencada infectada per aquell.

- **Detecció de canvis**: Els virus han de modificar els sectors d'arrencada o els arxius per infectar-los. L'antivirus pot detectar aquests canvis (fins i tot quan el virus és desconegut) sempre que es pugui discriminar entre canvis normals i canvis virals.

- **Anàlisi heurística**: Mitjançant aquest procediment s'intenta detectar-los monitoritzant els comportaments anormals en la màquina, característics dels virus.

- **Verificació**: Identificar el tipus específic de virus (només per virus coneguts).

- **Desinfecció**: hi ha dos tipus de desinfecció:

  - Específica: s'utilitza per contrarestar la infecció de virus coneguts.
  - Genèrica: mitjançant el coneixement de l'aspecte previ d'arxius i sectors d'arrencada (previ a la infecció) es poden reconstruir els elements danyats.

Els antivirus poden utilitzar-se per revisar l'ordinador periòdicament, o bé es poden carregar automàticament en la memòria per monitoritzar permanentment la màquina. També poden programar-se per fer una revisió completa del sistema en dates predeterminades.

5. Tipus d'antivirus

a) Antivirus gratuïts

Es poden fer escanejos (detecció de virus) de les diferents unitats de l'ordinador i de les unitats extraïbles (disquets, CDs, DVDs, llapis USB, etc.) a través d'un servei que donen alguns llocs d'Internet.

Dins dels antivirus gratuïts que es poden trobar en la Xarxa, hi ha els Antivirus d'Escriptori, que són programes que s'instal·len en l'ordinador i els Antivirus en Línia, als quals s'accedeix mitjançant el navegador web. Per als primers, es necessita estar connectat a Internet només per descarregar el programa. Els segons només funcionen sota demanda, és a dir, quan s'entra en la pàgina web de

l'aplicació. Per tant no protegeixen l'ordinador permanentment. Aquests són recomanables per fer una segona prova a un arxiu dubtós. Per exemple:

http://www.pandasecurity.com/spain/homeusers/solutions/activescan/

Aquests antivirus gratuïts en general no tenen suport per part del fabricant. Però d'altra banda, solen ser igual d'eficaços que les versions comercials i són molt adequats per usuaris domèstics amb requeriments de seguretat normals.

La raó per la que aquests productes es donen gratuïtament és que el mercat corporatiu de seguretat informàtica és molt més gran que el domèstic i alguns fabricants prefereixen donar-se a conèixer entre els usuaris domèstics regalant els seus productes per publicitar la seva marca o deixar que s'utilitzin de prova durant una període.

Antivirus d'Escriptori

- ***Security Essentials*** és l'antivirus gratuït de *Microsoft.* Senzill d'instal·lar i d'utilitzar. Proporciona protecció en temps real contra virus, *spyware* i *malware* (programari malintencionat); és a dir, es manté sempre actualitzat i executant-se en un segon pla sense interrompre a l'usuari. D'aquesta manera, s'assegura que l'ordinador estigui sempre protegit i avisa de la protecció.

  Es pot descarregar i veure un vídeo amb les instruccions de funcionament a:

  http://www.microsoft.com/Security_essentials/default.aspx

- ***ClamWin Antivirus*** és un analitzador capaç de detectar virus que hagin contaminat qualsevol directori o arxiu de l'ordinador. És de codi obert, és a dir, que pot ser modificat per l'usuari, i utilitza bases de dades que s'actualitzen freqüentment a través d'Internet. El programa s'integra en el menú contextual de l'Explorador de Windows per analitzar arxius amb major comoditat, i afegeix també un *plug-in* per al client de correu

Microsoft Outlook a fi d'analitzar els fitxers que t'envien com adjunts. Inclou diverses opcions de configuració com la programació d'anàlisi de sistema periòdics, guardar els informes generats, eliminar o moure a un directori de quarantena els fitxers infectats, etc.

- Alwil Software ofereix la versió domèstica del seu antivirus, ***Avast Home***, gratuït per ús "domèstic sense ànim de lucre". Està disponible en espanyol. Disposa de protecció resident, i la seva característica més rellevant és que el filtrat de correu electrònic és independent del client de correu, ja que implementa un servidor de correu SMTP on realitza l'exploració el correu. Simplement cal configurar el client de correu perquè usi com a servidor de correu entrant i sortint el de l'antivirus. Com a curiositat, disposa d'una interfície que podem personalitzar mitjançant caràtules (*skins*).

Antivirus en Línia

Aquests antivirus no s'instal·len en l'ordinador com un programa convencional, sinó que s'hi accedeix mitjançant un navegador web. El temps d'escanejat varia en funció de la velocitat de la seva connexió, la càrrega momentània dels servidors o el volum de dades que es vulgui rastrejar. La majoria d'aquests serveis descarreguen un subprograma (*ActiveX o Java*), i per això la primera vegada que s'hi accedeix triguen uns minuts a arrencar.

- ***Bitdefender***. Després de la càrrega del subprograma ActiveX i els seus components, mostra una vista en arbre de l'estructura de directoris del sistema. En ella, es poden seleccionar les unitats sobre les quals es desitja realitzar la recerca de codi maligne. En espanyol.

- ***TrendMicro***. Presenta una estructura d'arbre de directoris amb les unitats del sistema, per escollir aquelles de les quals es desitja realitzar l'escanejat de virus. La pàgina de descàrrega d'Internet està majoritàriament en anglès, però el producte està en castellà i té incorporada una eina de revisió de ports.

- **AVG:** Ofereix versions prèvies gratuïtes i un sistema de rastreig de virus tant per l'ordinador com per programes. Té una interfície molt senzilla d'utilitzar i es poden programar actualitzacions i escaneig del sistema.

b) ***Sharewares***

També és possible baixar (descarregar) d'Internet alguns programes d'antivirus. Per descarregar-los sempre és necessari pagar. No obstant això alguns donen la possibilitat de provar-los per un temps (aprox. 30 dies), és a dir, es tracta de *Sharewares* (programes per compartir).

- **Kaspersky.** És un complet i avançat sistema de protecció per usuaris professionals que requereixen una protecció extra de fiabilitat garantida. El programa inclou un ampli ventall d'utilitats i funcions per optimitzar la seguretat del PC i tenir sempre el màxim de seguretat possible: vigilància de totes les fonts possibles de virus, tecnologia de protecció integrada per aplicacions d'Office, suport per un gran nombre de clients de correu electrònic, possibilitat de controlar també arxius comprimits, eines millorades de gestió i notificació avançada d'amenaces i infeccions, etc.

  Kaspersky pot, a més a més, recuperar dades en arxius infectats, i compta

amb una base de dades de virus actualitzada cada hora. No només proporciona protecció en temps real, sinó també la possibilitat de realitzar anàlisis de sistema completes cada cert temps, tot això al més alt nivell de velocitat i efectivitat.

- **Panda**. És un paquet d'eines amb el qual es pot protegir l'ordinador de virus, intrusos, *dialers* no autoritzats (programes que realitzen trucades telefòniques des del PC), correus escombraria, etc., fins i tot amb eines de control de contingut web. Cada element es pot configurar o activar individualment, per això s'adapta a les necessitats de cada usuari. Es poden configurar les següents opcions: Antivirus, *Firewall*, *AntiSpyware*, *AntiDialers*, *AntiSpam*, Filtrat de continguts web, *TruPrevent*.

  En general la versió de prova és funcional durant un període de 30 dies.

Quan tenim l'antivirus instal·lat per un mes és possible fer escanejos de totes les unitats, i així fer una neteja general de l'ordinador i les unitats extraïbles. No obstant això, no s'ha d'oblidar de desinstal·lar el programa un cop que ha finalitzat el període de proves. Alguns es desinstal·len automàticament, però d'altres no. Si ens passem del termini el programa comença a funcionar malament i podria generar problemes en l'ordinador.

c)Instal·lació d'un antivirus de pagament

Aquesta és l'opció més recomanable, ja que el programa antivirus queda instal·lat en l'ordinador, i d'aquesta manera està en constant funcionament, compleix la funció de barrera permanent que detecta l'aparició de virus tant els que venen d'Internet com els que procedeixen d'alguna unitat extraïble. Igual que els antivirus que escanegen des d'un lloc d'Internet o els *shareware*, una vegada que detecten la presència d'un virus fan de "metge" i eliminen "l'agent patogen". Per

això és millor tenir instal·lat l'antivirus, ja que en estar funcionant constantment detectarà els virus tot just entrin a l'ordinador i així els eliminarà abans que provoquin algun dany. En canvi, en els altres sistemes (gratuït i *shareware*), pot ser que el virus hagi entrat abans, i si bé l'antivirus detectarà l'agent "estrany" i l'eliminarà, el virus pot haver provocat danys en l'ordinador que dependran tant del temps que l'haguem tingut allotjat com de les condicions que permeten la seva propagació.

Els programes d'antivirus més poderosos i coneguts són Norton Antivirus (Symantec), McAffe i Panda. Es poden comprar en botigues del ram o es poden descarregar i pagar via Internet. Els preus fluctuen, per això és recomanable buscar bé abans de fer un compra:

Norton AntiVirus www.symantecstore.com

Mc Afee 2006 www.mcafeestore.com

Panda http://www.pandasecurity.com/spain/homeusers/solutions/

Aquests antivirus disposen d'un instal·lador interactiu i només s'han de seguir les indicacions que ens van donant. En aquesta càpsula s'han detallat aspectes de les principals utilitats del programa *Norton AntiVirus* que ve amb els sistemes operatius de Windows.

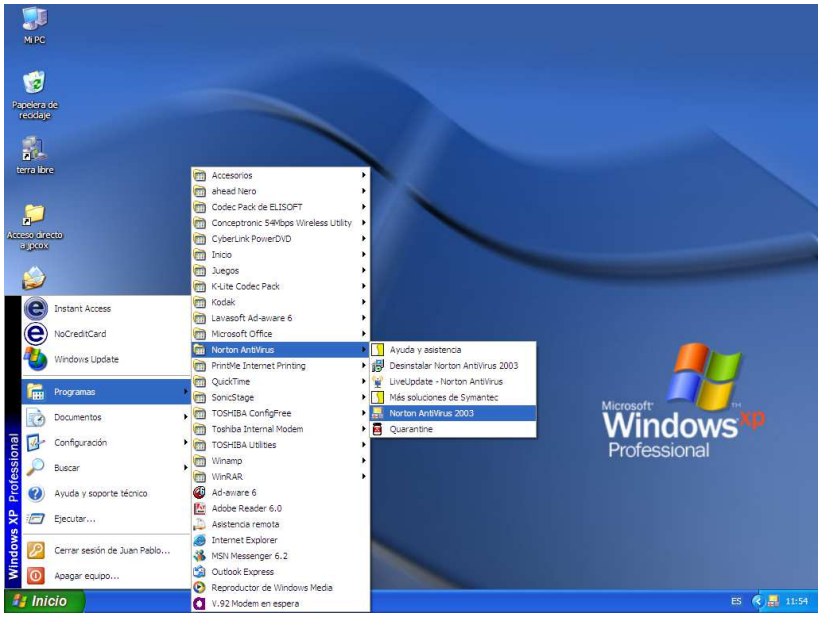
PRÀCTICA 1

Per fer un escaneig general de l'ordinador

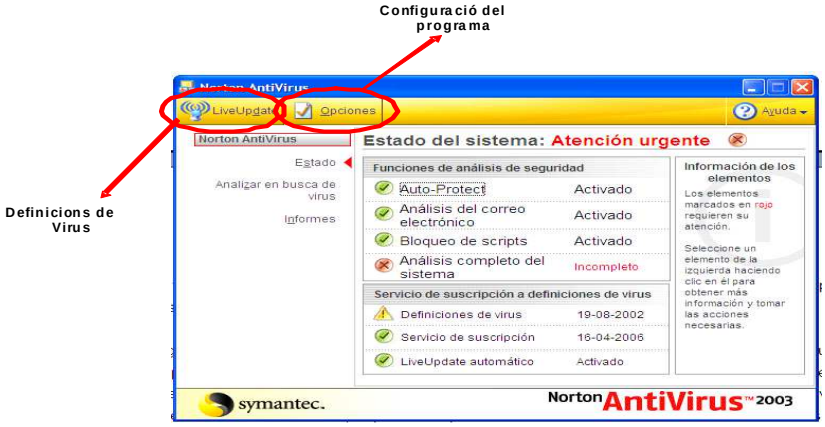
PAS 1: Entrar al programa Norton

Anar a "Inici" / "Programes" / "Norton Antivirus" / "Norton Antivirus 2003".

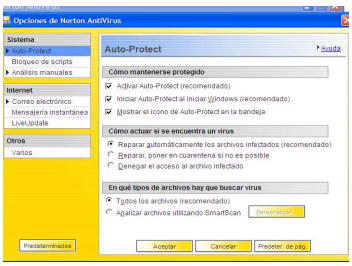
(Dependrà de la versió que tinguem. N'hi ha de més recents, però com veurem més endavant, l'important és la data del servei de subscripció a definicions de virus).



PAS 2: Una vegada obert el programa és necessari parar atenció als següents aspectes.

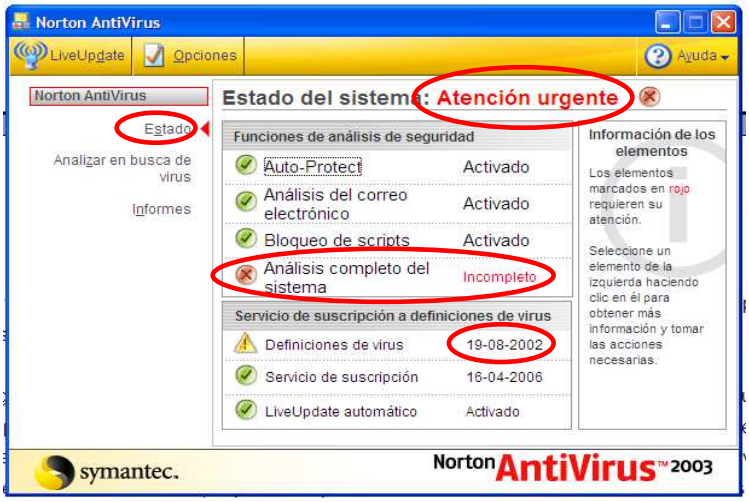


- El comandament *LiveUpdate* aconsegueix les definicions de virus més recents i les actualitzacions dels programes Norton Antivirus quan l'ordinador està connectat a Internet.



- El comandament d'Opcions permet configurar la forma com opera el programa. Se suggereix seguir les opcions recomanades on es desplegarà la següent pantalla:

PAS 3: Una vegada seleccionades les opcions de preferències, tancarem el quadre i tornarem al quadre inicial del programa. Aquí és necessari parar esment als següents aspectes:



- El programa sempre s'obre en la secció "Estat", on hi ha les funcions d'anàlisi i el servei de subscripció a definicions de virus.
- El que primer destaca en obrir el programa és que l'Estat del sistema requereix una "Atenció urgent", això es deu al fet que no s'ha fet una anàlisi completa del sistema (totes les unitats de l'ordinador). Dintre de las funcions d'anàlisi de seguretat s'han activat les següents funcions:
    - Auto-Protect: proporciona protecció contínua contra virus, cucs i troians; revisa tots els arxius que es descarreguen d'Internet. S'executa en segon pla i sense interrompre el treball que estiguem fent.
    - Anàlisi del correu electrònic: impedeix l'entrada i sortida de correus electrònics infectats amb virus.
    - Bloqueig d'***Scripts***: supervisa els *scripts* i alerta del seu comportament nociu.
    - Anàlisi completa del sistema: se suggereix fer una anàlisi completa com a mínim una vegada a la setmana per a assegurar-se que l'ordinador no tingui virus.

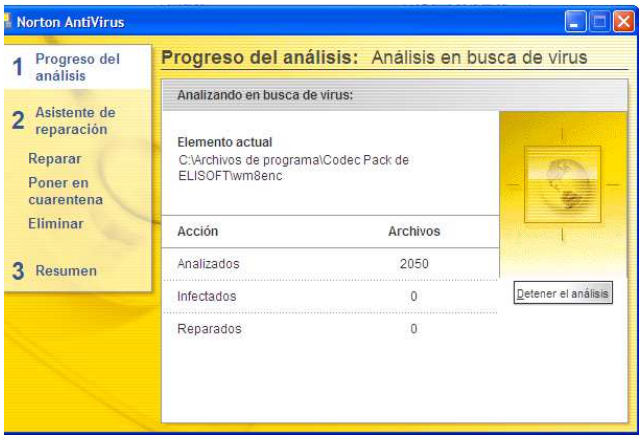
- Respecte del servei de subscripció a definició de virus cal tenir en compte els següents aspectes:
  - La vigència d'un Antivirus depèn del temps que duri la llicència, és a dir, fins a quina data funciona actualitzat la definició de virus perquè l'Antivirus pugui reconèixer-los. En el cas que no n'hi hagi, és possible suposar que l'ordinador amb aquest antivirus no està realment protegit, perquè des d'aquesta data fins a l'actualitat han aparegut una sèrie de virus nous per als quals no s'han integrat les eines per a reconèixer-los i eliminar-los.
  - El servei de subscripció, en l'exemple que es presenta, caduca, per tant es podria actualitzar la definició de virus i així fer una revisió completa amb aquesta nova informació. Per a això és necessari connectar a Internet l'ordinador, ja que les actualitzacions es baixen automàticament des del lloc web de Symantec (empresa creadora de Norton Antivirus).
  - El servei de *LiveUpdate* està activat perquè es realitzi de manera automàtica. D'aquesta manera Norton Antivirus aconsegueix les definicions de virus més recents i les actualitzacions del programa quan l'ordinador està connectat a Internet. Si ens aturem a analitzar el nostre exemple és possible suposar que el programa està instal·lat en un ordinador que no s'ha connectat a Internet i per això no s'han aconseguit les noves definicions de virus (per a solucionar això caldria connectar-lo i automàticament aquestes noves definicions quedarien integrades al sistema), ja que encara estem dintre de la data que dura la llicència.

PAS 4: Per a fer un escaneig o revisió de l'ordinador cal prémer "Analitzar en recerca de virus".

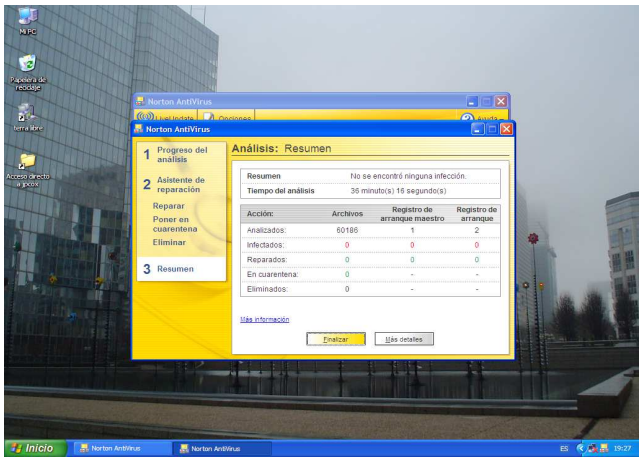
Aquí es presenten totes les unitats que es poden analitzar. Seleccionem l'opció desitjada amb un doble clic. Com s'ha esmentat anteriorment se

suggereix fer una anàlisi de tot l'equip una vegada a la setmana.

Apareixerà el següent quadre que informa de l'estat de l'anàlisi a la recerca de virus.



PAS 5: Una vegada que ha acabat el procés apareixerà la següent pantalla. Fer clic a "Finalitzar" per a acabar amb el procés d'anàlisi.



PAS 6: Quan un Antivirus troba virus, dóna l'opció per a reparar-lo immediatament o deixar-lo en quarantena, sempre és recomanable la primera opció.

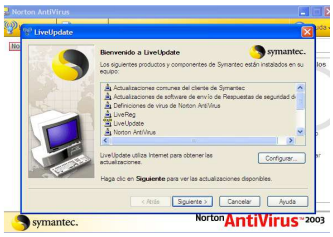
Per renovar la definició de virus i actualitzacions del programa

PAS 1: Obrir el programa.

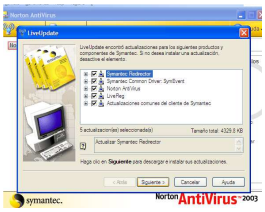
PAS 2: Seleccionar l'opció LiveUpdate

Quan l'ordinador està constantment connectat a Internet aquesta renovació de la definició de virus es realitza automàticament una vegada a la setmana. Quan es realitza aquesta actualització l'ordinador informa d'aquesta nova informació mostrant un quadre. Només cal acceptar perquè es renovin les definicions de virus.

PAS 3: Apareixerà un quadre de diàleg indicant els productes i components que ja s'estan instal·lant en l'ordinador. Fer clic en "Següent".



PAS 4: Després s'indiquen les actualitzacions que es van trobar per al programa.



PAS 5: Finalment es desplegarà un quadre indicant els components i productes que han estat actualitzats. Fer clic a "Finalitzar".

6. Configurar el nostre navegador

Internet ens ofereix una gamma d'oportunitats per obtenir informació, comunicar-se, aprendre, comprar o vendre, però així com té avantatges, també té el seu costat fosc: un món ple d'imatges o llenguatge inadequats, virus, programes espies i diversos elements delictius que s'amaguen sota identitats falses.

Els **navegadors** d'Internet ens ofereixen l'oportunitat de restringir l'accés a pàgines web des del sistema operatiu Windows, així com altres eines de seguretat, útils per tenir una navegació més fiable per Internet.

En general, es troben les següents eines des del menú Eines / Opcions d'Internet / Seguretat del navegador Internet Explorer o des del panell de control del sistema operatiu Windows:

- **Llocs de confiança**: on podem afegir pàgines web coneguts i que no suposen

un perill per l'ordinador. Aquesta configuració pot ser personalitzada o utilitzar el nivell predeterminat que en aquest cas és de seguretat "Baixa".

- **Llocs restringits**: on es poden incloure els llocs web que

considerem perillosos i als quals volem restringir-ne l'accés des del nostre sistema. Aquesta eina pot ser molt útil per limitar l'accés de menors a pàgines que es consideren no aptes per ells. Aquesta configuració també pot ser personalitzada o utilitzar-se la predeterminada que en aquest cas és de seguretat "Alta".

- **Internet**: es refereix al conjunt de webs que no s'han inclòs en cap de les

dues opcions anteriors. Com en els altres casos, ens permet escollir entre configurar els accessos de forma personalitzada o utilitzar el nivell predeterminat de seguretat que aquí és "Mitja".

- **Intranet**: ofereix les mateixes opcions que l'apartat Internet,

però aplicades a la nostra xarxa local, si se'n disposa d'una.

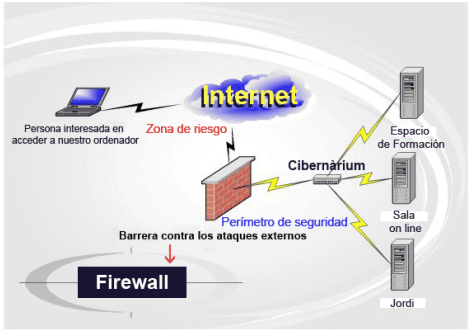
Per accedir a aquestes opcions hem de seguir els següents passos:

PAS 1. Anar a **inici**, després, fer clic a **panell de control** ☐ **Centre de seguretat** ☐ **Opcions d'Internet** ☐ icona d'**Internet.**

Escollir si volem configurar els accesos a Internet de manera personalitzada o si es prefereix el nivell predeterminat (seguretat "Media")

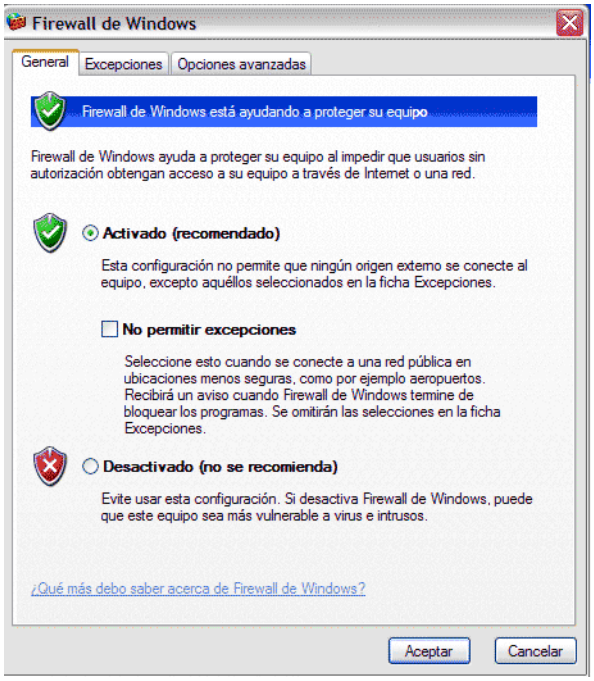
Igualment es podran establir els nivells de seguretat per la **Intranet, Llocs de confiança** (en el que es pot escollir seguretat "Baixa") i **Llocs restringits** en el que es recomana seguretat "Alta".

7. El *Firewall* o tallafocs



Un **tallafocs** o ***firewall*** és un sistema de seguretat que serveix per evitar incendis forestals i consisteix a establir una barrera física per protegir una zona de l'abast del foc. En el cas dels ordinadors un ***firewall*** o tallafocs és una barrera que protegeix el nostre ordinador dels possibles atacs d'un usuari extern que, a través de la connexió a Internet, intenti entrar al nostre ordinador. La zona protegida es diu "perímetre de seguretat" i la protecció es realitza separant-la d'una zona externa, no protegida, anomenada "zona de risc".

En l'actualitat, els sistemes operatius, com el cas de Vista o Windows 7, inclouen un *firewall* que simplement s'han d'activar. A més, es poden trobar, a Internet o en botigues especialitzades, **tallafocs personals** que són programes que s'instal·len a l'ordinador i que permeten filtrar i controlar la connexió a la xarxa Internet.



Per activar, el **tallafocs** de Windows se seguiran els següents passos:

Anar a **inici** i fer clic en **panell de control** ☐ **Centre de seguretat** ☐ **Firewall de Windows** ☐ clic sobre l'icona verda per activar el *firewall* recomanat per Windows

8. Els *Spyware* i troians

SPYWARE

Els programes espia (*spyware*) obtenen informació de l'usuari que està connectat a Internet sense el seu coneixement. Aquests programes permeten que una tercera persona accedeixi al nostre ordinador i monitoritzi el sistema sense que ens n'adonem. De vegades fan servir troians (veure punt següent i glossari) per aconseguir l'adreça de correu electrònic, saber quines son les pàgines web que visitem més vegades i en els casos més greus contrasenyes i números de targetes de crèdit de l'ordinador de l'usuari. Aquest tipus de programes també s'utilitzen per la publicitat: obtenen informació sobre els nostres hàbits de navegació que venen a empreses que, posteriorment, ens envien anuncis. Aquest tipus de *spyware* va inclòs freqüentment en altres programes *freeware* (gratuïts), *shareware* (de prova) o els denominats P2P, que funcionen per intercanvi d'arxius (KaZaa, eMule) que es poden descarregar d'Internet o en pàgines de televisió *online*.

Com podem saber si hi ha un spyware a l'ordinador?

Existeixen alguns "símptomes" a l'ordinador que poden ajudar a detectar si hi ha un programa espia com són els següents:

- L'aparició, sense motiu aparent, de *banners publicitaris* o *finestres emergents*, i en algunes ocasions noves barres d'eines en el navegador, que l'usuari no ha afegit.
- El *canvi sobtat en la pàgina d'inici* del navegador d'Internet.
- El *bloqueig inesperat* del navegador d'Internet.
- De vegades l'ordinador, sense cap causa aparent, comença a *funcionar molt lentament*. Això pot ser per diversos motius: molts programes treballant al mateix temps o problemes de xarxa, però també per un programa espia.
- *L'ordinador es bloqueja* (es queda penjat o desocupat) en moments de càrrega excessiva, però també pot bloquejar-se pel mal funcionament d'un programa espia. Això és especialment clar quan s'estan realitzant operacions senzilles que no suposen massa treball per a l'ordinador.
- Algunes *tecles* de l'ordinador no funcionen.
- Apareixen *missatges d'error* de Windows.

Com protegir-se de l'spyware i què fer si ja es troba en l'ordinador?

Hi ha dues coses a tenir en compte sobre els *spyware*: la "prevenció", que consisteix en el seguiment de certs consells bàsics, i la cura, que s'ha de fer quan hi ha un problema a l'ordinador.

1) Prevenció

- Quan es navega per Internet, assegurar-se de tenir activat un *firewall* (ja sigui el de Windows o un altre).
- Augmentar el nivell de seguretat del navegador per no permetre l'execució automàtica de finestres emergents o *banners*.
- Tenir especial cura amb els programes que es descarreguen des d'Internet: molts programes gratuïts, especialment aplicacions d'intercanvi d'arxius P2P, contenen arxius que són programes espia. Aquests programes restaran rendiment i memòria a l'ordinador i impediran l'òptim funcionament del seu ordinador i fins i tot bloquejaran el navegador d'Internet o el mateix sistema operatiu.
- Mantenir les aplicacions instal·lades a l'ordinador sempre actualitzades, instal·lant els **pegats de seguretat** (veure definició en glossari) desenvolupats pels fabricants. D'aquesta manera, els programes espia no podran instal·lar-se en el seu ordinador.

Una bona solució és instal·lar en el seu ordinador un anti*spyware*. Aquest programa funciona de manera similar a l'antivirus, és a dir, realitza una exploració en el nostre ordinador per identificar i eliminar els programes espia, registrar les entrades del sistema operatiu, a més de revisar els altres programes que tinguem instal·lats. També augmenta la privacitat en l'ús del nostre ordinador, manté el sistema sense els espies que puguin estar observant-nos, registrant i transmetent la nostra informació privada. Però perquè l'*antispyware* funcioni correctament cal mantenir-lo actualitzat i en funcionament sempre.

2) Cura

- Posar a treballar l'*antispyware*, tal i com es fa amb un antivirus i eliminar els espies que es trobin.

- Una vegada que s'eliminen els *spyware*, recomanem mantenir el seu antivirus i *antispyware* actualitzats. També és important tenir un sistema *firewall*.

SABIES QUE...

Els programes que permeten l'intercanvi d'arxius de màquina a màquina a través d'Internet estan de moda. A aquest tipus de tecnologia se li coneix com *Peer to Peer* (Punt a punt o Igual a Igual) o en poques paraules P2P. Però moltes vegades, els nostres programes favorits P2P com eMule o KaZaa (versió gratuïta), poden portar programes espia.

L'opció més adequada és:

1. Mantenir-se informat: revisar a Internet les pàgines que informen sobre els programes P2P infectats per no instal·lar-los en el nostre ordinador.
2. Tenir la darrera versió del P2P i mantenir-lo actualitzat.
3. Finalment, tenir el nostre sistema de seguretat sempre alerta.

TROIANS

Aquest tipus de programes-virus, si bé no són considerats programes espia, resulten ser molt semblats a aquests, ja que s'ocullen en l'interior d'un programa d'aparença innocent. Quan aquest últim s'executa, el troià realitza l'acció o s'oculta en l'ordinador de qui l'hagi activat, tal com succeeix amb els virus. Per això és considerat un programa tipus virus. La funció principal del troià és la d'espiar a persones, monitoritzar el que estan fent a cada moment, per a obtenir informació confidencial i controlar al nostre ordinador, però, a diferència dels programes espia, el troià, pot fer malbé.

part del disc dur.

Com podem saber si hi ha un troià a l'ordinador?

Com ja s'ha esmentat amb anterioritat, un troià és un programa tipus virus, per tant, la manera d'adonar-se'n si tenim un a l'ordinador és similar a la dels virus.

Si tenim un troià a l'ordinador es podrà observar:

- Disminució en el rendiment general de l'ordinador.
- Disminució de la memòria.
- Canvis en els arxius.
- Canvis en els programes, com el fet de tancar-se sense motiu aparent.
- Aparició de missatges d'error de Windows, per esmentar-ne alguns.

Per protegir-se del troià, simplement activar l'antivirus i revisar tots i cadascun dels arxius que es reben ja sigui en CD, USB o per Internet. Igualment mantenir l'antivirus actualitzat, i portar a terme una revisió regular de les noves amenaces. També, procurar no instal·lar programes pirates o arxius gratuïts d'Internet que no siguin de confiança.

9. L'spam i el correu electrònic

SPAM

Quantes vegades en obrir el correu electrònic, hi ha una quantitat impressionant de missatges no esperats? Al correu electrònic no sol·licitat se'l coneix amb el nom d'***spam***. Sol ser publicitat, ofertes o enllaços directes a una pàgina web. Aquests missatges són enviats a milers de destinataris alhora. Les adreces per a enviar els *spam* solen ser robades, comprades, recol·lectades o preses de cadenes de correus electrònics.

Es pot dir que hi ha 2 tipus d'***spammers*** (persones dedicades a enviar *spam*): els que ens envien només un missatge i els que bombardegen cada setmana amb el mateix missatge.

Com funciona?

Segurament ens hem preguntat alguna vegada: com m'arriba l'*spam* si jo no he donat a conèixer el meu correu electrònic? Quan s'envia un correu electrònic s'exposa el contingut del missatge, així com les dades del destinatari i del remitent. Aquest correu, abans d'arribar a la seva destinació passa per diverses parts d'Internet, de manera que persones malintencionades (*spammers*) a les que els interessa aquest tipus d'informació la poden aconseguir amb determinades tècniques. Els *spammers* registren les dades al seu ordinador i posteriorment envien l'*spam*.

Quines són les conseqüències de l'spam?

Esmentarem les més habituals:

- Són irritants per que arriben a la Safata d'Entrada.
- Es perd temps en eliminar-los. En el cas d'una empresa, això es pot traduir en fortes pèrdues de diners.
- Ens exposa a virus, programes espia o troians.

Què podem fer per protegir-nos de l'spam?

En l'actualitat, els proveïdors de correu gratuït més utilitzats com Hotmail o Yahoo, tenen un sistema anti*spam* que funciona com a filtre, de tal manera que els correus considerats *spam*, s'envien a una carpeta per ser eliminats posteriorment. Per activar aquests filtres és necessari anar a la secció d' "Opcions" o "Propietats" del nostre correu electrònic i seguir els passos que s'indiquen. Allí, ens donaran la possibilitat de personalitzar la protecció *antispam*.

Una altra manera per mantenir-se fora de perill és eliminant aquells correus que ens semblin sospitosos, és a dir, que vinguin amb un assumpte que sembli estrany o amb un idioma que desconeguem. Per a identificar-los, hem d'apel·lar al nostre sentit comú. Finalment, mai respondre a un *spam:* fer-ho és estar confirmant a l'*spammer* que l'adreça existeix.

Altres recomanacions

- Com que el correu electrònic és una de les vies més freqüents per les quals entren els virus als ordinadors, és necessari estar molt atent i posar-hi una especial cura. El primer que cal tenir en compte és que el simple fet de rebre un correu electrònic per Internet no representa perill, excepte quan tingui annexat al missatge un arxiu amb codi executable (encara així, l'arxiu hauria d'executar-se, per la qual cosa el simple fet de llegir el missatge de correu no representa perill).

- Alguns paquets de correu com l'Outlook de Microsoft, podrien ser susceptibles a un virus que es trobi amagat en el missatge mateix de correu (en forma d'un "*script*"). Però això es corregeix modificant la configuració de seguretat del paquet Outlook o bé aplicant una actualització al paquet. El virus no entrarà en acció mentre no s'obri el document annex. El missatge de correu en si mateix és inofensiu.

- De tota manera sempre se suggereix esborrar els correus "sospitosos", és a dir, els que tenen un assumpte estrany o en un altre idioma. Moltes vegades els remitents d'aquests missatges són persones desconegudes, però també arriben amb noms de persones que coneixem (virus Melissa). En aquests casos, és recomanable esborrar el missatge, avisar a la persona i per precaució revisar l'ordinador amb un antivirus actualitzat.

- Un altre element que afecta la seguretat són els *spam*. Si bé aquests generalment no porten virus, podrien tenir-los. Però més que això és una forma a través de la qual algunes empreses busquen obtenir dades de les persones, per això no és bo respondre un *spam* que no s'ha sol·licitat ja que així confirmem la direcció al *spammer*.

Scam

L'*scam* és una forma de frau per Internet. Consisteix en un correu electrònic fraudulent (o pàgines web fraudulentes) que pretén estafar econòmicament per

mitjà de l'engany, generalment presentat com a donació a rebre, loteria o premis als que s'accedeix previ enviament de diners.

Phishing

El *phishing* és un altre tipus de frau caracteritzat per intentar adquirir informació confidencial de manera fraudulenta (com pot ser una contrasenya o informació detallada sobre targetes de crèdit o altres informacions bancàries). L'estafador es fa passar per una persona o empresa de confiança (p.e.: un banc o entitat financera) i sol·licita contrasenyes bancàries, números de compte, etc.

Hoax

Els *hoax* són missatges amb continguts falsos o enganyosos, generalment provinents en forma de cadena. Solen anunciar virus desastrosos, enganys sobre persones malaltes que necessiten ajuda, o qualsevol tipus de noticia sensacionalista falsa.

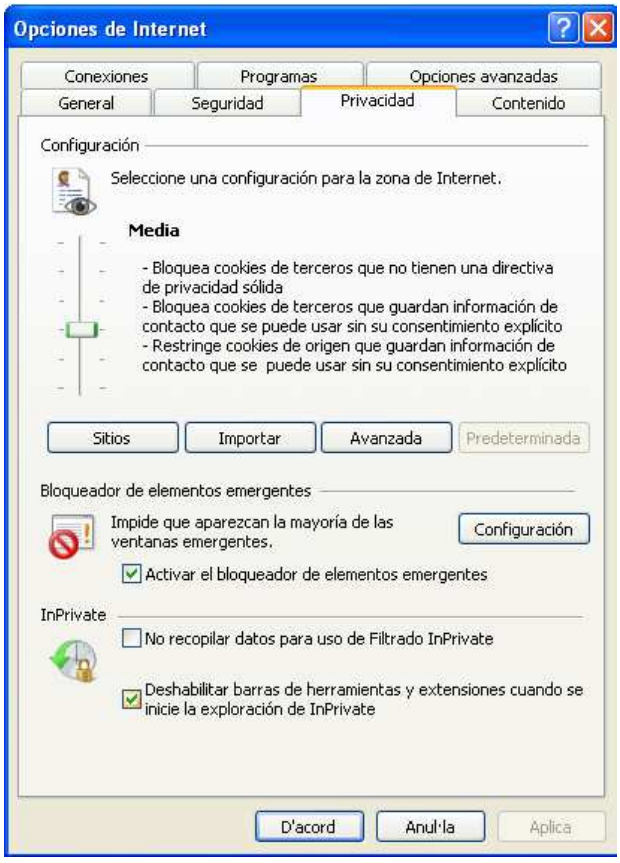
Per protegir-se de l'*Scam* i dels *Hoax* es recomana estar molt atent als correus rebuts i marcar com a *spam* els correus "sospitosos" (el que venen un assumpte estrany o en un altre idioma) i no creure's la informació si no hi ha una font per a corroborar-la.

El comerç electrònic

La compra i venda de productes, així com les transaccions bancàries via Internet, en general estan especialment protegides per aquelles empreses que ofereixen aquests serveis. No obstant això no és bo confiar-se. Abans d'escriure el número del compte corrent i/o de la targeta de crèdit s'ha de verificar que es tracta d'una empresa seriosa i de confiança per no ser víctimes d'un *phising*.

Els navegadors més recents tenen un sistema *anti- phishing* i un filtre de dades que es pot establir des d'Opcions d'Internet al menú d'Eines del Navegador.

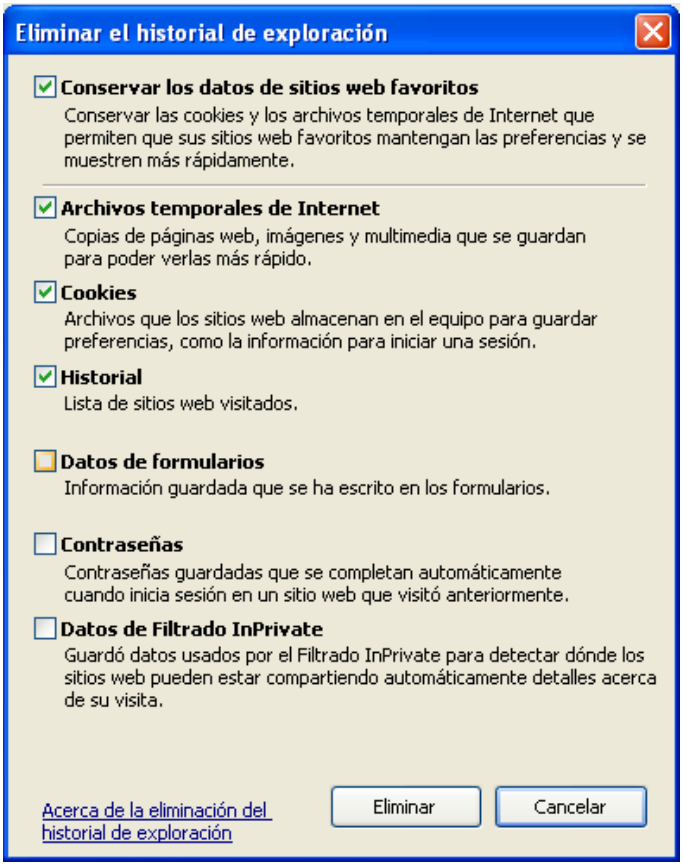
També es pot seleccionar en la configuració de **Privacitat** el nivell Mitjà i Bloquejar elements emergents.



Depenent dels navegadors que s'utilitzin es podran utilitzar opcions com l'*InPrivate* de l'Explorador de Windows que evita l'enviament d'informació durant la visita a un lloc web i així controlar que la informació sigui compartida. S'haurà de tenir en compte que a l'habilitar-ho és possible que no es pugui accedir a alguns continguts de la pàgina.

És possible que navegadors com Mozilla Firefox i Google Chrome puguin ser molt efectius en quant a seguretat (ja que no estan exposats a atacs per ser de codi lliure) però això no significa que es pugui descuidar la seguretat. Per això, sempre és una pràctica sana esborrar les dades de la navegació, en especial quan s'han deixat dades en una pàgina web.

Per fer-ho, s'ha de buscar en les eines del navegador les Opcions d'Internet i esborrar Formularis de dades.



10. Bones pràctiques de seguretat

Per protegir la informació, els arxius i programes que es troben ja sigui en els ordinadors del nostre entorn de treball o l'ordinador personal, i mantenir-se lliures de virus, troians, programes espia, *spam*, s'han de tenir en compte les següents recomanacions.

Normes bàsiques

- Actualitzar les nostres aplicacions i programes amb els pegats de seguretat. Per a això, hem de visitar periòdicament els llocs web de les companyies creadores del programa o programes que tenim en el nostre ordinador i instal·lar les actualitzacions.
- Instal·lar tallafocs (*firewall*), que ens garanteixin la seguretat en les nostres comunicacions via Internet perquè bloquegen les entrades sense autorització a l'ordinador i perquè la sortida d'informació queda restringida.
- Instal·lar l'antivirus per a detectar i eliminar virus; programar-lo perquè revisi l'ordinador de forma periòdica; verificar periòdicament que està actiu, a més de l'actualització constant.
- Instal·lar *antispyware* per a protegir l'ordinador de programes espia que controlen els nostres hàbits de navegació per Internet.
- Instal·lar eines anti*spam* que ens ajudin a filtrar el correu i protegir el nostre equip de tot tipus d'amenaces.
- Assegurar-nos que tot el programari instal·lat en l'ordinador provingui d'una font coneguda i segura.
- No instal·lar programari pirata.
- No confiar en els arxius gratuïts que es descarreguen de llocs web desconeguts, ja que són una potencial via de propagació de virus.
- Si s'envien correus a diverses persones, utilitzar la casella CCO (amb còpia oculta) per a què els correus dels nostres contactes no siguin utilitzats per *spammers*.

En el nostre ordinador personal

- En general mai hem de permetre que s'instal·lin en el nostre ordinador programes de procedència dubtosa.
- En navegar per Internet, únicament instal·lem programari obtingut d'empreses de reconegut prestigi.
- Mai obrim un arxiu annex a un correu electrònic a menys que estiguem segurs de la seva procedència.
- Sempre hem de protegir els programes i la informació més important.
- En compartir discs d'emmagatzematge, hem de protegir-los contra escriptura per a evitar que siguin infectats.
- Hem d' utilitzar un programa antivirus per a netejar-los i detectar-los.
- En cas que l'ordinador ja estigui infectat i no contem amb antivirus, avisem a un tècnic perquè revisi i netegi el nostre ordinador.
- Actualitzem freqüentment el programa antivirus, així com la base de dades de virus coneguts.

A la feina

- L'empresa ha d'establir una política de seguretat a nivell corporatiu.
- Ha de realitzar còpies de seguretat tant de la informació com dels programes utilitzats.
- Ha de mantenir el programari actualitzat i amb les llicències corresponents.
- S'ha d'usar programari legal i segur.
- No utilitzar programari innecessari ni d'origen poc confiable.
- Validar l'autenticitat dels usuaris i controlar el seu accés.
- Com a usuari, mai obrir un arxiu annex al correu electrònic sense revisar-lo abans.
- L'usuari no ha d'utilitzar el compte de correu electrònic de l'empresa per a activitats comercials.
- L'empresa ha d'utilitzar programari especialitzat: *firewall*, antivirus, *antispyware*, *antispam*.
- L'empresa ha de desenvolupar eines per a la gestió de l'actualització del programari a nivell massiu.
- Ús de protocols segurs en l'empresa (https, ftp, entre altres).
- Utilització de signatures i certificats digitals.
- Ús d'eines de programari lliure com: Linux, Mozilla Firefox, Mozilla Thunderbird.

GLOSSARI

Antispam. Programa que detecta i elimina els correus electrònics no sol·licitats.

Antispyware. Programa que detecta i elimina els programes espia.

Antivirus. Programa que detecta i elimina els virus informàtics que poden haver infectat els arxius en un disc dur, un disquet o qualsevol altre dispositiu d'emmagatzematge de dades.

***Banner* publicitari *Pop Up* o finestra emergent**. Gràfic, generalment rectangular, que s'insereix en una pàgina web, amb fins publicitaris o promocionals. Pot funcionar com a vincle o *link*, ja que enllaça amb una pàgina web de l'anunciant.

Contrasenya o *password*. Clau d'accés secreta coneguda solament per l'usuari informàtic, que permet entrar a una computadora que està protegida mitjançant un sistema de seguretat.

Tallafocs o *firewall*. Literalment, mur de foc. Els tallafocs, com també se'ls coneix, són programes que estableixen barreres que impedeixen a un usuari extern l'accés al nostre ordinador i per tant a la informació continguda en ell.

Compte d'usuari. Quan algú utilitza un ordinador, se li pot assignar un compte. Juntament amb aquest van un nom d'usuari únic (*login name*) i una contrasenya (*password*).

Disc flexible. Unitat d'emmagatzematge externa. També anomenada disquet o *floppie*, té una capacitat d'emmagatzematge de 1.44MB.

Hoax: Correus amb informació falsa per fer que els usuaris reenviïn correus i així rastrejar les dades.

Malware. El mot *malware* prové d'una agrupació de paraules (*malicious software*). Aquest programa o arxiu, que és nociu per l'ordinador, està dissenyat per inserir virus, cucs, troians, *spyware* i, fins i tot, *bots*, intentant aconseguir algun objectiu, com podria ser la recollida d'informació sobre l'usuari o sobre l'ordinador.

Pegats de seguretat. Conjunt de programes o aplicacions que actualitzen o reparen falles del programari (sistema operatiu, ofimàtica, navegadors, per esmentar-ne alguns) que tinguem instal·lat en el nostre ordinador.

Pishing: estafa caracteritzada per intentar adquirir informació condifencial de manera fraudulenta (com pot ser una contrasenya o informació detallada sobre targetes de crèdit o una altra informació bancària).

Scam: missatges de correu electrònic en els que s'ofereix la possibilitat de guanyar grans sumes de diners (inversions a Nigeria, Loteries que no s'han comprat, herencies d'un familiar desconegut) que demanen algun desemborsament per part de l'usuari.

Spam. Correu electrònic no sol·licitat.

Spammer. Persona que roba o compra adreces de correu electrònic robades i remet missatges no sol·licitats. També és qui envia missatges als grups de notícies per a anunciar qualsevol producte o servei, sense importar-li si el seu missatge pot molestar o no a la resta de subscriptors.

Spyware. Programa espia.

Troià. Programa tipus virus que conté un codi nociu dintre de dades aparentment inofensives. Pot funcionar com un programa espia, però a diferència d'aquests, pot arruïnar part del disc dur.

Virus. Programes que "infecten" un ordinador i que poden causar efectes indesitjables o danys irreparables.

Macros. Es tracta d'un grup de comandaments d'una aplicació d'Office, organitzats segons un joc d'instruccions l'execució de les quals pot ser demanada. El seu ús elimina la realització de tasques repetitives, automatitzant-les. No obstant això, hi ha persones que utilitzen aquesta eina per a escriure subrutines amb ordres malicioses i nocives: tenim així els virus macros.

Scripts. Petits programes de comandaments que realitzen processos més o menys complicats i que fàcilment poden ser utilitzats per portar virus.