**8.- AMENACES INFORMÀTIQUES:PROTEGIM ELS NOSTRES ORDINADORS**

Quan parlem de **seguretat en informàtica** ens referim a aquelles **mesures que podem prendre per evitar patir qualsevol mena d'acció malintencionada** contra el nostre ordinador. Des d'intentar robar-nos dades personals, omplir la nostra pantalla d'anuncis o danyar el nostre equip, aquestes accions són, sovint, portades a terme per programari maliciós, conegut genèricament com a virus. Aquests programes són difosos a través dels correus electrònics, enganxats en fitxers adjunts o amagats en un llapis de memòria USB, s'instal·laran en el nostre equip sense el nostre permís.

**8.1.- Les amenaces informàtiques: tinc un virus?**

Un virus informàtic és un programa que s'ha realitzat amb l'objectiu de modificar el funcionament normal d'un equip, sigui esborrant arxius, modificant el sistema operatiu o enviant dades personals als creadors del programa. Tot i que és l'amenaça informàtica més coneguda, sovint anomenem virus allò que no ho és. Farem servir la paraula ***malware*** per descriure a aquells programes maliciosos (de l'anglès ***mal****icious soft****ware***).

1. **Virus i cucs: malware infecciós**

Un **virus informàtic** és un programa que té com a objectiu **modificar el funcionament d'un ordinador**, **sense el coneixement de l'usuari/ària**. A l’executar aquest programa, aquest **es propaga infectant a altres programes**, de la mateixa manera que ho faria un virus biològic.

El funcionament d'un virus es basa en substituir els arxius executables d'un programa sa o del sistema operatiu per a altres infectats amb el seu codi, alterant el bon funcionament de l'equip. El seu objectiu pot ser el d'entorpir les tasques, però sovint poden amagar altres objectius com eliminar dades o fitxers vitals per al sistema operatiu.

Es denomina **cuc informàtic** el programa que és capaç de **duplicar-se a sí mateix**. El seu principal objectiu és el d'infectar a la major part d'usuaris/àries possibles, però també pot tenir objectius nocius.  
  
A diferència dels virus, **els** **cucs no modifiquen els arxius de cap programa**, sinó que s'allotgen en la memòria del sistema i es van duplicant. A la llarga, es detecten els cucs quan, a causa de la seva incontrolada replicació, **consumeixen els recursos del sistema**, fent que les tasques més habituals es tornin increïblement lentes.

Una altra diferència destacable entre cucs i virus és que el virus necessita la intervenció de l'usuari per propagar-se (cal que algú executi l'arxiu infectat), mentre que el cuc es propaga automàticament. Les infeccions trameses a través del correu electrònic, per tant, són virus (necessiten que s'obri el correu per executar-se).

1. **Malware que s'amaga: troians, rootkits i la porta del darrera**

Si el principal objectiu d'un *malware* és destruir parts dels sistema que ha infectat, quant més temps tingui per realitzar aquesta tasca més possibilitats tindrà per fer-la correctament. Amb aquest objectiu, hi ha diversos tipus de programari maliciós que intentarà mantenir-se invisible el màxim temps possible.

**El troià es presenta a l'usuari com si fos un programa legítim** i inofensiu que, al ser executat per l'usuari, modifica els sistema operatiu.

Pot desenvolupar diverses tasques, però la més comú és la d'obrir **portes del darrera** en el nostre ordinador, donant la possibilitats que un tercer usuari no autoritzat controli el nostre sistema operatiu o copiï les nostres dades personals (contrasenyes desades en el navegador, etc..).

Els **rootkits** ajuden també en aquesta tasca. Aquests són programes destinats a **esborrar qualsevol rastre deixat dintre d'un sistema infectat**, permetent que un *malware*es mantingui ocult a l'usuari. Per exemple, un rootkit evita que un procés maliciós fos visible en la llista de processos del sistema o que els seus arxius es mantinguin ocults en el navegador de fitxers, de la mateixa manera que pot contenir estratègies per evitar ser esborrat del sistema.

1. **Objectiu: fer diners**

Tot i que molts virus i cucs han estat creats com a simple exercici informàtic (per explorar les vulnerabilitats d'un sistema operatiu) la majoria estan fets amb l'objectiu de treure'n beneficis. Ja sigui amb fins publicitaris o amb voluntat d'obtenir il·lícitament dades personals, aquest programari buscarà traure el màxim profit del nostre ordinador.

Comencem per l'anomenat ***spyware***. El programari espia és un tipus de programa troià que s'instal·la a un ordinador amb l'objectiu de **recollir dades personals del seu propietari** i enviar-les a empreses publicitàries o altres institucions interessades. Les dades que acostuma a recollir són el correu electrònic, la llibreta de contactes, les pàgines web visitades, temps que s'ha passat l'usuari visitant-la, els fitxers que s'ha descarregat, i tota la informació que un usuari pugui intercanviar en una web: formularis web, números de targetes de crèdit i comtes de banc, contrasenyes...

En concret, el **keylogger** captura les pulsacions del teclat, el **stealer** intentarà fer-se amb la informació desada en els fitxers protegits del nostre sistema, on s'allotgen les contrasenyes o altres credencials privades.

Sovint, aprofitant la connexió a Internet, adjuntat en un correu electrònic o fent-se passar per programari legítim es pot instal·lar **adware**. Aquests programes s'executen automàticament i mostren missatges publicitaris, fent servir finestres emergents que dificulten l'ús de l'ordinador. En alguns casos, les versions gratuïtes de programes propietaris inclouen adware, per eliminar les molèsties que aquest causa cal fer-se amb la versió de pagament.

Alguns programes adware han rebut crítiques ja que recollien i feien seguiment de la informació personal de l'usuari, actuant com ho faria un spyware.

1. **També cal vigilar amb...**

Tot i que no entrin dintre de la categoria de programari maliciós, hi ha un seguit de **pràctiques que poden suposar un perill per als usuaris/àries d'ordinadors**, sobretot si no es tenen present les conseqüències que poden tenir.

* El **correu brossa**, conegut com **spam**, és una tècnica de venta directa consistent en fer enviaments massius de correus electrònics sense el consentiment de les persones que el reben.
* Els **hoax**, també dit falsa alarma o senzillament enganys. Aquests correus són la versió digital de les llegendes urbanes, històries en les que es **barregen referents reals amb ficcions per fer caure al lector en un engany**. Els més benignes poden senzillament demanar que reenviïs el correu, altres poden detallar instruccions precises perquè esborris un fitxer vital del sistema operatiu fent-te creure que és un virus.
* El **phishing** és una **estafa cibernètica** en què l'estafador intentarà aconseguir dades privades, com el número de la targeta de crèdit.., fent-se passar per membre de l'empresa fent servir una comunicació aparentment oficial.

1. **Defensem-nos!**

Aquests programes malintencionats aprofiten els forats del nostre sistema operatiu, sobretot les diferents versions de Windows fabricades per Microsoft. Aquest fet no vol dir que no existeixi malware per a Mac OS o GNU/Linux, però és molt minoritari. Sigui quin sigui els sistema operatiu que fem servir, convé que seguim els següents passos de protecció:

* **No fer servir l'usuari administrador del sistema** per a altres tasques que no siguin les d'administració. Crear usuaris per poder realitzar tasques del dia a dia.
* **Mantenir el Sistema actualitzat**.
* **Instal·lar un antivirus** actualitzat que ens ajudin a defensar-nos. Hi ha vàries opcions comercials que ens protegiran, però també podem fer servir les versions gratuïtes que acostumen a oferir menys prestacions, però protegiran igualment al nostre ordinador.
* [**Avast! Free Antivirus**](http://www.avast.com/es-ww/free-antivirus-download)
* [**AVG Antivirus**](http://free.avg.com/es-es/antivirus-gratis-avg).

Cal recordar que la principal defensa en matèria de seguretat informàtica està a les mans dels mateixos usuaris. Seguir unes senzilles **pautes** reduirà considerablement el nostre risc:

* Fer servir un **usuari sense permisos d'administració** en el nostre sistema operatiu.
* **Canviar la nostra contrasenya** del correu electrònic amb regularitat.
* **No obrir mai un fitxer enviat per correu electrònic** de remitent desconegut (acceptaries un caramel d'algú que no coneixes?)
* Comprovar que qualsevol arxiu nou no estigui infectat, **passant-hi l'antivirus**.
* Comprovar que el **nostre antivirus** estigui actualitzat.
* **No enviar les nostres dades personals per correu electrònic**, encara que ens ho estigui demanant una empresa de confiança.
* **Configurar el nostre navegador** perquè eviti les finestres emergents i denegui les galetes (cookies) de tercers.

I **mantén-te informat**! Trobaràs molta informació d'interès a les webs següents:

Centre de seguretat de la Informació de Catalunya <http://www.cesicat.cat>

Instituto Nacional de Tecnologías de la Comunicación. <http://inteco.es>

**ACTIVITATS**

1. Explica els següents conceptes:

|  |
| --- |
| **Virus informàtic** |
|  |
| **Cuc informàtic** |
|  |
| **Spyware** |
|  |
| **keylogger** |
|  |
| **adware** |
|  |
| **spam** |
|  |
| **hoax** |
|  |
| **phishing** |
|  |
| **antivirus** |
|  |

1. Llegeix el text següent i contesta les preguntes del final

## Addicció a les noves tecnologies: símptomes, causes i tractaments

## Què és l’addicció a les noves tecnologies?

L’addicció a les noves tecnologies és **una forta necessitat del subjecte per mantenir-se interactuant amb els aparells electrònics** que li permeten accés a Internet ja sigui per mitjà d’apps de telèfon intel·ligent o programes d’ordinador.

Sovint, a més de necessitar estar connectat a la web, el subjecte necessita d’aparells que compleixin uns paràmetres específics, de manera que li puguin oferir una experiència més completa, pel que fa als continguts als quals podria accedir.

## Símptomes d’aquest comportament addictiu

Hi ha tot un ventall d’addiccions, cadascuna amb les seves característiques i símptomes propis. **Totes representen una necessitat irracional de l’individu de tenir accés a alguna cosa o activitat**. Hi haurà diferències depenent de quin sigui el detonant del comportament addictiu del subjecte.

En el cas de l’addicció a les noves tecnologies, els símptomes seran els següents.

## 1. Necessitat compulsiva d’informació

Els subjectes que presenten aquest tipus d’addicció, senten una forta necessitat per estar informats constantment, sobretot pel que fa als temes relacionats amb el que resulta interessant en el seu cercle social.

## 2. Necessitat d’aparells tecnològics d’avantguarda

A mesura que l’addicció a les noves tecnologies es fa més intensa, al subjecte no en té prou amb satisfer la seva necessitat d’informació a través de qualsevol dispositiu, sinó que aquest **necessitarà d’un que li brindi els últims avenços teològics per sentir que satisfà la seva necessitat**.

## 3. Tendència a l’aïllament

Les persones que s’han tornat addictes a les noves tecnologies es tornen subjectes **relativament apartats del contacte social físic.** Això vol dir que poden socialitzar tranquil·lament per mitjà dels seus aparells, gràcies als seus perfils en xarxes socials, però la convivència personal els resulta una nosa.

## 4. Dependència tecnològica

Aquests subjectes centren tota la seva atenció i recursos en mantenir-se actualitzats respecte als avenços tecnològics, en tots els aspectes. Situació que representa **una limitació pel que fa a afrontar situacions fora del context de les pantalles**.

Per exemple, un addicte a la tecnologia pot ser molt eficient al moment de realitzar activitats per mitjà d’un aparell intel·ligent, però si cal que faci alguna cosa en un altre context el subjecte serà incapaç de fer-ho amb la mateixa eficàcia. En els casos més intensos d’aquesta addicció podria fins i tot ser incapaç de realitzar aquesta tasca sense ajuda de la tecnologia.

Qüestions:

1. Segons el text què s’entén per addicció a les noves tecnologies?

|  |
| --- |
|  |
|  |
|  |

1. Quins són els símptomes principals?

|  |
| --- |
|  |
|  |
|  |

1. Com creus que es podria evitar o disminuir?. Posa alguns exemples.

|  |
| --- |
|  |
|  |
|  |

1. Creus que tu tens aquest problema o presentes alguns dels símptomes?. Raona la resposta.

|  |
| --- |
|  |
|  |
|  |

1. Seguint l’exemple d’aquesta campanya publicitària, fes un anunci o eslògan, relacionat amb l’addicció a les noves tecnologies

