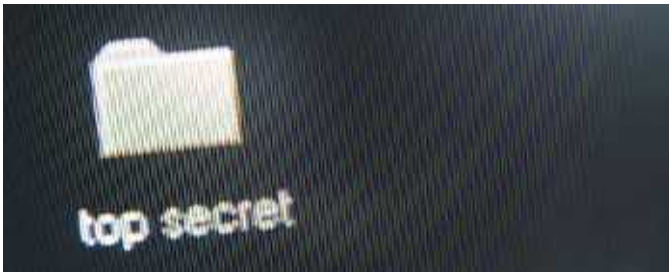
SEGURETAT: VIRUS, SPAM I ALTRES PERILLS

1. INTRODUCCIÓ

QUE HEM DE TENIR EN COMPTE

Un sistema segur ha de complir tres condicions: la confidencialitat, la integritat i la disponibilitat.

La confidencialitat vol dir que l'accés al sistema només es permet a persones autoritzades. La integritat significa que les modificacions que es facin a les dades o altres recursos del sistema, únicament poden ser realitzades per aquestes persones autoritzades. La disponibilitat implica que tots els recursos del sistema han d'estar a l'abast d'aquestes mateixes persones.



Imatge

2. QUE ÉS LA SEGURETAT

DE QUÈ HEM DE PROTEGIR AL NOSTRE ORDINADOR?

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 virus, nostre ordinador, provocada per terceres persones, spyware (programes espia), entre d’altres
- De falles en processos, emmagatzematge o transmissió de la nformació, 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.

3. ELS VIRUS

AQUESTS I LES SEVES VARIANTS

Per a poder assegurar-nos de que les comunicacions són segures, els navegadors Un virus informàtic és un programa que s'executa a l'ordinador tot utilitzant-ne el sistema operatiu. Tenen uns components bàsics:

- **L'agent infecciós**: És la part del virus que utilitza qualsevol vulnerabilitat del sistema per introduir-se a l'ordinador.
- **El duplicador**: Permet que el virus es copiï dintre de programes de l'ordinador o que s'enviï automàticament a través del correu electrònic.
- **El codi maligne**: És la part del virus que produeix el mal al sistema. S'activa en determinades situacions, com ara quan s'engega l'ordinador, quan s'executa un programa concret o quan s'arriba a una determinada data de l'any.
- Hi ha diversos tipus de virus. Cadascun utilitza un mecanisme diferent per estendre's i atacar. Entre els més habituals destaquen:
    - **Bombes lògiques**: S'activen quan es compleix una condició determinada, com quan s'arriba a una data en concret. El virus Divendres 13, s'activava cada dia 13 que coincidia en divendres.

- **Cucs**: Creen còpies de si mateixos i s'autoenvien a d'altres ordinadors connectats en xarxa (per exemple, via correu electrònic).
- **Troians**: Són programes que contenen un virus. Quan s'executa el programa, el virus s'estén i executa el seu codi maligne.
- **Exploits**: Aprofiten la vulnerabilitat del sistema operatiu, o dels programes, per infectar la resta de l'ordinador i expandir-se.
- **Virus polimòrfics**: Canvien de forma després de cada infecció; és a dir, canvien el seu codi maligne, el tipus d'arxius que ataquen, etc.
- **Virus ocults**: Una vegada s'han activat i han infectat un arxiu, romanen actius i eviten la seva detecció mitjançant l'enviament d'informació falsa.
- **Virus autoencriptats**: Són virus que encripten el codi maligne cada vegada que infecten un arxiu per tal de dificultar-ne la detecció.
- **Virus per correu**: Són virus que envien missatges a d'altres ordinadors per infectar-los.

4. PROGRAMARI MALICIÓS

El programari maliciós (spyware) és un programa espia que té l'objectiu d'obtenir informació sobre els nostres hàbits de navegació per Internet. Amb aquesta informació, ens poden enviar publicitat (finestres emergents), missatges no desitjats, o aconseguir dades confidencials.

Hi ha **dos tipus de programari maliciós**: Quan descarreguem un programa o un joc gratuït, podem instal·lar un programa maliciós al nostre ordinador sense saber-ho. És important llegir les pantalles prèvies abans de descarregar el programa, ja que a vegades ens informen que se'ns instal·larà un programari maliciós que ens omplirà l'ordinador de publicitat, com a forma de retribució per al creador del programa. Hi ha altres tipus de programari maliciós que s'instal·len al nostre sistema sense adonar-nos-en.

Alguns dels sistemes per protegir-nos dels virus i del programari maliciós són els antivirus i els programes antispyware (antiespia).

5. ANTIVIRUS

Un antivirus és un programa que presenta diverses funcions:

- Analitza el disc dur, o qualsevol suport d'emmagatzematge de l'ordinador, per tal de trobar arxius infectats per virus. El programa compara parts d'un arxiu amb els continguts d'arxius de virus coneguts. Per això és tan important mantenir actualitzat l'antivirus.

- Elimina els virus trobats. Segons com estigui configurat l'antivirus, el programa elimina el virus o el posa en quarantena.
- Evita que el virus estigui actiu.
- Analitza el correu electrònic.
- Analitza les pàgines web que es visiten quan naveguem per Internet.

Els antivirus es poden obtenir en línia, tot i que alguns d'ells són de pagament, i també les actualitzacions (programes com Norton o McAfee). Altres programes són gratuïts, especialment per a usuaris domèstics, com per exemple Avast!, AVG Antivirus o CLAM AV.

Per instal·lar un antivirus en línia, normalment s'ha de descarregar i executar l'arxiu setup.exe. Una vegada executat, apareixen diferents finestres (llicència, ubicació del programa, configuració, etc.) fins que el programa queda instal·lat.

És molt important mantenir actualitzat el programa. L'actualització es pot fer de forma manual o de forma automàtica, quan l'ordinador està connectat a Internet.

Normalment, els sistemes operatius de programari lliure pateixen menys problemes de seguretat que el sistema operatiu Windows.

6. ANTIESPIES

Els programes espies s'instal·len al nostre ordinador mentre naveguem per Internet, l'omplen de publicitat i obtenen dades nostres sense permís. Podem eliminar-los utilitzant un programa antiespia.

Imatge

Hi ha antivirus que porten aquesta funció incorporada. Alguns programes antiespies que es poden descarregar gratuïtament d'Internet són Ad-aware o Spybot.

El procediment per descarregar-los és el mateix que seguim amb els antivirus en línia.

7. TALLAFOCS

Un tallafoc és un programa que filtra i bloqueja les comunicacions en xarxa (per Internet o per xarxa local) no desitjades; és a dir, que protegeix la informació d'intrusions externes i optimitza l'accés per nivells als diferents programes i aplicacions que diversos usuaris d'un ordinador poden utilitzar.

El sistema operatiu Windows XP i qualsevol distribució de GNU/Linux inclou per defecte un tallafoc. La configuració permet activar-lo, amb excepcions o sense, o desactivar-lo.

La pestanya d'opcions avançades permet activar o desactivar el tallafoc per a una connexió en concret.

A la pestanya d'excepcions, podem seleccionar-hi els programes o serveis que no quedaran bloquejats pel tallafocs.

Quan s'utilitza un encaminador (router) per connectar-nos a Internet, també hem d'utilitzar un tallafoc.

8. CORREU BROSSA O SPAM

El correu brossa (SPAM en anglès) són els missatges enviats per un mitjà electrònic, indiscriminadament i massiva, sense el consentiment dels receptors. La seva finalitat generalment és comercial, amb missatges prenent forma d'anunci, tot i que també són freqüents els enganys amb intenció de treure profit econòmic de les víctimes. Tradicionalment els seus mitjans han estat el correu electrònic i els grups de discussió però amb popularització de noves tecnologies de comunicació electrònica l'spam hi ha saltat i el podem trobar en altres mitjans com blogs, wikis, fòrums i similars, missatgeria instantània, etc.

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

En l'actualitat, els proveïdors de correu gratuït més utilitzats com Gmail tenen un sistema antispam que funciona com a filtre, de tal manera que els correus considerats spam, s'envien a una carpeta per ser eliminats posteriorment.

Una altra manera per a 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.