

Subvencionat per



Patrocinat per



En col·laboració amb



Agencia de Protección de Datos
de la Comunidad de Madrid



Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos



Projecte CLI - PROMETEO 2008/09

Manual Pràctic de 15 a 17 anys

Amb el suport del Ministeri d'Educació i les conselleries corresponents
d'Andalusia, Catalunya, Euskadi, Extremadura i Madrid.

Equip directiu de la CLI:

Junta Directiva de l'Associació

Equip de Direcció del Projecte CLI-PROMETEO:

Antoni Farriols, José Manuel Ferrer, José Carlos Vaquero

Assessoria Jurídica:

Carlos Valero, Jordi Bacaria, Lola Albo, Ernesto Quílez

Equip informàtic:

José Manuel Ferrer, Carlos Ramón Ferrer

Col·laboració especial en el disseny de vinyetes:

M.^a del Carmen Labarquilla

***Manuais de protecció de dades
del Projecte CLI-PROMETEO:***

Manual de 9-11 anys. Coordinació: Salustiano Asencio

Manual de 12-14 anys. Coordinació: Alberto Leal

Manual de 15-17 anys. Coordinació: Débora Caballero

Traducció i adaptació al català:

Agència Catalana de Protecció de Dades

Maquetació:

Web y Media Diseñadores, S.L.

Direcció del manual:

Comissió de Llibertats i Informàtica

Impressió:

Centro Especial de Empleo Ponce de León

Dipòsit legal: M-53404-2008

EDICIÓ PRIVADA

Copyright © 2008

Queda prohibida la reproducció total o parcial de l'obra sense el permís escrit de la Comissió de Llibertats i Informàtica.

La Comissió de Llibertats i Informàtica (CLI) és una associació que treballa activament en la defensa del dret fonamental a la protecció de dades de caràcter personal amb el ferm objectiu de conscienciar les persones, les empreses i les administracions de la seva importància.

Formen part de la CLI, a més a més de persones interessades, les organitzacions següents:

AI: Associació d'Internautes.

ALI: Associació d'Enginyers i Enginyers Tècnics en Informàtica.

APDHE: Associació Pro Drets Humans d'Espanya.

FADSP: Federació d'Associacions per a la Defensa de la Sanitat Pública.

UGT: Unió General de Treballadors.

Projecte CLI PROMETEO 2008/09

La CLI desenvolupa el projecte CLI-PROMETEO, que s'adreça a nens i nenes i adolescents per fomentar des de l'escola l'ús de les tecnologies de la informació i, alhora, conscienciar-los de la necessitat de la protecció de dades de caràcter personal.

Índex

Capítol	Contingut	Objectius	Activitats	p.
Introducció	Presentació del manual	Motivació		2
Capítol 1. El bon ús de l'ordinador (Internet) i del telèfon mòbil	Activitats que es poden fer i benefici que ens aporten	Valorar les possibilitats i els avantatges que tenen ambdues tecnologies	Proposta d'actuacions. Test d'addicció	3
Capítol 2. El mal ús d'Internet: problemes que puc tenir	La protecció de dades personals i la seva privacitat: aspectes tècnics	Saber quins són els procediments tècnics per afavorir la nostra intimitat	Eliminació d'historials, galetes (<i>cookies</i>), arxius, contrasenyes automàtiques	6
Capítol 3. 3.1. Compartir arxius: «l'atac dels virus»	Antivirus, bloquejadors de finestres emergents (pop ups), tallafocs. Evitar correus no desitjats (correus brossa, spams)	Conèixer les possibles invasions de la nostra privacitat i els mitjans per evitar-les	Modificació d'arxius: alteració d'imatges reals	8
3.2. Trobades amb persones desconegudes: a través de la xarxa (en línia) i reals (cites a cegues)	Trobades amb altres persones a través de la xarxa: els xats	Identificar els perills d'establir contacte amb persones desconegudes	Anàlisi d'imatges amb doble personalitat: la realitat enganya	13
3.3. Ciberassetjament o <i>ciberbullying</i>	-Què és? -On succeeix? -Com puc reconèixer-lo? Un cas real d'assetjament electrònic	Reconèixer els casos d'assetjament i saber actuar-hi en contra. Alguns consells	Debat: models de personalitat	15
3.4. Fraus per Internet: compres i tècnica de la pesca o <i>phishing</i>	La identitat electrònica	Prendre consciència de les precaucions necessàries per protegir la identitat	" <i>Phishing</i> ": estudi d'un cas real	18
Capítol 4. El correu electrònic	Configuració i precaucions	Aprendre a configurar-se un compte de correu electrònic amb les garanties necessàries	Configuració d'un compte de correu electrònic	22
Capítol 5. Els nostres drets com a ciutadans: protecció de dades personals	Conèixer els drets que ens emparen: dret d'accés, rectificació, cancel·lació i oposició de dades personals. Model de denúncia	Conèixer els drets sobre protecció de dades personals d'una manera activa	Exercici pràctic sobre un cas de denúncia a l'Agència Catalana de Protecció de Dades	24
Capítol 6. Resum i conclusions	Consells per a pares, mares, educadors, educadores i tutors legals			31

Introducció

DE QUÈ TRACTA AQUEST MANUAL?

Internet, el telèfon mòbil, l'MP3, l'MP4 i allò que formalment s'anomena tecnologies de la informació (TI) són recursos habituals en la vida de les persones joves com tu. Després d'un estudi que hem fet amb més de vuit mil estudiants d'edats compreses entre els 9 i els 17 anys, hem comprovat que els dediqueu bona part del vostre temps. Un 37 % de vosaltres heu afirmat que utilitzeu Internet cada dia. Però ho saps tot, sobre les tecnologies de la informació? En fas un bon ús? Saps tots els perills a què t'exposes quan et connectes a Internet? Aquest manual et vol respondre totes aquestes preguntes. Volem ampliar la teva informació i el teu coneixement sobre aquestes tecnologies, avisar-te dels possibles perills i donar-te les armes per defensar-te. A més, amb aquest manual volem conscienciar-vos de la importància de la protecció de les dades de caràcter personal (nom, cognoms, telèfon, adreça, DNI, fotos...). Són la nostra intimitat i l'hem de protegir. T'informarem sobre els teus drets i deures en aquesta matèria, perquè sàpigues fer un bon ús de les teves dades.

COM US HO EXPLICAREM?

El manual està dividit en diversos capítols que tenen l'estructura següent:

- **Contingut:** Aquí et donem tota la informació que necessites sobre el tema. Et sorprendrà la gran quantitat de coses que no sabem sobre les tecnologies de la informació.
- **Consells:** En aquest apartat trobaràs recomanacions i consells pràctics i tècnics per fer un bon ús de les tecnologies.
- **Activitat:** Al final de cada capítol t'oferim un petit joc per posar en pràctica el que has après.

Aquest manual està pensat perquè t'animis a llegir-lo i a fer les activitats amb els teus pares, tutors i professors. Junts aprendreu moltes coses i, a més, et podran explicar tot allò que no acabis d'entendre.

Al final del manual també s'inclou un apartat de consells per a pares, mares, educadors, educadores i tutors legals.

Capítol 1

EL BON ÚS DE L'ORDINADOR (INTERNET) I DEL TELÈFON MÒBIL

En aquest capítol et proposem una llista d'activitats que pots fer amb Internet i amb el telèfon mòbil, i t'expliquem els beneficis que et poden aportar. També et donem una sèrie de consells per fer un bon ús d'aquestes tecnologies i, finalment, et posem a prova: ets un addicte a les tecnologies de la informació? Comprova-ho fent el test que et proposem al final de cada capítol.

QUINES ACTIVITATS PODEM FER AMB INTERNET I AMB EL TELÈFON MÒBIL?

- **Informar-nos i aprendre.** Internet és una enciclopèdia gegant. Només cal que introduïm en qualsevol cercador d'Internet els conceptes que volem saber i obtindrem milers de resultats de la nostra cerca: esdeveniments històrics, curiositats, receptes, trucs, la biografia del nostre artista favorit...; la xarxa ens proporciona una quantitat infinita d'informació que ens ajuda a seguir aprenent.
- **Comunicar-nos.** Telegrames, cartes, felicitacions de Nadal... Sona antic, oi? Doncs fins fa poc temps no hi havia cap altra manera de comunicar-se. Ara gràcies a Internet i al telèfon mòbil podem parlar amb els nostres amics i familiars en qualsevol moment, és igual en quina part del món siguem. Aquest és sens dubte un dels grans beneficis de les tecnologies de la informació. A més, l'anonimat que ofereix Internet ens ajuda a perdre la timidesa i a relacionar-nos amb més facilitat. Podem conèixer gent de tot arreu del planeta i descobrir noves cultures i nous costums que també ens ajudaran a ser més tolerants. Els blocs o fòrums ens permeten expressar les nostres opinions sobre temes que ens agraden. En definitiva, aquestes tecnologies ens ajuden a relacionar-nos i socialitzar-nos.
- **Divertir-nos.** A la xarxa i al telèfon mòbil, hi trobem moltíssims jocs per entretenir-nos amb els nostres amics o sols. Ens ajuden a millorar les nostres habilitats, a posar a prova el nostre enginy i, sobretot, a divertir-nos!
- **Viatjar.** A més de poder tramitar les nostres vacances còmodament des de casa, hi ha programes genials que ens permeten visitar qualsevol lloc del món des del nostre ordinador: les piràmides d'Egipte, l'estàtua de la Llibertat o la torre Eiffel, sense moure'ns de la cadira!

CONSELLS PER FER UN BON ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ

Un percentatge molt alt de vosaltres dieu que utilitzeu Internet cada dia. Però ho feu d'una manera adequada? Et proposem una sèrie de consells i d'activitats perquè facis un bon ús de les tecnologies de la informació.

- 1. Temps.** És important que controlis el temps que passes davant de l'ordinador o amb el telèfon mòbil. Són eines molt útils però, com tot, cal utilitzar-les amb moderació. Entre les classes, els deures i altres activitats extraescolars, et queda molt poc temps d'oci. No t'oblidis de passar temps amb la teva família i els teus amics, llegir llibres o escoltar la teva música preferida. Així, fes comptes i organitza't bé. Hi ha temps per a tot!
- 2. Informació.** Vigila!, a Internet hi ha molta informació fiable i certa, però també n'hi ha molta de falsa. Abans de creure't tot el que la xarxa et diu, pregunta-ho a una persona adulta o contrasta la informació amb un llibre que tinguis a mà.
- 3. Diversió.** Fuig dels jocs que continguin qualsevol tipus de violència o que et puguin donar problemes!
- 4. Blocs, fòrums, xats...** Sigues sempre respectuós i tolerant amb les opinions dels altres. No insultis, ni amenacis ni facis res que pugui perjudicar altres persones. Diverteix-te i passa dels mals rotllos!
- 5. Compres:** Si has vist alguna cosa que t'agrada a Internet, consulta-ho amb els pares o una persona adulta responsable. No confiïs en les ofertes ni les promeses miraculoses: no existeixen!

ACTIVITAT. Ets addicte a les tecnologies de la informació?

La major part de vosaltres afirmeu que sempre que us connecteu a Internet us hi esteu més estona de la que us havíeu proposat. Però, saps si hi estàs enganxat? Esbrina-ho amb el test que et proposem. Quina d'aquestes respostes és la més semblant a la que donaries tu?

- Quantes hores al dia dediques a Internet?
 - A.** Menys d'una hora. Faig moltes activitats i gairebé no tinc temps per connectar-me a Internet.
 - B.** Entre dues i tres hores. M'agrada dedicar força temps del meu oci a connectar-me per parlar amb amics i també per buscar informació per a les classes.
 - C.** Més de quatre hores diàries. Quasi sempre estic davant de l'ordinador, jugant, parlant, buscant informació que m'interessa...
- Quants SMS acostumes a enviar amb el telèfon mòbil a amics i familiars en una setmana?
 - A.** Un o dos com a molt. Només envio SMS per a qüestions importants o moments especials.
 - B.** Entre tres i sis SMS. Acostumo a enviar algun missatge i a contestar els que m'envien.
 - C.** Més de set missatges a la setmana. Perdo el compte dels SMS que envio. Encara que vegi els meus amics cada dia, ens enviem missatges contínuament. M'encanta!

3. Com et sentiries si durant una setmana desapareguessin Internet i el telèfon mòbil?
- A. Puc aguantar una setmana i més temps sense Internet i el telèfon mòbil.
 - B. Se'm faria molt estrany, però una setmana passa de seguida!
 - C. No ho podria suportar! Quin avorriment! Com em comunicaria amb els meus amics? Seria molt dur...
4. Quan NO et connectes a Internet o el telèfon mòbil, què fas gairebé sempre?
- A. Faig esport, parlo amb la meva família, estudio, llegeixo...
 - B. Miro la tele o estudio.
 - C. Penso en l'hora de connectar-me, de mirar si m'han escrit un correu o han firmat en el meu bloc. Només tinc ganes de navegar!
5. Quan et connectes a Internet o utilitzes el telèfon mòbil, què fas gairebé sempre?
- A. M'hi estic el temps just per fer el que haig de fer, i si els meus pares em truquen o tinc altres coses per fer, ho deixo de seguida.
 - B. Em diverteixo i m'agrada navegar una estona, negocio amb els meus pares el temps que puc estar-m'hi i ho compagino amb altres activitats.
 - C. És el millor moment del dia. M'ho passo bé mentre sóc a Internet o utilitzo el telèfon mòbil. Si algú m'interromp o em diu que pari... m'enfado moltíssim!

SOLUCIONS

- **Majoria de respostes A: «Ni fu ni fa».** Ets una persona pràctica i creus que les tecnologies de la informació són sobretot eines que ens fan més fàcil la vida, però podries viure perfectament sense. Saps mil maneres alternatives de fer el que faries amb Internet o amb el telèfon mòbil.
- **Majoria de respostes B: «El punt mitjà».** «En el punt mitjà hi ha la virtut» és la frase que et defineix. Utilitzes les tecnologies de la informació d'una manera moderada i no deixes de fer altres coses com estudiar o estar amb la teva família. Molt bé! Les tecnologies de la informació són molt útils i pràctiques, però no hem de deixar que es converteixen en una obsessió. No canviïs!
- **Majoria de respostes C: «Totalment enganxat!».** Has d'anar amb compte. No donis prioritat en la teva vida a Internet o al telèfon mòbil. Mentre et connectes, deixes de banda la relació amb la teva família o els estudis, i això pot tenir conseqüències greus. Has de reduir l'ús d'aquestes tecnologies i dedicar el temps que guanyaràs a fer esport, parlar amb els teus pares, llegir o estudiar.

Capítol 2

EL MAL ÚS D'INTERNET: PROBLEMES QUE PUC TENIR

LA PROTECCIÓ DE LA NOSTRA INTIMITAT: ALGUNS CONSELLS TÈCNICS

Tal com hem vist, Internet té moltíssims avantatges, però també és ple de perills i riscos. Quan sortim al carrer, vigilem que no ens prenguin la cartera o el moneder on portem tota la nostra documentació, totes les dades que ens identifiquen, com el DNI, les nostres fotos, aquella entrada del nostre concert preferit... En definitiva, protegim la nostra intimitat. Per què no fem el mateix a Internet? Les dades de l'estudi que hem fet revelen que la major part de vosaltres sabeu si el vostre ordinador està protegit per antivirus o antiespies. Però, encara que en la tranquil·litat de la nostra habitació, ens sentim a recer del món, en el moment en què el nostre ordinador es connecta a la teranyina mundial que és Internet estem totalment desprotegits, exposats a milions de riscos que poden tenir conseqüències greus si no prenem les mesures oportunes.

EL TEU ORDINADOR: «UN ROBOT CLASSIFICADOR»

El teu ordinador ho anota tot, guarda totes les pàgines webs que has visitat, les pel·lícules i la música que has baixat, les cerques que has fet a Google o Yahoo, el teu correu electrònic, les dades que has emplenat en un formulari d'inscripció, les teves contrasenyes, les teves converses del programa de missatgeria instantània..., tot! No oblida mai res si no és que tu li ho dius i, encara pitjor, qualsevol que tingui uns coneixements mínims d'informàtica podrà saber-ho tot sobre tu i utilitzar les teves dades d'una manera inapropiada. Però anem a pams: el teu ordinador ho té tot classificat i guardat en llocs diferents; abans de donar-te uns quants consells informàtics perquè estiguis protegit dels lladres de dades, veurem què es guarda a cada lloc:

- **Historial:** És on s'emmagatzemen la majoria de pàgines web que has visitat. Són algunes de les «traces» que vas deixant per la xarxa. Convé esborrar-les perquè ningú no les pugui seguir.
- **Galetes (cookies, empremtes):** Són arxius que contenen l'adreça de la pàgina que acabes de visitar. Algunes són temporals, però d'altres poden quedar-se molts anys dins del teu ordinador. A través de les galetes, els espies poden fer un seguiment de les pàgines web que has visitat i accedir als teus arxius per saber quins són els teus gustos i les teves preferències, amb l'objectiu de configurar llistes de possibles clients que després venen a empreses comercials. És important que les vagis eliminant de tant en tant.
- **Arxius:** Les imatges i els continguts de les pàgines web que has visitat s'emmagatzemen a l'ordinador per accelerar la càrrega de les pàgines quan tornes a visitar-les, però a partir d'aquests arxius es pot accedir a les dades que has escrit

a les pàgines web que has visitat. Quan esborris aquests arxius trigaran una mica més a baixar les pàgines que revisitis, però estaràs protegit dels espies i els lladres informàtics.

Ara ja saps què guarda el teu ordinador i on ho guarda. T'aconsellem que de tant en tant, com a mínim un cop la setmana, dediquis cinc minuts a esborrar totes aquestes dades que es queden al teu ordinador, per evitar que els lladres de dades envaeixin la teva intimitat. Com? Continua llegint i podràs estar protegit amb quatre passos molt senzills. Si tens l'última versió d'Internet Explorer (v. 7) és molt fàcil: només has d'obrir una pàgina d'Internet i seleccionar «**Herramientas** > **Eliminar el historial de exploración**» i t'apareixerà un quadre com aquest:

En aquesta finestra pots eliminar l'historial, les galetes, els arxius i les contrasenyes simplement seleccionant eliminar en cada opció i després confirmant la teva decisió.

Si tens el Windows XP i la versió anterior d'Internet Explorer, els passos que has de fer també són molt simples. Obre també una pàgina d'Internet i selecciona «**Herramientas** > **Opciones de Internet**», fes un clic a la pestanya «**General**», selecciona «**Eliminar el historial**», les galetes o els arxius i després fes clic a «**Aceptar**».

Per esborrar el teu historial amb Firefox 7.x, fes el següent: «**Editar** > **Preferencias**», fes clic al Navigator, selecciona «**Historial**» i clica a «**Borrar historial**». El procés per esborrar les galetes és semblant: selecciona «**Herramientas** > **Gestor de cookies** > **Gestionar cookies guardadas**» i al quadre que apareixerà podràs seleccionar quines còpies vols esborrar o fer clic al botó «**Eliminar todas las cookies**» i «**Aceptar**». Per eliminar els arxius amb Firefox 7.x, selecciona «**Editar** > **Preferencias**» i fes un doble clic sobre «**Avanzadas**». Selecciona «**Caché**» i fes clic a l'opció «**Vaciar caché de disco**».



Capítol 3

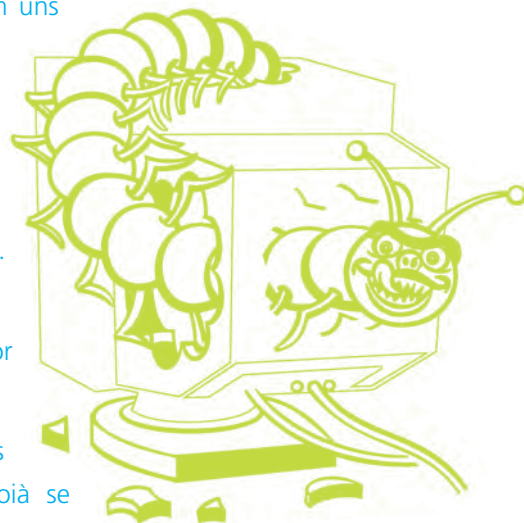
3.1. COMPARTIR ARXIUS: «L'ATAC DELS VIRUS»

Ara ja saps com funciona el teu ordinador, però encara no estàs protegit i tens una nova missió: no deixar que es converteixi en un *zombi* manipulat per estranys i protegir-lo de tots els perills que hi ha a Internet. Encara no saps els noms d'aquests atacants? A continuació et donem tota la informació que necessites sobre aquests malfactors i els escuts que et calen per estar protegit:

VIRUS

A Internet n'hi ha una plaga i, encara que et sorprengui de saber-ho, també n'hi ha al telèfon mòbil. Són programes informàtics que es propaguen amb una gran facilitat i que són molt perjudicials. A vegades es manifesten i sabem que hi són, però molt sovint s'amaguen en arxius o programes que es baixen i que poden destruir les dades del teu ordinador, sostreure'n les teves dades personals, les teves fotos... En definitiva, que poden manejar el teu ordinador en lloc teu, convertint-lo en un *zombi*. Hi ha una gran varietat d'aquests virus; te'n donem uns quants noms perquè estiguis alerta:

- **Stealth:** És un dels pitjors, ja que se't fica dins de l'ordinador sense que te n'adonis i infecta tot el que hi troba. Fins i tot enganya l'antivirus, tot modificant les dades perquè no el pugui detectar.
- **Paràsit:** Pot estar ocult en aquells programets en què ens diuen «Executar». Et sona, oi?
- **Cuc:** Es propaga amb moltíssima facilitat, ja que es transporta d'un ordinador a un altre per mitjà del correu electrònic o la missatgeria instantània.
- **Cavall de Troia o troià:** S'amaguen darrere d'alguns programes que ens baixem pensant que són inofensius. Un cop baixat el programa, el troià se t'introdueix a l'ordinador i pot fer-hi tot el que vulgui.
- **Cabir, el virus del telèfon mòbil:** Viatja a través del Bluetooth. Si entra dins el teu telèfon mòbil, en pot extreure els teus missatges de text o contactes, seguir els teus moviments o escoltar les teves converses. Vés amb compte quan utilitzis el Bluetooth, i no acceptis arxius de gent que no coneguis.



ESCUTS PER DEFENSAR-TE DELS VIRUS

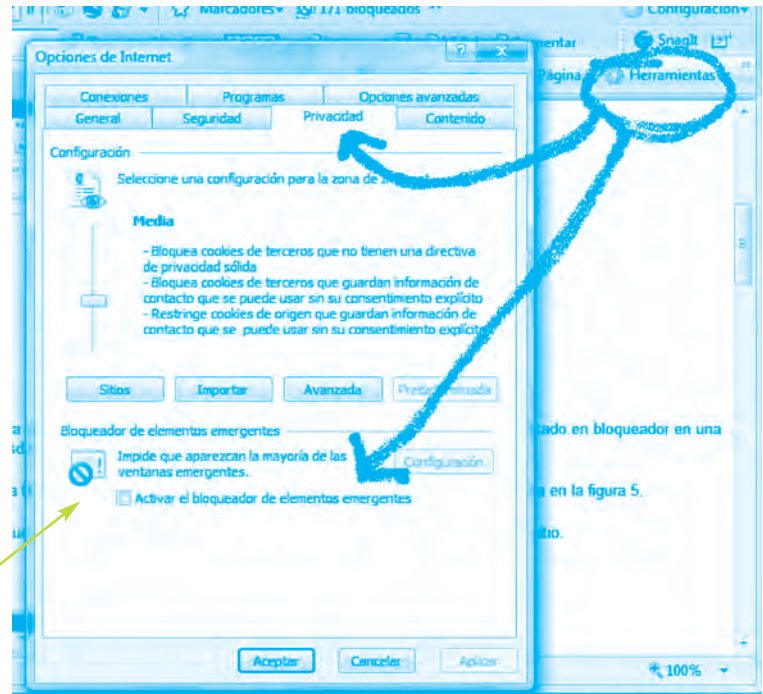
- **Antivirus:** És molt important que tinguis instal·lat un antivirus al teu ordinador. Aquests paquets informàtics són com els nostres guardaespalles, que sempre estan alerta davant de possibles programes perjudicials que se'ns poden introduir a l'ordinador i utilitzar les dades i els arxius que hi tenim guardats. Per això, perquè estiguis més segur, et recomanem que sempre tinguis un antivirus instal·lat. A més, recorda't d'actualitzar-lo periòdicament, perquè aquests paquets tenen una caducitat i en el moment en què passi la data tornaràs a estar en perill.
- **Tallafocs o firewall en anglès:** Aquest tipus de programes són el porter del teu ordinador; ningú no hi pot entrar sense que ell li doni permís per fer-ho. T'avisava de programes que poden actuar en perjudici del teu ordinador i et fan invisible davant dels possibles lladres que cerquen víctimes. En alguns webs trobaràs tallafocs que et pots baixar gratuïtament; és molt recomanable que t'instal·lis un d'aquests porters.

RECORDA

Consulta sempre els teus pares o tutors a l'hora d'esborrar qualsevol document, galeta o historial de l'ordinador per evitar un mal major, i també quan instal·lis un antivirus o un tallafocs.

FINESTRES EMERGENTS O POP-UPS

Un altre risc d'Internet són les maleïdes finestretes de publicitat que de vegades surten en una pàgina web que intentem llegir. No ens deixen navegar tranquil·lament, fan que la nostra connexió sigui més lenta i ens porten a altres pàgines que no volem visitar mentre intentem tancar-les desesperadament. Són les anomenades finestres emergents (*pop-ups*). Si vols eliminar per sempre aquestes finestretes tan molestes, segueix aquests passos: obre una pàgina web, vés a «**Herramientas > Opciones de Internet**», clica la pestanya de «**Privacidad**» i activa la casella del «**Bloqueador de elementos emergentes**». Algunes versions d'Internet Explorer inclouen aquesta opció directament a «**Herramientas**».



- També pots aconseguir un programa bloquejador de finestres emergents, que revisa periòdicament els programes que s'han instal·lat al teu ordinador sense que tu ho sàpigues i que t'atabalen amb les finestres emergents. Així estaràs totalment segur que no et tornaran a molestar!

CORREUS BROSSA O SPAMS

Com el seu nom indica són escombraries i, per tant, no els has d'obrir mai. Generalment són correus amb finalitat comercial, però en molts altres casos són portadors de virus, troians o cucs, que poden fer malbé l'ordinador, agafar-ne dades o portar-nos molts maldecaps.

- Com els podem identificar? Alguns servidors de correu electrònic ens avisen que el missatge pot ser un correu brossa, però la majoria de vegades no ho fan. Normalment són de persones que no coneixes i amb assumptes com ara:
 - «Guanya milions amb el mínim esforç»
 - «L'amor de la teva vida t'està esperant»
 - «Problemes? Des d'avui s'han acabat»

Però no te'n refiïs! Hi ha la possibilitat que rebis un correu brossa des de l'adreça d'un amic o conegut, del teu banc, d'alguna institució que coneguis, fins i tot des de

la teva pròpia adreça electrònica informant-te que el teu missatge no ha arribat al destinatari.

En aquests casos, el missatge ve amb un arxiu adjunt; no l'obris! Segueix la segona regla d'or de la informàtica: «Davant del dubte, esborra».

Els *spammers* (gent que envia correu brossa) s'aprofiten de la nostra curiositat o del desig de solucionar els nostres problemes, amb la intenció d'introduir-nos un virus i poder controlar el nostre ordinador convertint-lo en un *zombi*. Et recomanem que estiguis sempre alerta i no et refiïs de cap correu abans de contrastar que ve d'un lloc fiable.

- Com arriben fins al meu correu? Els *spammers* poden aconseguir la teva adreça de correu de diverses maneres.
 - Vas escriure la teva adreça per participar en un fòrum o per enregistrar-te en una pàgina web.



- Quan et vas apuntar a una pàgina, vas acceptar de rebre correu brossa sense ni tan sols estar-hi d'acord.
- Potser un amic ha inclòs la teva adreça en una d'aquestes pàgines web que et demanen que reenviïs a d'altres amics.
- Han trobat la teva adreça en bases de dades d'empreses o institucions privades.
- Potser has estat víctima d'un atac dels *spammers*, que es dediquen a crear adreces de correu a l'atzar.
- Com puc desfer-me del correu brossa? Per desgràcia, no hi ha manera de desfer-nos d'aquests molestos correus, però sí que podem donar-te una sèrie de consells pràctics per evitar-los:
 - Si els correus brossa t'envaeixen contínuament, crea un nou compte de correu electrònic.
 - Obre un altre compte secundari que et serveixi per enregistrar-te a les pàgines web i fòrums.
 - Posa un nom complicat al teu compte, que inclogui números, guions..., com per exemple *noves467technologies9_@protegeixte.com*, perquè et farà més resistent als programes de cerca automàtica d'adreces.
 - No t'enregistris ni donis les teves dades a les pàgines que puguin constituir un risc per a la teva seguretat.

ELS 10 MANAMENTS DEL GUERRER INFORMÀTIC

1. Instal·laré i actualitzaré un antivirus i un tallafocs.
2. No baixaré ni executaré arxius adjunts sense verificar abans si el remitent és de confiança.
3. No m'enregistraré ni introduiré les meves dades en pàgines insegures.
4. No baixaré programes de procedència desconeguda, perquè podrien estar infectats i portar virus al meu ordinador.
5. Davant del dubte... esborraré! Qualsevol correu que em faci desconfiar, l'esborraré immediatament.
6. No enviaré ni penjaré les meves fotos. Podrien utilitzar-les altres persones, violant la meva intimitat.
7. No em deixaré enganyar ni seduir per correus que em prometin miracles.
8. Aniré amb compte a l'hora de compartir el meu llapis de memòria USB (*pen drive*) i passaré sempre l'antivirus. Fins i tot els nostres amics ens poden encomanar un virus que tinguin al seu ordinador quan compartim aquests utensilis.
9. No obriré ni enviaré missatges cadena. Només es tracta de tècniques utilitzades pels pirates informàtics per recol·lectar més i més adreces i fer de les seves.
10. No faré res que pugui ocasionar algun d'aquests problemes a d'altres persones.

MODIFICACIÓ D'ARXIUS: ALTERACIÓ D'IMATGES REALS PER QUÈ NO HAS DE PENJAR LES TEVES FOTOS A INTERNET?

Si penges les teves fotos a Internet, qualsevol persona hi pot accedir i manipular-les tant com vulgui per ridiculitzar-te, amb tots els problemes que això comporta. Mira què li ha passat a aquest pobre noi.

* Aquesta és la foto original que va penjar a Internet



* Això és el que van fer amb la foto...

Font: www.youtube.com

ACTIVITAT. Endequina el final de la història

Et proposem un joc: endequina el final d'aquesta història basada en un fet real. Llegeix atentament i escull un dels tres possibles finals. No facis trampes, i no llegeixis la solució fins al final!

Karl Schofield, anglès, de 39 anys i enginyer de telecomunicacions, és detingut i arrestat per un delictes de pornografia infantil. La policia ha trobat al seu ordinador 14 fotos pornogràfiques de menors. S'enfronta a una condemna de deu anys de presó per cada foto trobada, és a dir, 140 anys darrere les reixes.

Quin creus que és el final de la història?

Opció A: Karl Schofield és condemnat a la presó, perquè si han trobat aquestes fotos al seu ordinador és que ell se les ha baixades. No pot ser de cap altra manera, per tant a la presó!

Opció B: El condemnen i el tanquen a la presó, però al cap d'uns quants anys un dels seus millors amics confessa que va ser ell qui va posar les fotos a l'ordinador del Karl, per venjar-se d'un antic conflicte que van tenir.

Opció C: Karl Schofield és innocent i no va a la presó, ja que els seus advocats poden demostrar que aquestes fotos pornogràfiques les va col·locar al seu ordinador un cavall de Troia.

SOLUCIÓ

Has escollit la darrera opció? Doncs l'has encertada! Karl Schofield era totalment innocent. Ell no es va baixar mai aquestes fotos, sinó que va ser víctima dels pirates informàtics. Els seus advocats van aconseguir demostrar que al seu ordinador s'hi

havia instal·lat un cavall de Troia des d'on s'havien baixat les fotos, sense que el propietari de l'ordinador ho sabés, per mitjà del seu correu electrònic o en acceptar de baixar algun altre arxiu. El Karl se'n va poder sortir, però va perdre la feina i va passar dos anys horribles fins que es va saber la veritat. Així doncs, pren-t'ho seriosament i protegeix-te quan et connectis a la xarxa!

(Cas real extret de la notícia «Trojan horse defence results in child porn acquittal». Font: <http://www.out-law.com> 25/04/2003)

3.2. TROBADES AMB PERSONES DESCONEGUDES: A TRAVÉS DE LA XARXA (EN LÍNIA) I REALS (CITES A CEGUES)

En l'estudi que hem fet, observem que un dels principals usos que feu d'Internet i el telèfon mòbil és el contacte amb altres persones a través dels xats, missatges de telèfon mòbil o missatgeria instantània: el 65,7 % de vosaltres dieu que feu servir els xats per conèixer gent nova, a més del 69,5 % que ho feu enviant missatges curts de telèfon mòbil. Per això volem que sàpigues quins són els beneficis i els riscos que comporta establir relacions amb persones desconegudes.

TROBADES AMB ALTRES PERSONES A TRAVÉS DE LA XARXA: ELS XATS

El món ha canviat i les maneres de relacionar-se també. Abans els nostres amics eren els que fèiem a l'escola, a l'institut, a la discoteca o al lloc on estiejàvem, però ara podem tenir amics a l'Argentina sense haver de sortir de la nostra habitació. Els xats i les comunitats virtuals, definits com a converses en línia i en temps real que s'estableixen entre dues o més persones, els fan servir gent de totes les edats i condicions socials, ja que aporten molts beneficis:

- Tens companyia sempre que vols. Només t'has de posar un àlies (*nickname*) i entrar en un xat per estar connectat amb milions de persones de tot el món.
- Enriqueixes el teu coneixement d'altres cultures i costums, cosa que et fa més tolerant amb les persones que són diferents.
- L'anonimat que proporcionen els xats t'ajuda a superar la timidesa i possibles complexos, i t'és molt més fàcil establir relacions amb altres persones.



ÉS IMPORTANT QUE IDENTIFIQUIS ELS PERILLS D'ESTABLIR CONTACTE AMB PERSONES DESCONEGUDES I QUE SÀPIGUES ACTUAR

No tothom té bones intencions a Internet, per això has d'anar amb molt de compte. No te'n refiis!

- Les persones amb qui parles per Internet et poden mentir sobre la seva edat, el seu aspecte físic o la seva professió. Fins i tot poden enviar-te una foto que no és real. No et deixis enganyar!
- Algunes d'aquestes persones poden ser molt més grans que tu i tenir males intencions. El 95 % dels pederastes (persones majors d'edat que abusen sexualment de menors) coneixen les seves víctimes a través dels xats.
- A Internet és molt fàcil mentir i amagar que ets un altre tipus de persona. Normalment et tractaran amb una amabilitat excessiva, et diran coses boniques encara que ni t'hagin vist, et prometran portar-te a llocs on els teus pares no et deixen anar com un concert o una discoteca... No et creguis tot el que et diuen.
- La majoria et demanarà de veure't per la càmera web, fins i tot et poden rebutjar si no ho fas. Intentaran convèncer-te que facis el que volen veure. No et deixis convèncer i no acceptis cap videoconferència amb persones estranyes.
- És molt probable que et demanin fotos o dades personals, com la teva adreça o la zona on vius. No enviïs mai les teves fotos ni donis les teves dades personals a ningú.
- No acceptis arxius de persones que coneixes del xat, perquè podrien incloure algun dels virus dels quals t'hem parlat i copiar les teves fotos i dades personals. Fins i tot les cançons o les fotos que t'envien poden ser perilloses.
- No quedis amb persones que coneguis a la xarxa. La majoria de vegades, aquest tipus de cites són un fracàs. En els casos més lleus, la persona no és físicament com deia que era, però també hi ha la possibilitat que sigui una persona depravada i que intenti abusar de tu.
- Parla amb els teus pares o tutors de les relacions que estableixes per Internet. Ells sempre miraran pel teu bé i et podran orientar millor sobre la classe de persona que has conegut.
- Si et saltes tots aquests consells i decideixes quedar amb una d'aquestes persones que vas conèixer per Internet, no hi vagis mai sol/sola! Convenç el teu grup d'amics i aneu-hi tots junts.

ACTIVITAT. Anàlisi d'imatges amb doble personalitat: la realitat enganya

A vegades la realitat no és el que sembla. Per això et proposem aquest senzill joc que demostra que la realitat enganya. Què hi veus, a cada imatge? Hi pots veure les dues personalitats? Trobaràs les solucions al final de la pàgina.



SOLUCIONS

Imatge A: Pots veure-hi una vella i una jove de perfil. (El nas de la vella és la mandíbula de la jove.)

Imatge B: Hi pots veure un trompetista i la cara d'una dona.

Imatge C: Segons com miris aquesta imatge, hi veuràs un conill o un ànec. (Les orelles del conill són també el bec de l'ànec.)

Imatge D: En aquesta imatge veuràs, de color negre, un gerro, i de color blanc, dues cares què es miren.

D'aquí en pots treure una lliçó. Has aconseguit veure les dues personalitats a cada imatge? Això només és un exemple de com la realitat et pot arribar a enganyar. Amb les persones que coneixem als xats ens pot passar el mateix: que es disfressi de jove però en realitat sigui una vella, o que hi vegis un saxofonista (imatge B) però al darrere hi hagi la cara d'una dona. Sigues sempre molt prudent i no confiïs en tot el que et diguin: ja has pogut comprovar que la realitat, de vegades, enganya.

3.3. CIBERASSETJAMENT O CIBERBULLYING

Amb el nostre estudi hem detectat que un 21,9 % de l'alumnat enquestat reconeix haver rebut alguna vegada insults o comentaris violents o racistes a través de la xarxa. Això pot ser el principi d'un assetjament, que quan es fa a través de les tecnologies de la informació s'anomena ciberassetjament (ciberbullying). És un tema que ens preocupa molt i per això en aquest capítol procurarem apropar-te una mica més a la trista realitat del ciberassetjament. T'explicarem en què consisteix i et donarem algunes claus perquè sàpigues reconèixer-lo si arriba el cas, i uns quants consells perquè sàpigues que has de fer aleshores.

QUÈ ÉS?

És l'ús d'Internet, el telèfon mòbil o els videojocs per humiliar, agredir, maltractar, difamar, insultar, amenaçar o desprestigiar companys o persones conegudes d'una edat semblant.

ON SUCCEIX?

Podem trobar ciberassetjament en xats, fòrums, SMS, blocs, fotoblocs, jocs en línia, videojocs virtuals, el nostre espai o converses de missatgeria instantània, o fins i tot podem ser-ne víctimes sense adonar-nos-en mentre algú fa servir els seus coneixements informàtics per introduir-se al nostre ordinador i manipular la càmera web, copiar dades i contrasenyes o fotos.

COM EL PUC RECONÈIXER?

A continuació et posem alguns exemples concrets de ciberassetjament perquè puguis identificar-lo:

- **Fotos.** Utilitzen les fotos que algunes persones tenen penjades a Internet, ja sigui al seu espai personal o al fotobloc, o fins i tot les que els prenen els troians o virus. Després manipulen i exposen aquestes fotos a Internet per avergonyir i humiliar les seves «víctimes». A vegades les exposen en webs en què es vota la persona més lletja o la més totxa, carregant el seu perfil de punts i fent que aparegui en les primeres posicions d'aquest rànquing. Altres vegades les utilitzen com una arma per xatejar amb la seva víctima i amenaçar-la que ensenyaran la foto en qüestió si no fa el que li diuen.
- **Suplantació de la personalitat.** Amb les dades d'una altra persona editen perfils o pàgines web amb comentaris ficticis sobre les seves experiències sexuals, manies o qualsevol altre comportament per fer-ne burla. Es fan passar per aquesta persona en fòrums i pàgines on escriuen opinions que ofenen altres persones o comentaris violents que provoquen la seva expulsió immediata de la pàgina i que no pugui tornar a accedir-hi.
- **Amenaces.** Se serveixen d'SMS, correus electrònics o vídeos per amenaçar i insultar la seva víctima.
- **Atac a la intimitat.** S'introdueixen dins del correu electrònic per manipular-lo, llegir els missatges i registrar la persona que n'és propietària en pàgines on pot ser víctima de correus brossa o de virus informàtics.

SABER ACTUAR

Si has identificat alguns d'aquests símptomes al teu entorn, et donem uns quants consells perquè sàpigues com has d'actuar i aturar aquest assetjament.

- Comenta-ho amb els teus pares o professors. Ells són persones adultes i t'ajudaran a trobar més ràpidament una solució.
- Sigues sempre molt prudent amb les teves dades personals i les teves fotos, ja que no saps mai quin ús poden fer-ne. Com menys persones les coneguin, millor!
- Pots buscar el teu nom i cognoms o els teus sobrenoms en qualsevol cercador d'Internet per comprovar si algú ha suplantat la teva personalitat o ha utilitzat les teves dades personals per perjudicar-te.
- Guarda totes les proves de l'assetjament, els missatges de text, els correus electrònics, els vídeos o les converses de missatgeria instantània.
- Demana l'ajuda d'especialistes en informàtica per identificar el ciberagressor.

UN CAS REAL DE CIBERASSETJAMENT

Per completar la informació que tens sobre aquesta forma d'assetjament, t'exposem una notícia real d'un cas de ciberassetjament. Llegeix atentament la notícia i no oblidis de seguir els nostres consells i denunciar el cas si tu o algú del teu entorn n'és víctima.

Arriba l'e-bulling: Xantatge a companys de classe per la xarxa

“La Guàrdia Civil ha detingut dos escolars de 17 anys a Crevillent (Alacant) que havien inventat una manera molt curiosa de fer xantatge als seus companys. Els dos menors van crear un troià (virus informàtic) capaç d'activar les càmeres web dels ordinadors a casa dels seus companys, i els gravaven sense que ho sabessin en situacions compromeses (com ara desvestint-se a l'habitació). Després els amenaçaven de difondre les imatges a l'escola si no els pagaven els diners que els demanaven, «entre 100 i 200 euros», segons els agents de la Guàrdia Civil.

Falsificació de targetes

Els dos menors tenien molts coneixements informàtics i van ajudar dos joves més, majors d'edat i que han estat detinguts a Madrid, a falsificar targetes de crèdit i fer compres il·legals per Internet. Van arribar a fer estafes per valor de 60.000 euros.”

Font: www.20minutos.es 03/08/08

ACTIVITAT

- Debat: *Ciberassetjament* i models de personalitat

Anima els teus professors i companys o a la teva família a casa a fer un debat sobre el *ciberassetjament* i els models de personalitat. Escolliu un moderador i seguïu el guió que us proposem tot seguit:

- Qualsevol persona pot ser víctima de ciberassetjament, o només les persones més dèbils i insegures?
- Quin creieu que és el perfil del ciberagressor? Us plantegem dues opcions:
 - Un company amb el qual estàs bé, que és popular, fa esport i treu bones notes a classe.
 - Un company que treu males notes, sovint busca baralles, no està bé gairebé amb ningú i falta molt a classe.
- Una persona que assetja un company és un malalt, o una mala persona que només vol divertir-se fent mal als altres?
- Creieu que si algú és víctima de *ciberassetjament* ho ha de denunciar i explicar als seus pares, o ha de callar i esperar que passi?
- Quin tipus de condemna posaríeu a un ciberagressor? Una pena lleu considerant que segurament és un malalt que necessita ajuda, o una pena més dura?

3.4. FRAUS PER INTERNET: COMPRES I TÈCNICA DE LA PESCA O PHISHING

Una altra manera que tenen els pirates informàtics d'apropiar-se la teva identitat és per mitjà dels fraus i les estafes, cosa que en argot cibernètic s'anomena pesca o *phishing*. En l'enquesta, un 38,7 % de vosaltres reconeixeu que freqüentment rebeu publicitat no desitjada, és a dir, que no heu sol·licitat i que es fica al vostre correu per intentar vendre els seus productes. Això pot ser el començament d'una estafa o pesca. Així doncs, continua llegint i aprèn com pots reconèixer la pesca i quines precaucions has de prendre per no ser-ne víctima.

3.4.1. IDENTITAT ELECTRÒNICA. TÈCNICA DE LA PESCA O PHISHING

Identitat electrònica:

- **Què és?** Són les teves dades personals, tot el que diu alguna cosa de tu, que et diferencia de la resta de persones en edició digital: el teu nom i cognoms, la teva adreça, el teu DNI, el número de la targeta de crèdit, el telèfon, la data de naixement, les teves fotos, la teva agenda, les teves contrasenyes...
- **Com arriba la teva identitat a Internet?** Segur que més d'una vegada per poder utilitzar serveis d'Internet t'han demanat que t'enregistris, la qual cosa implica emplenar formularis interminables on no tan sols et demanen les dades personals, sinó que, a més, et fan preguntes sobre les aficions que tens, els gustos, la ideologia, la religió, el grup ètnic o la vida sexual. Així és com arriben les teves dades a Internet. Sense que te n'adonis, ets tu qui les proporciones. Vés amb molt de compte.
- **Per a què?** No sempre tota la informació que dones lliurement en aquests qüestionaris o formularis s'utilitza amb una finalitat correcta. En alguns casos, volen les teves dades per fer-les servir amb finalitats comercials. És fàcil: saben moltes coses sobre tu i, per tant, saben què et poden vendre i com ho han de fer. Però, alerta! A vegades també et poden demanar les dades per robar-te-les! Vigila molt i no siguis víctima de la pesca. I això, què és? Segueix llegint i ho sabràs tot.

La firma electrònica

És una clau personal per usar-la per Internet. Has d'obtenir un certificat digital. La firma electrònica és una mica complexa, ja que es basa en dos números: una clau pública i una altra de privada amb una relació matemàtica entre elles. Quan es firma electrònicament, es genera el que s'anomena una empremta digital, que és totalment diferent en cada document. Amb una segona funció, l'empremta es xifra amb una clau privada i ja tenim la firma electrònica. La persona que rep la firma ha d'aplicar la clau pública, que ha estat enviada per la persona que n'és titular, per assegurar-ne l'originalitat.

Què és això de la pesca o phishing

És una estafa, un engany per apropiarse una identitat i utilitzar-la a Internet. Aquests lladres se serveixen d'estratègies com ara els correus electrònics o les finestres emergents per aconseguir els seus objectius.

Com s'apropien les nostres dades?

Primer ens envien un correu electrònic fent-se passar per llocs web que considerem de confiança, com el banc, una empresa coneguda, pàgines web de xarxes socials com Facebook, Hi5, Myspace o pàgines d'enviament de postals electròniques. Després ens diuen que anem a l'enllaç que surt al missatge, i aquest enllaç ens transporta a un web pirata semblant a l'original. Un cop allí, ens demanaran les nostres dades amb qualsevol excusa. Com que pensem que el web és de confiança, donem les dades sense posar-hi problemes i l'estafador ja té el que volia: ara utilitzarà les teves dades per fer compres o qualsevol altra gestió que vulgui, com ara obrir comptes de correu.

PRECAUCIONS PER PROTEGIR LA NOSTRA IDENTITAT

- Si et demanen les teves dades a canvi d'algun servei, desconfia! Ja saps on poden anar a parar...
- No t'inscrivis en pàgines insegures.
- No responguis correus electrònics que et sol·liciten informació personal. Les empreses de prestigi mai no demanen contrasenyes o informació personal per correu electrònic. Quan t'arribi algun correu d'aquest estil, truca a l'entitat i comprova que és veritat.
- Quan t'arribi algun missatge amb un enllaç, no el segueixis! Pot portar-te a un web fals i enganyar-te perquè donis les teves dades.
- Encara que a la barra d'adreces surti l'adreça correcta, continua desconfiant! Els pirates informàtics saben falsejar-les i que sembli que són les reals. Tecteja l'adreça a la barra d'adreces per assegurar-te que entres a la pàgina web original.
- Per saber si el lloc web en què estàs és segur, comprova que veus una icona amb un cadenet groc tancat. Això significa que el web protegeix tota la informació personal que donis. Fes un doble clic sobre el cadenet; si el nom que surt no coincideix amb el web en què et trobes, vol dir que aquest web és fals.
- Atreveix-te a trencar els missatges cadena!



«Tindràs mala sort en l'amor si no ho reenvies a vint persones en menys de dos minuts». Et sona, oi? Però no et creguis res: l'única cosa que es pretén amb aquests correus és acumular més i més adreces per enviar-hi publicitat i brossa.

- Posa contrasenyes per accedir al teu *bloc* o *fotobloc*, perquè només hi pugui entrar qui tu vulguis.
- Si no ho has pogut evitar i has estat víctima de la pesca, denuncia-ho! Hi ha un Centre de Denúncies de Fraus a Internet, que col·labora amb les autoritats legals que s'encarreguen d'atrapar els lladres d'identitat.

3.4.2. COMPRES PER INTERNET

Recorda que ets menor i no pots fer compres per Internet. Els resultats del nostre estudi indiquen que teniu bastant present aquesta qüestió, ja que només el 9,4 % heu admès que feu compres per Internet, però en un alt percentatge (41,4 %) sí que consulteu catàlegs de compra o venda. És important que sàpigues que a la xarxa ens bombardegen amb milions d'ofertes i de productes meravellosos a preus increïbles que en realitat són un engany. Les pàgines de subhastes o de compres són plenes d'estafes que només pretenen prendre't els diners i la identitat. Per això, vé's amb molt de compte i, si t'ha agradat alguna cosa i vols comprar-la, consulta-ho als teus pares o tutors i segueix les recomanacions que et donem a continuació:

- Només fes compres en empreses serioses i reconegudes, i sempre amb una connexió d'Internet segura.
- Com que et demanaran que t'enregistris, escull bé la contrasenya, que no sigui fàcil d'endevinar.
- Assegura't que estàs a la pàgina oficial de l'empresa i que no ha estat falsejada pels pirates informàtics. Comprova que l'adreça comença per «**https**», que indica que la pàgina és segura, i que hi ha un cadenet al racó inferior de la pantalla.
- No et creguis les ofertes increïbles que venen productes a un preu molt inferior al del mercat. Tot i que per a un anunciant és més barat anunciar els seus productes per Internet, és impossible comercialitzar productes a preus molt per sota dels que hi ha al mercat.
- Comprova els comentaris d'altres persones sobre la seva experiència de comprar al web on tu ho vols fer; sempre et poden donar pistes sobre aquest web en qüestió.
- No donis les teves dades personals ni dades bancàries per correu electrònic.
- Utilitza formes de pagament segures, un sistema que et permeti pagar quan ja hagis rebut el producte. Desconfia si no pots fer el pagament d'aquesta manera.
- No utilitzis mai dades personals com la teva data de naixement o el teu número de DNI a l'hora de posar una contrasenya, ja que són dades molt fàcils de saber i que poden posar en perill la teva privadesa

ACTIVITAT. La pesca o phishing. Estudi d'un cas real

Et mostrem un cas real d'estafa per Internet.

Un ciutadà de Toledo rep al seu correu electrònic aquest missatge:

Estimat usuari de Banc XXXX!

Per favor, llegeixi atentament aquest avís de seguretat. Prenent en consideració els freqüents casos de frau, hem decidit implementar la confirmació del seu compte cada mes. Li demanem que ompli totes les finestretes per verificar la seva identitat. Si vostè no entra les seves dades no podem verificar la seva identitat i haurem de bloquejar el seu compte.

El saluda atentament El servei de seguretat de Banc XXXX.

Teclegi el número d'usuari:

Clau d'accés:

Introdueixi la seva clau d'operacions:

Clau secreta de la seva targeta (PIN que utilitza als caixers):

Hi surt el logotip del banc i el missatge sembla de confiança. Així, el nostre pobre amic contesta totes les preguntes que li fan i no posa traves a donar les seves dades i contrasenyes perquè no vol que el seu compte quedi bloquejat.

Què va passar després?

Era un frau. Dos ciutadans de nacionalitat russa van aconseguir mitjançant aquest correu electrònic totes les claus de les targetes de crèdit de la seva víctima i van treure 21.500 euros del seu compte. Per sort, aquests lladres van ser detinguts per la policia quan intentaven cobrar la transferència en un banc d'un poble proper.

Què hauria d'haver fet aquest home?

1. Desconfiar! Hem d'anar alerta quan rebem qualsevol missatge que ens demani les nostres dades.
2. Hauria d'haver trucat al seu banc per comprovar si, efectivament, el que li indicava el correu electrònic era veritat.
3. El més important de tot: no donar les seves dades ni contrasenyes a través d'un correu electrònic.

Font: www.elpais.com, «Dos detenidos en Gavà por estafar 21.500 euros mediante 'phising'» 12/11/2000



Capítol 4

EL CORREU ELECTRÒNIC

És un servei molt útil que permet que et comuniquis amb la teva gent de manera immediata. En aquest capítol t'expliquem com pots configurar el teu propi compte de correu electrònic i les precaucions que has de tenir.

CONFIGURACIÓ

1. Necessites una connexió a Internet, ja sigui al teu ordinador o al telèfon mòbil.
2. Has de demanar permís als teus pares o tutors per poder crear un compte. Els menors d'edat legalment no poden fer-ho sense autorització.
3. Escull el servidor que més t'agradi per crear el teu compte de correu; a Internet n'hi ha una infinitud: *Yahoo, Hotmail, Gmail...*
4. Un cop escollit el teu servidor, vés on t'indiqui «Registre» o «Crear un compte de correu».
5. Et demanaran algunes dades personals. Abans de donar-les, ja saps que has de comprovar que el lloc web és segur.
6. Escull un nom per a la teva adreça i una contrasenya.
7. Per acabar, et demanaran que marquis una casella acceptant les condicions de servei i de privadesa del portal d'Internet en qüestió. Què és això? És una mena de contracte entre tu i el portal. És recomanable que llegeixis aquestes condicions, perquè així sabràs quins són els serveis que t'ofereixen, els drets que es reserven —com per exemple poder fer modificacions als serveis sempre que vulguin— i les normes que has de seguir per fer-ne un bon ús. En la majoria de casos, amb aquest «contracte» també acceptes que t'enviïn publicitat al teu correu. Alguns servidors et permeten evitar-ho, simplement indicant que no vols rebre informació d'ofertes ni promocions, però d'altres, no.

PRECAUCIONS

- Escull una adreça de correu que no contingui les teves dades personals, nom i cognoms o data de naixement. Alterna majúscules i minúscules, números, posa-hi guions..., així serà més difícil que els pirates i estafadors informàtics la trobin.

SÍ: exemple758_cOmpTe@servidor.com

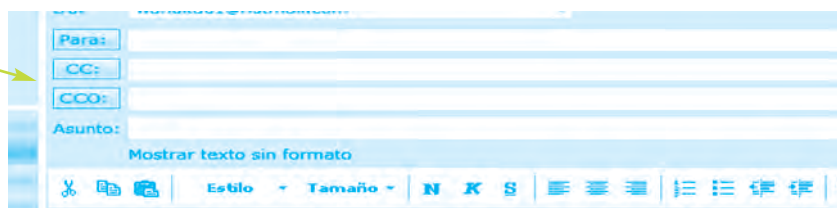
NO: elmeunomicognoms@servidor.com

- Fes el mateix amb la teva contrasenya. Procura que no siguin dades evidents, com la data del teu aniversari, o paraules fàcils d'endevinar.
- No donis la teva adreça de correu electrònic a qualsevol persona; ara ja saps què poden arribar a fer.
- Quan enviïs missatges a diverses persones, recorda't d'incloure'ls en còpia oculta. D'aquesta manera evitaràs que la resta de persones sàpiguen quines són les altres adreces i circulin per la xarxa, amb el perill que comporta: no sabem on poden anar a parar! Per enviar missatges en còpia oculta a Hotmail, busca l'opció «**Mostrar CC:** (còpia) i **CCO:** (còpia oculta)». Introdueix les adreces dels teus destinataris a la barra de CCO.

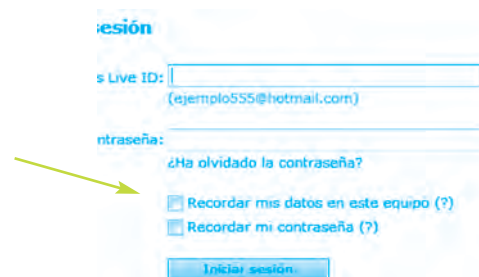


Clica i veuràs el següent:

Escriu les adreces a la barra CCO



- No obris missatges amb arxius adjunts d'origen desconegut o sospitosos, i sobretot no te'ls baixis. Poden portar virus.
- Si reenvies algun missatge a diversos destinataris, esborra les dades de l'enviament anterior (del remitent i dels destinataris).
- No reenviïs els missatges cadena: no els ho posis fàcil, als estafadors informàtics!
- No et fiïs mai dels missatges cadena. De vegades vénen disfressats d'una bona causa, com una nena perduda, un nen que necessita suport per a una operació... Ja saps que l'únic que pretenen amb aquests correus és emmagatzemar adreces.
- Sempre que entris en altres ordinadors que no siguin el teu, assegura't de desactivar la casella que diu: «**Recordar mis datos en este equipo**» o «**Recordar mi contraseña**». I vigila de no deixar-te el teu correu obert.
- Recorda que el teu correu electrònic està protegit per la llei, igual que qualsevol dada personal teva: si algú te l'agafa o en fa un mal ús, ho has de denunciar!



Capítol 5

ELS NOSTRES DRETS COM A CIUTADANS: PROTECCIÓ DE DADES PERSONALS

L'estudi que hem fet revela que molts de vosaltres desconeu les garanties de la protecció de dades (el 39,8 % de l'alumnat enquestat no la coneix) i que, a més, teniu tendència a facilitar-les en fòrums, càstings, xats, concursos o comunitats virtuals. En aquest capítol t'expliquem quins són els teus drets en aquesta matèria i quines són les obligacions dels que et sol·liciten les dades. És important que estiguis ben informat i sàpigues quan atempten contra la teva intimitat.

- Saps que hi ha una Llei de protecció de dades personals? Aquesta llei es diu **LLEI ORGÀNICA 15/1999, DE 13 DE DESEMBRE, DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL**.
- Què diu aquesta llei? Quins drets tinc?

Tinc dret...

- que m'informin de la recollida de les meves dades;
- a saber per a què volen les meves dades;
- a saber la identitat i l'adreça de qui les sol·licita, normalment la persona responsable del tractament de les meves dades o el seu representant;
- a negar-me a proporcionar-les, si no és que una llei m'hi obliga;
- a accedir-hi sempre que vulgui, rectificar-les o cancel·lar-les i oposar-me al tractament de les meves dades en determinades circumstàncies.

Els que em demanen les dades estan obligats a...

- garantir la seguretat de les meves dades, evitant que es perdin, es manipulin o algú hi accedeixi sense autorització;
- demanar el meu consentiment per al tractament de les meves dades;
- contestar totes les preguntes que els planteji sobre l'ús de les meves dades;
- mantenir el secret professional respecte de les meves dades, fins i tot quan les relacions amb ells hagin finalitzat;
- cancel·lar o rectificar les meves dades en un termini de 10 dies, en cas que jo ho sol·liciti;
- no utilitzar les meves dades amb una finalitat diferent a la que em van informar quan les van recollir;
- no proporcionar o vendre les meves dades sense el meu consentiment;
- crear un fitxer i notificar-ho a l'Agència Espanyola de Protecció de Dades o a l'Agència Catalana de Protecció de Dades;

Dades especialment protegides, també anomenades dades sensibles

- Mai no poden obligar-te a donar dades referents a la teva ideologia, la teva religió, les teves creences, el teu origen racial, la teva salut o la teva vida sexual.

El que s'exposa als apartats anteriors no s'aplicarà...

- Quan el tractament de les dades tingui finalitats històriques, estadístiques o científiques (per exemple, el cens o el padró).

ALGUNES DEFINICIONS QUE HAS DE CONÈIXER

Dades personals

Són totes les dades que ens identifiquen com a individus únics i diferenciats dels altres o que permeten identificar-nos; així, tenim el nostre nom complet, el document nacional d'identitat, l'adreça de casa nostra, la nostra pròpia imatge recollida en una foto, un vídeo o una pel·lícula, la nostra veu, les nostres empremtes digitals, les dades referents a la nostra salut o a la nostra estructura corporal i mental, les dades que revelen d'alguna manera la nostra ideologia, religió o creences, la nostra orientació sexual, així com altres dades que són d'ús menys freqüent o menys rellevants.

Som persones

Totes les persones que som a l'Estat Espanyol, independentment de la nostra nacionalitat, tenim el dret que les nostres dades no es revelin a ningú perquè són de la nostra propietat exclusiva, de conformitat amb la nostra Constitució i les lleis que la desenvolupen, entre les quals hi ha la **LLEI ORGÀNICA 15/1999, DE 13 DE DESEMBRE, DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL**, que ens garanteixen el dret a la protecció de dades personals, a l'honor, a la intimitat personal i familiar i a la pròpia imatge.

La nostra Constitució i les lleis també protegeixen les nostres dades personals un cop nosaltres les hem revelades als altres i/o han estat publicades per qualsevol mitjà, amb el nostre consentiment o sense, ja que ens permeten controlar en tot moment el bon ús i la circulació de les nostres dades.

Norma general

Per tant, la norma general és que cadascú de nosaltres és l'amo de les seves dades personals i no està obligat a facilitar-les; qui vulgui utilitzar-les, ha de demanar-nos-en permís, és a dir, ha de fer-ho amb el nostre consentiment i tenir la nostra conformitat.

Excepció

Estem obligats a facilitar les nostres dades personals quan una llei ens obliga a fer-ho de manera clara i amb una finalitat concreta. Per exemple: la Llei de registre civil obliga els nostres pares a facilitar les dades personals dels seus fills acabats de néixer per incorporar-los a un arxiu amb l'objectiu d'identificar-los i atribuir-los una nacionalitat.

DRETS PER PROTEGIR LES TEVES DADES

Dret d'informació

Quan et sol·licitin les teves dades personals per qualsevol mitjà oral o escrit, tens el dret que t'informin sobre la necessitat de la recollida de les dades, així com de la seva finalitat o el seu propòsit, de les conseqüències si et negues a donar-les, de la localització de l'arxiu que contindrà les teves dades i de la identitat de la persona responsable del funcionament d'aquest arxiu. D'una manera específica, t'han d'informar d'aquests drets:

Silenci absolut: Ningú i en cap cas no pot obligar-te a declarar dades sobre la teva ideologia, religió o creences personals. No hi ha cap llei que t'hi obligui.

Autorització expressa: Si ets major de 14 anys, únicament mitjançant el teu consentiment o autorització expressa i per escrit poden sol·licitar-te i usar dades de caràcter personal que revelin la teva ideologia, religió, creences, afiliació sindical, origen racial, vida sexual o dades referents a la teva salut; només poden fer-ne ús quan una llei ho autoritza expressament i clarament, per raons d'interès general i amb una finalitat concreta o amb el teu consentiment.

Accés: Tens la possibilitat de saber quines dades personals tenen arxivades o recollides altres persones sobre tu, i també l'origen d'aquestes dades i les comunicacions o els traspassos que se n'hagi fet a tercers (altres, a part de tu i el responsable de l'arxiu al qual accedeixes), salvant les limitacions que la llei imposa a alguns arxius oficials.

Rectificació: Un cop sàpigues que les teves dades són en poder d'altres persones, tens el dret que les rectifiquin en el sentit que creguis convenient.

Cancel·lació: En aquest mateix sentit, tens dret que les teves dades personals siguin bloquejades, cancel·lades o definitivament esborrades quan resultin excessives per a la finalitat per a la qual es van recollir, inadequades o no pertinents.

Oposició: Tens dret a oposar-te a l'ús i la circulació de les teves dades personals que són en poder d'altres persones i a oposar-te a les valoracions sobre aspectes concrets de la teva personalitat, basades únicament en el tractament de les teves dades personals.

Si algú té les teves dades sense que tu ho sàpigues i a més vol utilitzar-les, prèviament ha d'informar-te de l'existència d'aquest arxiu i de la seva adreça, del seu contingut, de la identitat del responsable, de l'origen de les dades o de com les va aconseguir i de la possibilitat que tens d'accedir-hi, oposar-te al seu ús, rectificar-les o cancel·lar-les. Aquesta obligació d'informar-te no existeix quan una llei ho permet, quan les teves dades són tractades amb finalitats històriques, estadístiques o científiques o quan per qualsevol causa justificada és impossible informar-te'n.

Seguretat: La persona responsable del registre i del tractament de les teves dades i els que treballen per a ella han de guardar un secret absolut sobre el seu contingut i tenir-les en un arxiu segur, on ningú hi pugui accedir fàcilment.

IMPORTANT: Quan la recollida de les teves dades es fa per escrit, per mitjà de qüestionaris o altres impresos, han de figurar clarament en el paper tots els drets que acabem d'exposar, de manera que abans d'escriure els has de poder llegir amb tranquil·litat i, després d'entendre'ls, exercitar-los a l'acte si ho creus convenient, en funció de la situació en què et trobis. En el cas d'Internet, has de llegir atentament les condicions de servei i la política de privacitat. Al final de cada formulari hauries de trobar frases del tipus:

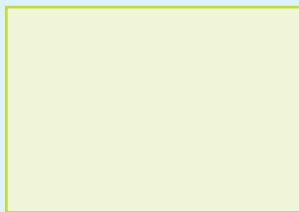
«Les dades personals seran recollides i tractades al fitxer [...], que té la finalitat de [...], inscrit al Registre de Fitxers de Dades Personals de l'Agència de Protecció de Dades de [...] i podran ser cedits a [...], a més d'altres cessions previstes a la Llei. L'organisme responsable del fitxer és (nom i adreça).»

Ara et proposem un exercici pràctic per aplicar aquests drets, mitjançant l'estudi d'un cas trobat a Internet.

Al mes de gener vinent començarà la 5^a edició del programa de televisió «Et donem una oportunitat». Per presentar-te al càsting, has d'emplenar per Internet aquesta fitxa d'inscripció i enviar-nos-la.

FITXA D'INSCRIPCIÓ

Foto actual, indicant el pes, l'alçada i les mides (si ets dona)



Nom i cognoms:

Data de naixement:..... DNI o passaport:.....

Estat civil:Telèfon mòbil:

Adreça electrònica:

Professió actual (indica si estudies, treballes o estàs a l'atur):

Nom dels pares i DNI:Raça:

Malalties o al·lèrgies que tens:.....Religió:

Condició sexual (heterosexual o homosexual).....

Estaries disposat a...?:

- | | | | |
|--|----|----|-------|
| • Pintar-te els cabells de color | SI | NO | DEPÈN |
| • Tallar-te els cabells | SI | NO | DEPÈN |
| • Desfilat en roba de bany | SI | NO | DEPÈN |
| • Fer nus parcials (topless) | SI | NO | DEPÈN |
| • Ser gravat durant el dia sense saber quan | SI | NO | DEPÈN |
| • Consentiries l'emissió de les imatges gravades seleccionades per la productora Globo Tour RTV? | SI | NO | DEPÈN |

Aficions:

.....

.....

Indica si t'has presentat anteriorment en algun concurs de televisió i en quina cadena

.....

.....

Un cop finalitzades les proves de selecció, es publicaran a la nostra pàgina web el nom, el DNI i l'adreça de correu electrònic de cadascun dels seleccionats per l'empresa GLOBO TOUR RTV SA, Barcelona

Després de llegir la fitxa d'inscripció del càsting, respon aquestes preguntes:

1. Estaries disposat a presentar-te a aquest càsting? Raona la teva resposta

.....

.....

2. Quina és la finalitat principal que persegueix aquesta empresa quan sol·licita aquestes dades?

.....

.....

3. Quines dades creus que són innecessàries per a la finalitat prevista? Enumera-les i justifica la teva resposta

.....

.....

DENÚNCIA EN UNA AGÈNCIA DE PROTECCIÓ DE DADES

Si alguna vegada creus que no s'han respectat els teus drets en matèria de protecció de dades, explicats anteriorment en aquest manual, has d'interposar una denúncia perquè es compleixi la Llei i no facin un mal ús de les teves dades. Per fer-ho, hauràs de presentar un escrit de denúncia en els termes que preveu l'article 70 de la Llei 30/1992 de règim jurídic de les administracions públiques i del procediment administratiu comú.

En aquest escrit hi han de constar:

- Nom i cognoms de la persona interessada i, si és el cas, de la persona que la representi, així com la identificació del mitjà preferent o l'assenyalament del lloc a efectes de notificacions.
- Fets, raons i petició en què es concreti, amb tota claredat, la sol·licitud.
- Lloc i data.
- Firma de la persona sol·licitant o acreditació de l'autenticitat de la seva voluntat expressada per qualsevol mitjà.
- Organisme, centre o unitat administrativa a la qual s'adreça (que en aquest cas seria la Subdirecció General d'Inspecció de Dades d'aquesta Agència).
- Documents que s'adjunten.



Emplena, amb els teus pares o professors, el model de denúncia que et facilitem a continuació.

MODEL DE DENÚNCIA DAVANT L'AGÈNCIA CATALANA DE PROTECCIÓ DE DADES

Dades de la persona denunciant

Nom

DNI (cal adjuntar-ne la fotocòpia)

Adreça

Dades de la persona denunciada

Nom (cal indicar una entitat de les esmentades a l'article 3 de la Llei 5/2002, de 19 d'abril)

Adreça

Localitat

D'acord amb el que estableix l'article 17 de la Llei 5/2002, de 19 d'abril, de l'Agència Catalana de Protecció de Dades, denuncio, perquè vulneren el que disposa la normativa vigent en matèria de protecció de dades, els fets següents:

(La persona sol·licitant ha d'enumerar quins són els fets ocorreguts que vol denunciar.)

.....
.....
.....

Per tal de justificar els fets denunciats, apporto la documentació següent:

(La persona sol·licitant ha d'indicar la documentació que correspongui.)

.....
.....
.....

Localitat i data

Signatura de la persona denunciant

Directora de l'Agència Catalana de Protecció de Dades

D'acord amb l'article 5 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, us informem que la presentació de la denúncia dóna lloc a la inclusió de les dades de caràcter personal en el fitxer de registre d'entrada i sortida de documents de l'Agència Catalana de Protecció de Dades i en el fitxer d'expedients d'exercici de drets, d'inspecció i sancionadors, creats mitjançant Resolució de 23 de setembre de 2004, per la qual es creen els fitxers de dades de caràcter personal de l'Agència Catalana de Protecció de Dades. La persona afectada podrà exercir els drets d'accés, rectificació, cancel·lació i oposició davant el responsable del fitxer, l'Agència Catalana de Protecció de Dades, carrer Llacuna núm. 166, 7a planta, Barcelona (08018). Us informem que les vostres dades poden ser cedides a altres autoritats que tinguin competències en procediments de garantia del dret a la protecció de dades, així com a altres instàncies competents en la garantia dels drets dels particulars, per tal de resoldre la vostra petició.

Lloc web per tramitar la denúncia: Agència Catalana de Protecció de Dades, www.apd.cat

Capítol 6

RESUM I CONCLUSIONS

Aquest manual és el resultat de l'estudi que vosaltres ens heu ajudat a fer amb la vostra participació. Les vostres respostes ens han orientat a l'hora d'escollir els temes que calia tractar. Ens han fet veure quin és l'ús que feu d'Internet i del telèfon mòbil. La finalitat d'aquest text és apropar-vos una mica més a les tecnologies de la informació, que sapigueu no tan sols quins són els beneficis, sinó també tots els riscos als quals us exposeu, i donar-vos els recursos per protegir-vos i saber actuar.

A continuació us oferim també consells per a pares, mares, educadors, educadores i tutors legals, que esperem que us siguin útils.

Consells per a pares, mares, educadors, educadores i tutors legals

DE CARÀCTER GENERAL

1. Intenteu estar al dia pel que fa a Internet i el telèfon mòbil. Com més informació tingueu sobre aquestes tecnologies, més fàcil us serà ajudar els vostres fills i filles a fer-ne un bon ús.
2. Parleu amb els joves sobre el que fan a Internet, amb qui parlen o quines pàgines visiten més. Establiu entre tots unes regles bàsiques d'ús i consum de les tecnologies.
3. És recomanable que situeu l'ordinador en un lloc comú de la casa. NO deixeu que tinguin l'ordinador a la seva habitació.
4. Controleu el temps que passen els vostres fills i filles a Internet o fent servir el telèfon mòbil. Establiu uns horaris d'ús que s'adaptin al temps d'estudi.
5. Fomenteu les activitats en família i animeu els vostres fills i filles que facin esport, teatre o qualsevol altra alternativa a l'ordinador i al telèfon mòbil.

SOBRE L'ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ

6. Instal·leu un antivirus, tallafocs i programes de filtratge de correu brossa al vostre ordinador i assegureu-vos que els actualitzeu de tant en tant.
7. Prepareu diferents inicis de sessió personalitzats per a cada fill o filla.
8. Configureu el vostre compte com el de l'administrador de l'equip per poder controlar el que cadascun dels vostres fills pot i no pot fer.
9. Configureu el compte dels vostres fills per protegir-los de tots els perills d'Internet. En els exploradors d'Internet de

tots els sistemes operatius hi ha la possibilitat d'un control patern. El trobareu en l'opció «**Herramientas > Opciones de Internet > Contenido**».

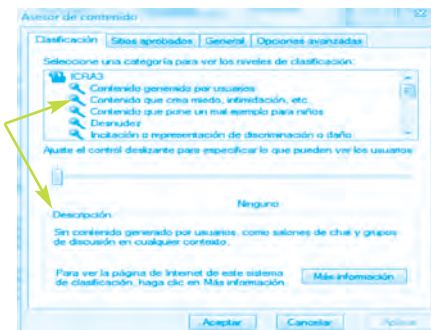
Cliqueu en l'opció de «**Control parental**» i podreu desactivar els jocs que no voleu que els vostres fills facin servir i rebre al vostre compte informació sobre les activitats dels comptes dels vostres fills, setmanalment o diàriament.

Trobareu també l'opció d'«**Assessor de contingut**». A la pestanya de «**Classificació**» podreu indicar, movent el cursor, el nivell de sexe, por, nuesa o llenguatge vulgar, tot allò a què no voleu exposar el vostres fills quan accedeixen a Internet (el nivell més estricte és el 0, a l'esquerra de tot).



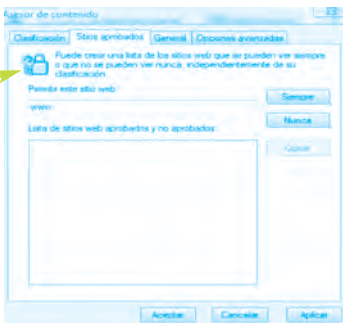
10. Creeu una llista dels llocs web que els vostres fills poden visitar sempre o que no poden visitar mai. Per això, en l'opció d'«**Asesor de contingut**» heu de fer clic sobre la pestanya de «**Sitios aprobados**», escriure l'adreça de la pàgina web en qüestió i seleccionar «**Siempre**» o «**Nunca**».

11. Creeu una contrasenya perquè els vostres fills no puguin canviar la configuració que els heu fet al seu compte i no puguin entrar als llocs web que heu valorat com a perillosos. Per fer-ho, aneu a l'opció d'«**Asesor de contenido**» i feu clic a la pestanya «**General**».



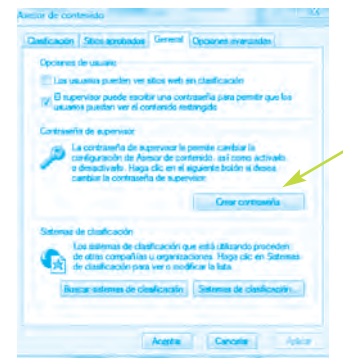
Si voleu protegir més els vostres fills quan es connecten a Internet, hi ha programes amb més opcions de seguretat i configuracions diferents en el mercat.

12. Expliqueu als vostres fills els beneficis del xat, però també els perills que té; sobretot remarqueu que no poden quedar amb persones desconegudes. Si envien un missatge o visiten sales de xat, si utilitzen videojocs en línia o altres activitats a Internet que exigeixen un nom d'inici de sessió per identificar-se, ajudeu-los a escollir-lo i assegureu-vos que fan servir contrasenyes segures, que no les comparteixen amb ningú i que no donen cap informació personal. Al mercat hi ha una àmplia varietat de programes amb més opcions de seguretat i de filtratge de continguts.



13. Fixeu-vos en els jocs que es baixen o que intercanvien amb els amics. Assegureu-vos que el contingut és adequat a la seva edat i que no inclou violència.

14. Acompanyeu els vostres fills quan es baixin programes, música o arxius, encara que siguin legals. Ensenyeu-los que si comparteixen arxius o agafen textos, imatges o dibuixos del web ho han de fer sense infringir les lleis de drets d'autor i propietat intel·lectual, i que pot ser il·legal.



SOBRE LA PROTECCIÓ DE DADES PERSONALS

15. Parleu amb els vostres fills de la importància de protegir les dades personals. En aquest manual incloem els drets que ens emparen com a ciutadans i ciutadanes, inclosos en la legislació de protecció de dades de caràcter personal, tant d'àmbit estatal com autonòmic.
16. Ensenyeu als vostres fills adolescents que mai no han de facilitar informació personal sense el vostre permís quan utilitzin el correu electrònic, sales de xat, missatgeria instantània, o bé quan emplenin formularis de registres i perfils personals o quan participin en concursos en línia.

Resum de consells

- Controla el temps que passes davant l'ordinador o el telèfon mòbil. No t'oblidis d'estudiar i de dedicar un temps a la família.
- Sigues sempre respectuós i tolerant amb les opinions dels altres, en blocs, fòrums o xats.
- Vés amb compte amb les ofertes i les promeses miraculoses que et fan per Internet. Si has trobat alguna cosa que t'agradaria comprar per Internet, consulta-ho sempre amb els teus pares o amb una persona adulta responsable.
- Per protegir la teva intimitat recorda't d'esborrar periòdicament l'historial, les galetes i els arxius del teu ordinador.
- Instal·la un antivirus i un tallafocs al teu ordinador per protegir-lo dels virus i troians. No t'oblidis d'actualitzar-ne sovint les versions.
- Perquè no et molestin les finestretes emergents de publicitat (*pop-ups*), bloqueja-les seguint els passos que t'hem mostrat en el manual i aconsegueix un programa bloquejador de *pop-ups*.
- Analitza bé els correus electrònics que arriben a la teva adreça, si duen un arxiu adjunt, si provenen d'un remitent que no coneixes o si el seu titular et fa promeses miraculoses, convé que els esborris abans d'obrir-los, ja que poden ser els famosos correus brossa o *spams*.
- Per fer-te més resistent als programes de cerca automàtica d'adreces, posa't un nom complicat al teu compte, que no doni informació sobre les teves dades personals, com ara el teu nom o cognoms o la data de naixement, i convé que inclogui nombres, guions... Per exemple: *noves467tecnologies9_@protegeixte.com*. Fes el mateix amb la teva contrasenya.
- No pengis les teves fotos a Internet; ja saps que els pirates malintencionats poden fer-ne un mal ús.
- Vés molt amb compte quan et connectis a un xat. No revelis mai les teves dades ni les dels teus pares, ni enviïs fotos a persones desconegudes. Evita de citar-te amb persones que has conegut a través del xat, i si finalment decideixes de fer-ho no hi vagis mai sol/sola.
- Per protegir les teves dades de caràcter personal i evitar de ser víctima dels fraus a la xarxa, no et registris en pàgines insegures, ni responguis correus electrònics que et demanin informació personal, i assegura't sempre que la pàgina que visites és l'original.
- Si creus que les teves dades han estat utilitzades d'una manera inadequada, recorda que tens drets i que hi ha una Llei de protecció de dades de caràcter personal que t'empara. No dubtis, doncs, de denunciar-ho a les autoritats competents.

RELACIÓ D'ESCOLES QUE HAN PARTICIPAT AL PROJECTE CLI PROMETEO 2008-09

ANDALUCIA

I.E.S. Aurantia	Almeria
I.E.S. La Janda	Cádiz
I.E.S. Cárbula	Córdoba
I.E.S. Villanueva del Mar	Granada
I.E.S. Delgado Hernandez	Huelva
I.E.S. Iulia Salaria	Jaén
I.E.S. Martín Rivero	Malaga
I.E.S. Néstor Almendros	Sevilla

CATALUNYA

Ceip Pere Vila	Barcelona
I.E.S. Salvador Espriu	Barcelona
Col·legi Lestonnac	Barcelona
Escola Thau	Barcelona
Ce Jacint Verdaguer	Barcelona

EUSKADI

Cep Angel Ganivet-Izarra-Sta. Lucia	Alava
Cep Lateorro	Alava
I.E.S. Zaroabe	Alava
Cep Aitor Ikastola	Guipuzcoa
Cep Harri Berri Oleta	Guipuzcoa
I.E.S. Egape Ikastola	Guipuzcoa
I.E.S. Lezo	Guipuzcoa
Cep Derio	Vizcaya
Cep Atxondo	Vizcaya
Cep Maestro Zubeldia	Vizcaya
Cep Barrutia	Vizcaya
I.E.S. Derio	Vizcaya
I.E.S. Bengoetxe	Vizcaya
Cep Zaldupe	Vizcaya
I.E.S. Barrutialde	Vizcaya
Cep Velázquez-M.Cervantes	Vizcaya
Cep San Gabriel	Vizcaya
Cep Urretxindorra	Vizcaya
I.E.S. Ategorri	Vizcaya
I.E.S. Balmaseda	Vizcaya

EXTREMADURA

Colegio Claret	Badajoz
I.E.S Sáez de Buruaga	Badajoz
I.E.S. Tamujal	Badajoz
Ceip Ntra. Sra. de La Caridad	Badajoz
I.E.S.O. Via Dalmacia	Cáceres

MADRID

I.E.S. Prado de Santo Domingo	Madrid
I.E.S. José de Churriguera	Madrid
I.E.S. Isabel La Católica	Madrid
I.E.S. Cervantes	Madrid
Colegio Sagrado Corazón	Madrid



Comissió
de Llibertats
i Informàtica

C/ José Ortega y Gasset 77, 2ªA - 28006 Madrid
Tels. 914 023 204 · 915 237 566 · Fax 915 238 621
secretaria@asociacioncli.es · www.asociacioncli.es