

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



CAJA MADRID
OBRA SOCIAL



Comissió
de Llibertats
i Informàtica

Projecte CLI - PROMETEO
2008/09

Manual Pràctic
de 12 a 14 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.

Altres Col·laboracions tècniques:
Javier García Álvarez.

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

Número de Registre M-000781/2009

Copyright © 2008
Reservats tots els drets. Es permet la seva còpia i distribució per qualsevol mitjà sempre i quan es mantingui el reconeixement dels seus autors, no es faci ús comercial de les obres i no es realitzi cap modificació de les mateixes.

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
1. El bon ús d'Internet a l'ordinador i al telèfon mòbil	Activitats que es poden fer i benefici que ens aporten	Valorar les possibilitats i els avantatges que tenen totes dues tecnologies	Present i futur d'Internet: reflexió i debat	4
2. Problemes derivats d'un mal ús d'Internet	La protecció de dades personals i la privadesa: aspectes tècnics	Conèixer els procediments tècnics per afavorir la nostra intimitat		6
• Compartir arxius: textos, fotos, vídeos, etc.	Virus, antivirus, bloquejadors, tallafocs. Evitar correus no desitjats (correus brossa, <i>spams</i>)	Detectar les possibles invasions en la nostra privadesa i mitjans per evitar-les	Modificació d'arxius: alteració d'imatges reals	6
• Trobades amb persones desconegudes: en línia i reals (cites a cegues)	Trobades amb altres persones a través de la xarxa: els xats	Identificar els perills de contactar amb persones desconegudes	Anàlisi d'imatges amb doble personalitat: la realitat enganyada	11
• Assetjament electrònic (<i>cyberbullying</i>)	Mitjans d'assetjament: – correu electrònic – participació en un xat i en jocs en línia	Reconèixer els casos d'assetjament i saber actuar-hi en contra	Ciberconte: el mirall de la Blancaneu	13
• Fraus per Internet: – compres – suplantació de la personalitat (<i>phishing</i>)	La identitat electrònica	Prendre consciència de les precaucions necessàries per protegir-la	Pesca electrònica (<i>phishing</i>): definició, descripció de fotos, anàlisi d'un cas real	15
3. El correu electrònic	Configuració i precaucions	Aprendre a configurar un compte de correu electrònic amb garanties	Configuració d'un compte de correu electrònic	19
4. Els nostres drets 4.1. Som ciutadans: protecció de dades personals 4.2. Som persones	Els drets que ens emparen: dret d'accés, rectificació, cancel·lació i oposició al tractament de dades personals. Models de denúncia	Conèixer els drets sobre protecció de dades personals d'una manera activa	Cas pràctic de denúncia a l'Agència de Protecció de Dades	22
5. Consells per a pares i mares, educadors i educadores, o tutors				30
6. Consells per a estudiants				32

Introducció

Un dels sectors que més evolucionen cada dia és el de les noves formes d'informació i de comunicació, sobretot per mitjà d'Internet, ja que ens acostem a noves formes de coneixement i nous tipus de relació amb els altres. Avui dia podem tenir accés gairebé a tota la informació que vulguem i unir-nos a milions de persones d'arreu del món sense límit de temps ni de distància.

Però també hi ha riscos si no fem un ús adequat de tots aquests avenços. Per això, la Comissió de Llibertats i Informàtica ha fet un estudi en el qual han participat més de 8.000 estudiants d'escoles i instituts de diferents comunitats autònomes, amb la finalitat de saber quines són les preferències dels nois i les noies de 12 a 14 anys sobre l'ús de tecnologies com ara els ordinadors i els telèfons mòbils, i el seu accés a Internet, els reproductors de so i vídeo, etc., així com molts altres aspectes interessants. Una primera dada: gairebé el 30 % dels estudiants de la teva edat es connecten a Internet cada dia, davant el 20 %, que només ho fan els caps de setmana; la resta ho fan de manera més esporàdica.

Aquest manual és el resultat de les conclusions extretes d'aquest estudi. Una de les més importants és el desconeixement que sovint teniu dels riscos ocasionats per un mal ús d'Internet. Per això t'ofereixo alternatives per defensar-te d'aquests perills, sobretot en tot allò que fa referència a la protecció de les dades personals: el nom, l'adreça, fotografies, enregistraments de la veu, etc.; tot allò que t'identifica davant els altres i que podria arribar a circular per Internet sense cap control. A més a

més, per tal que es respecti la teva intimitat, t'indiquem els drets que ens emparen i la manera de defensar-los, si calgués. Has de saber que, per autoritzar el tractament o l'ús de les teves dades personals per part d'altres persones, es considera que ets **major d'edat**, segons la llei, a partir dels 14 anys.

D'una manera fàcil i pràctica, el contingut d'aquest manual s'estructura en tres grans blocs:

- 1. L'ús d'Internet:** beneficis que aporta i problemes derivats del mal ús de la xarxa (virus i altres intromissions, fraus, etc.).
- 2. Els nostres drets com a ciutadans,** especialment els vinculats a la protecció de dades personals.
- 3. Consells per a pares i mares, educadors i educadores, i estudiants.**

Aquest manual està pensat perquè t'animis a llegir-lo i a fer les activitats que et proposa amb els teus pares, tutors o professors. Ells et podran explicar tot allò que no acabis d'entendre, però, a més, junts aprendreu moltes coses. Hi afegirem uns quants consells que no volem que oblideu.

Una autèntica aventura de coneixement que t'ajudarà a enfrontar-te als nous reptes tecnològics.

Vine amb nosaltres! T'agradarà!

Capítol 1

EL BON ÚS D'INTERNET A L'ORDINADOR I AL TELÈFON MÒBIL

L'ús d'Internet és un gran benefici per a tothom. Navegant per la xarxa amb l'ordinador o amb el telèfon mòbil podem conèixer moltes coses noves i comunicar-nos amb diferents persones. I en temps real!

HI POTS:

- Xatejar amb els teus amics, connectats simultàniament en una mateixa conversa en un moment donat. Veure els seus noms a la llista de l'ordinador i anar intercanviant missatges. Fins i tot, en molts casos, t'hi pots comunicar per la transmissió de la teva pròpia veu o imatge.
- Buscar informació sobre temes que t'interessen i aprendre per tu mateix. Internet integra actualment la base de dades més gran del món en suport informàtic, el **World Wide Web** (www), formada per milions de pàgines web plenes d'informació de tota mena, repartides per milers de servidors (ordinadors connectats permanentment a la xarxa). Quina independència!
- Fer o completar treballs que et demanen a l'escola o a l'institut. Imagina't que vols fer visites virtuals a les ciutats i als llocs més importants del món i, en alguns casos, recórrer-los en tres dimensions. I tot això, davant una pantalla i dirigit per tu mateix. Sorprendràs els teus professors i companys!
- Comunicar-te amb amistats o familiars que viuen lluny, superant les barreres del temps i de la distància. Dos mil quilòmetres o més, només fent un clic amb el ratolí o la pantalla.
- Tenir la teva pròpia pàgina web o el teu bloc. Un diari personal que pots anar actualitzant amb tot allò que et passa. Els blocs o fòrums permeten expressar la teva opinió sobre els temes que t'agraden.
- Compartir gustos i interessos amb altres persones. L'ús d'Internet com a font d'informació pot afavorir el treball en grup i el cultiu d'actituds socials, l'intercanvi d'idees, la cooperació i el desenvolupament de la personalitat.



- Passar-ho bé: jugar, escoltar música o mirar vídeos. Molts jocs milloren les habilitats (rapidesa, agilitat mental, etc.) i posen a prova l'enginy.

A l'enquesta que vam fer a nens, nenes i joves de 12 a 14 anys, i de la qual ja t'hem parlat, vam donar a triar entre diferents tecnologies. El resultat pel que fa a l'ús va ser el següent: el 50 % prefereixen l'ordinador amb accés a Internet; el 26 %, el telèfon mòbil; el 12 %, els reproductors d'àudio (MP3, MP4, etc.) i de fotografia o vídeo, i el 9 %, l'ordinador, encara que no tingui accés a Internet.

REFLEXIONA

Pensa almenys cinc invents o avenços de la humanitat que hagin revolucionat el món durant els últims vint o trenta anys. Escriu-ne el nom. On situaries Internet? Intercanvia la teva opinió amb la dels teus pares o companys de classe i escriu-ne les coincidències o les diferències.

1.
2.
3.
4.
5.

Coincideixen en:

.....
.....

Difereixen en:

.....
.....

Intenta també endevinar el futur d'Internet i d'altres tecnologies. Què més ens permetran fer?

.....
.....

Capítol 2

PROBLEMES DERIVATS D'UN MAL ÚS D'INTERNET

Probablement et deus haver preguntat qui controla tot allò que podem trobar a Internet.

Moltes vegades, ningú, per la gran quantitat d'informació disponible, tot i que existeixen organismes i autoritats que vetllen per protegir els ciutadans davant possibles delictes. A més a més, has de tenir en compte que, sovint, Internet ens pot oferir una visió parcial de la realitat amb informacions falses o antiquades.

En això consisteix el veritable problema.

Internet es pot convertir en una autèntica bomba de rellotgeria... i esclatar!, si no prens les precaucions adequades. Per aquest motiu has de saber quines limitacions té aquest mitjà, que t'indiquem als apartats següents.



PROBLEMA 1. COMPARTIR ARXIUS: TEXTOS, FOTOS, VÍDEOS, ETC.

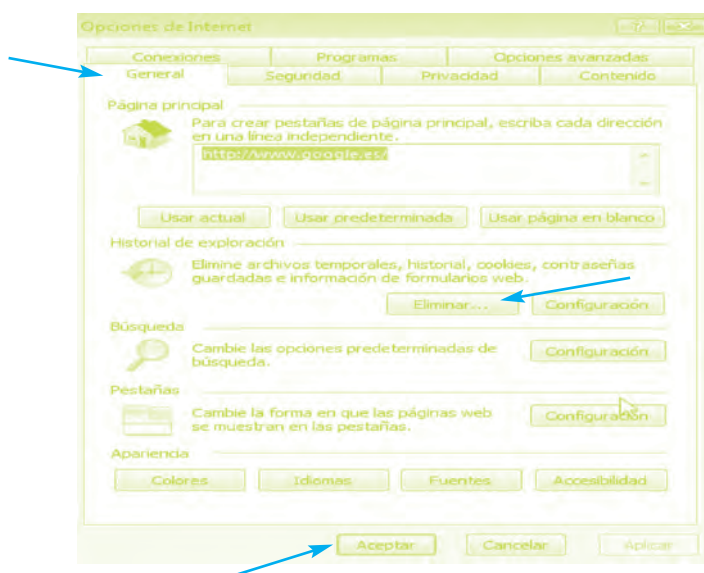
El teu ordinador ho anota tot. Guarda les pàgines web que has visitat, els arxius que t'has baixat, les teves contrasenyes, etc. Mai no oblida res si no és que tu li ho dius i, el pitjor de tot, hi pot haver persones que utilitzin els seus coneixements informàtics per accedir a aquesta informació, espia-la i apoderar-se'n.

Com a bon secretari, ho té tot classificat d'aquesta manera:

- **L'historial.** Aquí s'emmagatzemen les pàgines web que has visitat. Són algunes de les «empremtes» que vas deixant per la xarxa, de manera que cal esborrar-les perquè ningú no les pugui seguir.
- **Les galetes (cookies).** Són arxius que contenen l'adreça de la pàgina que acabes de veure. N'hi ha de temporals, però altres poden romandre al teu ordinador durant anys. Els espies poden fer un seguiment de les que has visitat i accedir als teus arxius. D'aquesta manera poden saber els teus gustos i preferències, i amb aquestes dades crear llistes de possibles clients que després venen a empreses comercials. És important eliminar-les periòdicament.

- **Els arxius.** Emmagatzemen les imatges i els continguts de les pàgines que has consultat a Internet per accelerar-ne la càrrega quan hi tornis a entrar. Has de tenir en compte que entrant en aquests arxius es poden saber les dades que ja has escrit. Si els esborres, trigaràs una mica més a carregar la pàgina, però estaràs protegit dels espies i els intrusos informàtics.

Per evitar que algú tingui accés al teu ordinador et recomanem que, juntament amb els teus pares, esborris aquests arxius de tant en tant. Si el sistema operatiu que utilitzes és el *Windows XP* i la versió anterior d'*Internet Explorer*, ho pots fer des de l'«Historial d'exploració» («Eines» > «Opcions d'Internet», fes clic a la pestanya «General» i a «Elimina l'historial, les cookies o els arxius», i accepta).



A més a més, molts arxius que t'envien persones que no coneixes poden contenir **virus**.

Saps que n'hi ha alguns que són molt difícils de detectar pels antivirus de l'ordinador i que poden fer malbé el teu equip i tot el que hi hagi guardat, com ara música, fotos, jocs i tasques? Aquests són els virus més freqüents:

- **Cavall de Troia o troià.** S'amaga darrere alguns programes que ens baixem perquè creiem que són inofensius. Una vegada baixat, el troià entra dins el teu ordinador i hi pot fer tot el que vulgui.
- **Stealth.** N'és un dels pitjors, que fins i tot intenta enganyar l'antivirus modificant les seves dades perquè no el detecti.
- **Paràsit.** Es pot amagar en els programes que inclouen el missatge d'«Executar».
- **Cuc.** Es propaga amb moltíssima facilitat perquè es trasllada d'un ordinador a un altre a través del correu electrònic o de la missatgeria instantània.
- **Cabir.** El virus del mòbil. Viatja de mòbil a mòbil a través del Bluetooth. Et pot robar els missatges de text o els contactes, i pot seguir els teus moviments o escoltar les teves converses.

No et preocupis. Aquí t'ofereim alguns consells pràctics per protegir-te de l'atac dels virus:

1. Per descomptat, has de tenir instal·lat a l'ordinador:
 - **Un antivirus.** L'ordinador és com una casa, que ha d'estar tancada per evitar que no hi entri qui no vols. De vegades, fins i tot hi instal·lem sistemes de vigilància afegits. Fem el mateix amb l'ordinador? Per evitar que per les portes d'Internet entrin possibles intrusos, necessitem un programa de vigilància que anomenem antivirus. És el nostre sistema de seguretat, un guardaespalles que es manté sempre alerta davant possibles programes perjudicials que es puguin esmunyir dins l'ordinador i fer ús de les dades i els arxius que hi tens emmagatzemats. No oblidis actualitzar-lo sovint; si no ho fas, té una utilitat pràcticament nul·la.
 - **Un tallafocs.** O *firewall*, en anglès. Aquesta mena de programa és el «porter» del teu ordinador: ningú no hi passarà sense el seu permís. T'avisava de possibles programes que et poden danyar l'ordinador i, a més, et protegeix davant els estafadors que hi vulguin entrar.
2. No has de facilitar a ningú la teva contrasenya d'accés.
3. No has d'obrir ni desar arxius que t'enviïn persones desconegudes.
4. Has d'instal·lar un programa anti *pop ups* per bloquejar les finestres que, sense haver-ho sol·licitat, es mostren a l'ordinador amb aquesta publicitat tan molesta.

CORREU ELECTRÒNIC NO DESITJAT

Segurament deus haver sentit parlar dels correus no desitjats, els anomenats correus brossa (o spam, en anglès).

Es tracta de missatges o correus que acostumen a contenir publicitat enganyosa amb finalitats comercials. S'aprofiten de la nostra curiositat i sembla que ens vulguin solucionar la vida. En realitat, la seva intenció sol ser introduir un virus dins el nostre ordinador i controlar-lo.

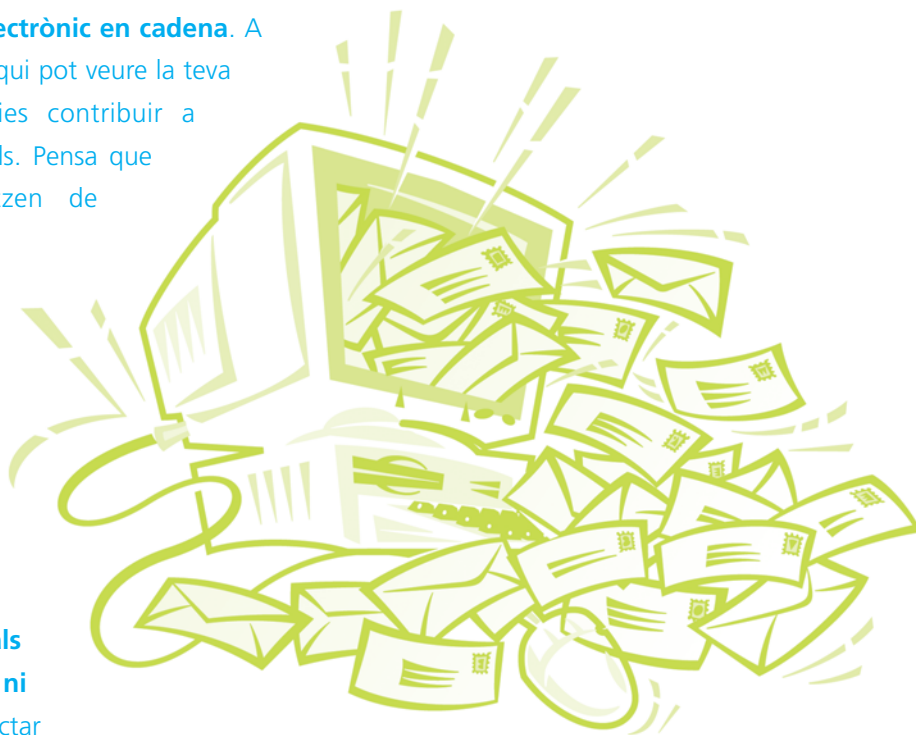
Són dels tipus següents:

- «Guanya milions amb el mínim esforç»
- «L'amor de la teva vida t'està esperant»
- «Has estat seleccionat entre milions de persones per provar... (X) ... Una nova il·lusió per a la teva vida. Envia les teves dades a ... [un número o adreça de correu electrònic] i rebràs gratuïtament...».



T'afegim alguns consells per evitar que entrin a la teva bústia:

1. **Elimina els missatges de correu electrònic no desitjats sense obrir-los.** En alguns casos alertem els creadors d'aquesta mena de correus tan sols obrint els missatges.
2. **No responguis als missatges de correu electrònic no desitjats**, excepte si n'estàs totalment segur de l'origen.
3. **Pensa-t'ho dues vegades abans d'obrir arxius adjunts o fer clic en vincles inclosos dins els xats o els correus electrònics**, encara que coneguis el remitent. Si no n'estàs segur, elimina el missatge. Si fos imprescindible, desa'l primer al disc dur i utilitza l'antivirus abans d'obrir-lo.
4. **No reenviïs missatges de correu electrònic en cadena.** A més a més de perdre el control sobre qui pot veure la teva adreça de correu electrònic, podries contribuir a transmetre un virus o un missatge fals. Pensa que molts d'aquests missatges s'utilitzen de vegades per obtenir dades disfressats d'una bona causa: buscar una nena que s'ha perdut, recollir signatures per a un nen que necessita diners per operar-se urgentment, etc. Sempre et demanen que enviïs el missatge en cadena a totes les persones que puguis.
5. **No proporcionis dades personals als xats, per missatgeria instantània ni als correus electrònics.** Es podria tractar d'un engany. Els llocs de confiança mai no demanen així aquestes dades. Si reps una sol·licitud d'aquesta mena d'una empresa en la qual confies, comprova l'autenticitat del missatge abans de respondre-hi. El telèfon també és un bon mètode per assegurar-se'n.

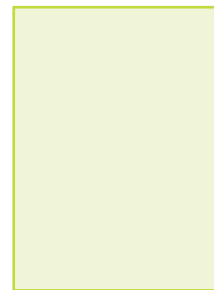


ACTIVITAT: ALTERACIÓ D'IMATGES

Hi ha persones que oculten la seva identitat i busquen informació personal sobre altres persones utilitzant noms i altres dades falsos. Et poden demanar dades com ara el nom i els cognoms, el DNI, el correu electrònic, l'adreça, els gustos o les contrasenyes, així com **alguna foto**.

Si envies **fotos teves, dels teus familiars o dels teus amics** a llocs d'Internet que no coneixes, les poden utilitzar amb finalitats molt diferents de les que t'imagines.

Per això, evita enviar i compartir fotos personals amb persones desconegudes. Una foto és per sempre. Pensa-hi.



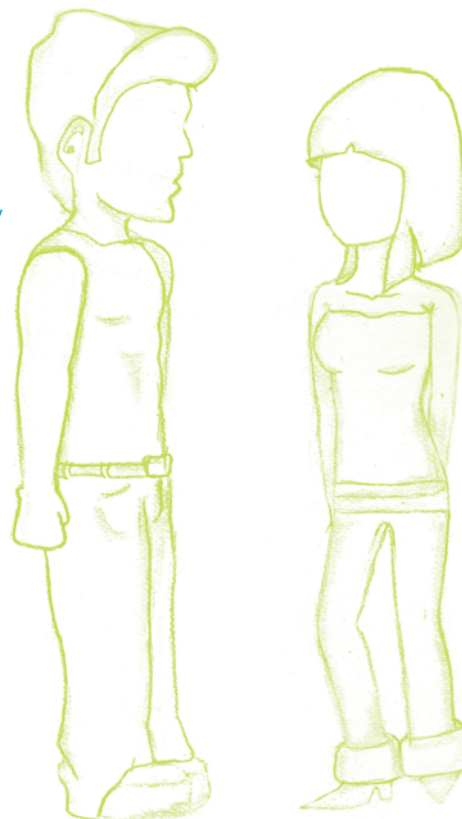
La meua foto

El *Bluetooth* dels telèfons mòbils és una manera molt fàcil i ràpida de compartir fotos, programes i arxius. Això augmenta el risc que hi entrin virus o t'enviïn correus brossa. Vés amb compte.

Saps que hi ha programes d'ordinador que canvien les fotos i les imatges, de manera que et poden posar al costat d'altres persones, en altres llocs i, fins i tot, et poden alterar la roba, els cabells, etc.?

Fes-ne una pràctica amb aquests dibuixos i canvia tu mateix la imatge d'aquestes persones, alterant-los els cabells, els trets de la cara, l'alçada, la manera de vestir, etc.

Tot això es podria fer amb qualsevol programa de tractament d'imatges de l'ordinador.



RECORDA

DONAR LES TEVES DADES PERSONALS A PERSONES DESCONEGUDES PER INTERNET ÉS PERILLÓS.

PROBLEMA 2: TROBADES AMB PERSONES DESCONEGUDES: EN LÍNIA I REALS (CITES A CEGUES)

Pensa la quantitat d'hores que passem davant la presència lluminosa d'una pantalla. Pantalles a casa, a la feina, al carrer, als bars, als bancs, al metro, al cotxe, pantalles de butxaca a les agendes electròniques, a les calculadores, als telèfons mòbils, etc. Les pantalles ens sedueixen i ocupen un espai creixent en les nostres vides.

Actualment, milions d'homes i dones de totes les edats utilitzen les possibilitats que els ofereixen les xarxes per comunicar-se amb persones que ni tan sols coneixen físicament. Moltes d'elles ho fan per entretenir-se, altres busquen amics per compartir bons moments i n'hi ha que van a la recerca d'una relació sentimental. Fins i tot hi ha persones que prefereixen el contacte a través d'una pantalla i un teclat que trobar-se cara a cara. Substitueixen els gestos, les mirades, la presència en general, pels clics del ratolí. Internet s'erigeix en un canal que facilita les relacions afectives amb eines com ara el correu electrònic, el xat o els llocs web.

En l'estudi que hem elaborat, els nois i les noies de 12 a 14 anys manifesteu en el 70 % que la vostra forma preferida de relació és el **xat**, que us arriba a ocupar fins a la meitat del temps que esteu connectats. Com molts de vosaltres ja deveu saber, el xat és com una gran sala de reunions en la qual qui entra es troba de manera virtual amb un munt de gent amb la qual pot compartir textos, veu, fotos, vídeos o programes des del seu ordinador. En alguns casos s'aprofita per quedar en un lloc determinat. Es tracta de les cites a cegues, que solen ser molt perilloses. Creus que moltes d'aquestes persones són de la teva mateixa edat, gustos, etc., i potser no és així. No saps quines intencions tenen. Algunes poden ser més grans del que diuen i tenir intencions deshonestes. El 20 % de les enquestes manifesten que alguna vegada heu rebut alguna proposta d'aquest tipus. Les dades indiquen que el 95 % dels pederastes (majors d'edat que abusen sexualment de menors) coneixen les seves víctimes a través dels xats.

La realitat també ens pot enganyar. Té moltes cares i, de vegades, només en veiem una. Et proposem un joc. Observa la imatge d'aquesta dona. Porta un mocador al cap i una ploma als cabells. Calcula quina edat deu tenir i compara-la amb la que proposen els teus companys.



Com has pogut comprovar, de vegades no ens posem d'acord en una cosa aparentment fàcil a simple vista.

Potser ja coneixes el mite grec de Narcís. La versió de l'escriptor clàssic Ovidi explica que un dia Narcís tenia set i es va acostar a beure en un rierol, i va quedar fascinat per la bellesa del seu reflex. Ni tan sols no es va atrevir a beure per por de danyar-lo. Incapaç de deixar de mirar-lo dia i nit, finalment va morir contemplant la seva imatge. La flor que porta el seu nom va créixer al lloc on va morir Narcís (pots ampliar aquesta informació a Internet).

Observa el quadre següent, del pintor català Dalí, en el qual es representa aquest mite, i descriu el lloc on situa el personatge i els objectes que hi veus. Parlant d'ordinadors, què creus que podria ser el fons d'aigua cristal·lina en el qual es mira Narcís?



La metamorfosi de Narcís (Salvador Dalí, 1937)

Escriu les teves pròpies conclusions sobre aquestes dues activitats amb relació al que estàs aprenent:

La imatge de la dama:

.....

.....

El mite de Narcís:

.....

.....

RECORDA

SI VOLS QUEDAR AMB ALGÚ QUE HAS CONEGUT A TRAVÉS DE LA XARXA, HO HAS D'EXPLICAR A ALGUNA PERSONA ADULTA EN QUI CONFIÏS.

PROBLEMA 3: ASSETJAMENT ELECTRÒNIC (CYBERBULLYING)

A Internet, com en el món real, hi ha persones en les quals es pot confiar i altres que intenten aprofitar-se'n en tot moment. Imagina't que aquestes persones poguessin, d'una manera anònima, utilitzar l'ordinador o el telèfon mòbil i, per mitjà d'Internet, humiliar, agredir, maltractar, insultar, amenaçar o desprestigiar altres persones. Pensa que l'anonimat pot ser la millor disfressa per refugiar-s'hi i enviar missatges desagradables (violents o de contingut sexual) o inventar històries que facin que altres persones se sentin malament.

Moltes vegades utilitzen les fotos que les seves «víctimes» han penjat a Internet dins el seu espai personal (pàgina web o bloc), o fins i tot es figuren dins el seu ordinador a través de virus per robar-los les fotos, manipular-les i exposar-les a Internet per avergonyir i humiliar aquestes persones.

Normalment solen utilitzar:

- El correu electrònic, l'entrada en un xat o l'enviament de missatges pel mòbil.
- La participació de jocs a la xarxa. Et demanen informació personal o que facis determinades tasques. Tot, perquè puguis «pujar un nivell» en el joc.

Si algú t'envia informació desagradable en un xat, el millor és esborrar aquesta persona de la llista de contactes. Aquesta persona no sabrà qui ho ha fet. Mai no contestis els seus missatges ni les seves trucades. El millor és no facilitar l'adreça de correu electrònic ni el número de telèfon mòbil a persones desconegudes. Recorda que, si has facilitat aquestes dades, una vegada enregistrades són de domini públic i molta gent hi pot tenir accés.

A les enquestes fetes, els insults i la pornografia són els continguts no desitjats que més heu rebut a l'ordinador o al mòbil (dues de cada deu vegades).



ACTIVITAT: EL MIRALL DE BLANCANEU

En aquest context, et proposem que redactis un ciberconte basat en el clàssic Blancaneu i els set nans utilitzant els mateixos personatges del conte, però adaptats al tema de què tractem. Per fer-ho, et donem algunes pistes, perquè hi vegis les semblances:

- la reina malvada = l'assetjador
- el mirall = la pantalla de l'ordinador
- la persecució de Blancaneu = l'assetjament i la persecució d'alguna persona coneguda
- el servent o el vassall de la reina = la persona enviada per assetjar
- els nans = el grup d'amics
- la casa dels nans = el refugi
- el príncep = la persona que ajuda
- el petó = la solució ???

Inventa't el final que vulguis, però recorda introduir en algun moment una frase semblant a aquesta: «Mirall, mirall màgic, qui és la dona més bella i formosa del regne?».

I, si t'hi animes, el pots enregistrar en vídeo amb el teu grup d'amics i presentar-lo als teus companys (assegura't que tots hi estan d'acord).



UN CAS REAL D'ASSETJAMENT ELECTRÒNIC

Perquè completis la informació que tens sobre aquesta forma d'assetjament, t'exposem una notícia sobre un cas real. Llegeix atentament la notícia. I, si tu o algú del teu entorn pateix un cas semblant, no oblidis seguir els nostres consells i fer-ho saber als teus pares o professors, o, fins i tot, denunciar-ho davant l'Oficina del Defensor del Menor o la policia.

Arriba l'assetjament electrònic: xantatge a companys de classe per la xarxa

La Guàrdia Civil ha detingut a Crevillent (Alacant) dos escolars de 17 anys que havien inventat una forma molt curiosa de fer xantatge als seus companys.

Els dos menors van crear un troià (virus informàtic) que aconseguia activar les càmeres web dels ordinadors a les cases dels seus companys, i els enregistraven sense que ells ho sabessin en situacions compromeses (com ara mentre es despullaven a l'habitació).

Després els amenaçaven de difondre les imatges a l'institut si no els pagaven una quantitat d'entre 100 i 200 euros, expliquen a la Guàrdia Civil.

Falsificació de targetes

Els dos menors tenien molts coneixements d'informàtica i havien ajudat a uns altres dos joves, majors d'edat i que van ser detinguts a Madrid, a falsificar targetes de crèdit per fer-hi compres il·legals a Internet.

Havien arribat a estafar 60.000 euros.

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

PROBLEMA 4: FRAUS PER INTERNET

Et sorprendria saber que a l'Estat Espanyol ha augmentat en un 80 % el nombre de compres per Internet l'últim any. Això ho saben molt bé els lladres informàtics, els hackers. Per això et recomanem que segueixis aquestes mesures de seguretat.

La URL o adreça del navegador ha de començar per **https**, en què la s significa 'segur'. Exemple:

[https:// www.tumejorbanco.com](https://www.tumejorbanco.com)

També és important localitzar la icona del cadenet a la barra d'estat (part inferior) de l'explorador.

Per saber si el lloc web on ets és segur, comprova que tens una icona amb un cadenet groc tancat. Això significa que el lloc web protegeix tota la informació personal que donis. Fes doble clic sobre el cadenet; si el nom que apareix no coincideix amb el lloc on ets, es tracta d'un web fals.



En la mesura que puguis, t'has de connectar des d'un lloc segur, com ara casa teva. Els llocs públics com ara cibercafès, locutoris i biblioteques són llocs més fàcils perquè persones amb males intencions puguin registrar tot el que escriguis al teclat i apoderar-se de les teves dades confidencials.

PHISHING LA GRAN AMENAÇA



Si saps anglès, segurament quan hagi vist la paraula *phishing* et deus haver imaginat què vol dir. Mira els dibuixos anteriors i intenta explicar en què consisteix.

.....

.....

.....

.....

.....

Ara aprofundirem una mica més en aquest tema.

Es parla de pesca electrònica com de l'ús de tècniques per suplantar la personalitat i robar la identitat electrònica d'algu, de manera que així s'aconsegueix tenir accés a àrees o serveis privats d'una manera il·legal.

Un autèntic delicte de frau!

QUÈ ÉS LA IDENTITAT ELECTRÒNICA?

A Internet, per poder estar segurs, tots tenim un **nom d'usuari** i una **contrasenya** que ens permet entrar a l'ordinador, a llocs privats com ara el correu electrònic o a la banca per Internet, i a altres llocs públics. Possiblement deus haver vist els teus pares com accedien al seu compte del banc, o com feien o consultaven la declaració de la renda per Internet. És com la clau per entrar en una casa.

De vegades tu t'inventes la teva pròpia identitat electrònica, i altres cops te la faciliten ja creada (un banc o qualsevol altre organisme), però és convenient canviar-la de seguida. D'això se'n diu personalitzar.

Ara farem un exercici mental de lletres. Aquesta és la identitat d'algú de la teva edat. Fes de detectiu i intenta descobrir el nom veritable i la contrasenya. ESCRIU-LOS A LA PART DRETA.

Nom d'usuari: Mrt lpz frnndz

Nom d'usuari:

Contrasenya secreta: ## ## #####

Contrasenya:

(Trobaràs la solució al final del manual.) Si ho has encertat, treu-ne les teves pròpies conclusions.

Imagina't ara que un delinqüent s'apodera de la identitat electrònica dels teus pares al banc i els vol robar els diners. Com ho podria fer? Comenta-ho amb ells a casa.

Els pescaires (phisher), els delinqüents que porten a terme l'activitat de la pesca electrònica, utilitzen una combinació d'enginyeria social i elements tècnics per apropiarse de la identitat electrònica d'algú.

El procediment més utilitzat és enviar correus electrònics falsos dissenyats per atreure les víctimes a llocs igualment falsos. El procés típic és el següent:

1. Es difon massivament un correu brossa en el qual s'informa que els usuaris de la caixa o banc X han de confirmar les seves dades d'accés (identitat electrònica) al seu compte bancari.
2. El missatge inclou un enllaç a una pàgina des de la qual han de confirmar les seves dades personals.
3. L'usuari accedeix a l'enllaç que porta a una pàgina semblant a l'autèntica de la caixa o el banc X i, amb tota confiança, hi introdueix aquestes dades. Ja els ha donat la clau d'entrada!
4. Com que la pàgina és falsa i està controlada pels estafadors, són ells els que realment reben les dades de l'usuari, i d'aquesta manera tenen lliure accés al compte real de l'usuari estafat i li poden prendre o es poden gastar tots els diners.

Perquè ho entenguis millor, aquí tens un exemple real de correu de pesca electrònica trobat a Internet.

Una vegada hagis llegit aquest exemple, completa les dades que et demanem en aquest exercici per ajudar-te a entendre millor el procediment que utilitzen els pescaires (segueix els nombres).



1. T'envien aquest correu brossa amb el nom d'un suposat banc anomenat
2. Però qui realment envia el missatge és, de manera que no hi ha cap vinculació amb aquell banc.
3. Identifica l'assumpte del missatge, així com el text que escriu a continuació, i explica què vol dir. A quines dades es refereix si es tracta de Bancolombia?
4. Si poses el ratolí damunt el punt 3, enllaces amb una pàgina que simula ser el banc, però que en realitat és la pàgina web d'un estafador.

Si ets bon detectiu, trobaràs en algun lloc l'adreça real des de la qual s'envia el correu brossa:..... Ja els tenim! No esborris la prova i acudeix a una persona adulta perquè t'aconselli.

RECORDA

Davant aquest tipus de problemes, el primer que has de fer és explicar als teus pares o a una persona adulta responsable el que passa, i ells seran capaços d'ajudar-te. Si alguna vegada arribes a tenir problemes seriosos, pensa que no ets l'única persona que ha pogut fer alguna cosa equivocada.

Capítol 3

EL CORREU ELECTRÒNIC

El correu electrònic, en anglès **e-mail** (electronic mail), és un servei de xarxa que permet als usuaris enviar i rebre missatges ràpidament per mitjà de sistemes de comunicació electrònics. El nom prové de la semblança amb el correu postal, i utilitza «bústies» intermèdies, anomenades servidors, en què es guarden temporalment els missatges abans d'arribar a la seva destinació i que els rebi el destinatari. És necessària una adreça de correu electrònic que sigui personal i única per a cada usuari.

Quan et vulguis fer un compte de correu, has de tenir en compte els suggeriments següents:

1. **Crea una adreça que no sigui gaire típica.** Evita fer servir dades fàcils i que revelin la teva identitat (nom, any de naixement, etc.). Intenta utilitzar combinacions de lletres, nombres i altres caràcters. Per exemple: pepo2lea4@.....com.

Inventa-te'n ara una que no utilitzaràs mai.

.....@.....

2. **Disfressa la teva adreça de correu electrònic** quan la utilitzis en xats, fòrums de discussió o qualsevol altre tipus de pàgina web. Copia una altra vegada l'adreça que has escrit abans, però substitueix ara el símbol @ per la paraula *arrova* i el símbol . per la paraula *punt*.
3. **Compte amb les caselles marcades de forma predeterminada.** Algunes empreses inclouen caselles per indicar que tenen el teu consentiment per vendre o proporcionar la teva adreça de correu electrònic a altres persones. Si no hi estàs d'acord, marca-ho.

En cas contrari, i sense adonar-te'n, podries concedir el permís perquè aquestes empreses compartissin amb altres la teva informació personal.

4. Quan enviïs missatges a diverses persones, recorda d'incloure les seves adreces en còpia oculta.

Així evitaràs que la resta de persones coneguin les altres adreces i circulin per la xarxa, amb el perill que això representa. No sabem on poden anar a parar! Un procediment per enviar missatges amb còpia oculta pot ser buscar l'opció de mostrar CC (còpia) i CCO (còpia oculta), i introduir les adreces dels teus destinataris a la barra CCO.



Fes-hi clic i apareixerà això:



Escriu les adreces a la barra CCO.

Has de fer servir la teva adreça de correu electrònic preferentment amb les persones que coneixes o que et transmeten seguretat.

Recorda que també al telèfon mòbil queden enregistrats els noms de les persones amb qui has parlat i els missatges que has enviat.

Observa en aquesta pàgina les dades que et solen demanar per registrar-te com a usuari d'un compte de correu:

BENVINGUT O BENVINGUDA!

Si vols tenir un compte de correu electrònic amb nosaltres, només has de contestar unes preguntes, triar el teu nom d'usuari i la teva contrasenya, i llestos!

1. Les teves dades personals

1.1 Nom:

1.2 Sexe:

1.3 Data de naixement:

1.4. Lloc de naixement:

1.5 Codi postal:

2. Selecciona el teu ID (nom de la teva nova adreça de correu) i contrasenya:

.....@.....com

Només es permeten lletres, nombres, guions baixos i un sol punt (.). En total, 8 caràcters.

Ej: pepa4.lea @.....com

Si no està disponible l'ID que vols fer servir, canvia lletres o algun nombre perquè sigui única.

2.1 Contrasenya:

2.2 Repeteix la contrasenya (per seguretat):

Per si oblides la contrasenya, et fem una pregunta de seguretat:

Hi estàs d'acord?

Si marques aquesta casella, indiques que has llegit i acceptes les condicions de servei i les del centre de privadesa, i que també acceptes rebre les notificacions oportunes en format electrònic que t'envii aquesta empresa o altres.



Capítol 4

ELS NOSTRES DRETS

4.1 SOM CIUTADANS: PROTECCIÓ DE DADES PERSONALS

Pensa que, com a ciutadans residents a Catalunya, i emparats per la Constitució espanyola (article 18) i l'Estatut D'Autonomia, tenim dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge, així com a la protecció de les nostres dades personals.

Aquests drets ens reconeixen i ens permeten reconèixer-nos com a individus únics i diferenciats davant els altres: el nom sencer, l'adreça de casa nostra, les fotos pròpies o de la família, la veu enregistrada en qualsevol aparell, les empremtes dels dits de la mà, etc. ens pertanyen en propietat des del moment en què naixem.

Quan facilites aquestes dades a una entitat (escola, banc, club, ajuntament, etc.) o algú les obté, es guarden en un fitxer manual o informàtic, i hi ha una persona que se'n fa responsable i informa sobre la finalitat, el contingut i l'ús d'aquest fitxer. A més, aquesta persona ha de guardar secret absolut sobre el seu contingut i tenir les dades custodiades en un lloc segur.

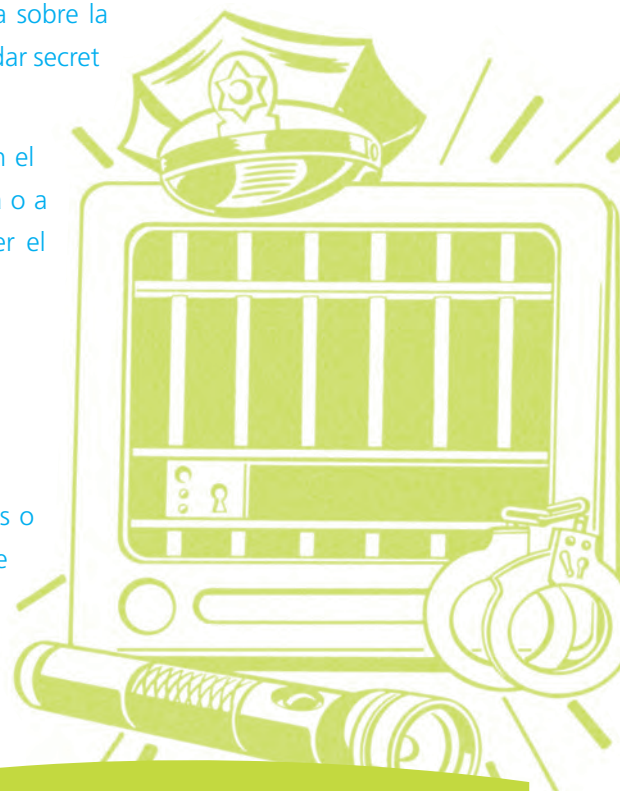
Davant aquest fitxer podem exercir els nostres drets i de manera gratuïta. En el cas dels menors de 14 anys, ho han de fer els seus pares o tutors. A l'escola o a l'institut, la persona a qui t'has d'adreçar com a primer responsable sol ser el director o la directora, o el secretari o la secretària del centre.

També els estatuts d'autonomia emparen i reforcen aquests drets.

Aquests són els teus drets:

1. Dret d'accés a les dades

És la possibilitat de saber quines dades personals teves tenen arxivades o recollides altres persones, l'origen i les comunicacions o cessions que s'hagin fet a altres persones o es vulguin fer. Si volem saber-ho, ens adreçarem al responsable del fitxer, que té un termini màxim d'un mes per contestar.



2. Dret de rectificació i dret de cancel·lació

Si crec que les dades que hi ha en aquest fitxer són errònies, incompletes o inadequades perquè no són necessàries per a la finalitat que es pretén, ho faré saber al seu responsable perquè:

- o bé rectifiqui les dades,
- o bé les cancel·li, les bloquegi perquè no puguin ser usades ni tractades i, fins i tot, les esborri definitivament.

En aquest cas també he d'adreçar la sol·licitud al responsable del fitxer, que ha d'atendre la meva petició en un termini de deu dies.

3. Dret d'oposició

També puc demanar que no es tractin algunes de les meves dades personals. Per exemple, que el número de telèfon de casa meva no surti a la guia telefònica de la meva localitat.

No oblidis que:

- Ets l'amo absolut de les teves dades personals i no estàs obligat a donar-les a ningú, excepte si t'hi obliga una llei.
- Sempre tens el dret a controlar-les en tot moment i a saber què se'n fa.
- Pots donar les teves dades i permetre que les utilitzin si ets més gran de 14 anys. Si ets més petit, només ho poden fer els teus pares.
- Ningú, i en cap cas, et pot obligar a donar dades referides a la teva ideologia, religió o creences personals, ni les poden utilitzar sense el teu consentiment exprés i per escrit. Les dades sobre la salut, l'origen ètnic o la vida sexual només es poden recollir en el cas que hi hagi una llei que ho disposi per raons d'interès general.



- Desconfia de les persones que et demanen les dades personals amb l'excusa de voler completar les que ja tenen. Pensa que les han pogut obtenir per Internet (concessió de beques per a estudis, inscripció o participació en curses o esdeveniments esportius, dades dels teus pares, etc.).
- Quan et demanin les dades personals per qualsevol mitjà, ja sigui per telèfon, per escrit o per Internet, has d'avisar els teus pares, perquè tu i ells heu de saber qui les necessita i amb quina finalitat, on les guardarà, quines mesures de seguretat els aplicarà i qui és la persona encarregada d'utilitzar-les.
- La persona responsable del fitxer t'ha de demanar sempre el consentiment per cedir les teves dades a una altra entitat o empresa, i ha d'informar sempre de l'existència d'aquest arxiu, del seu contingut, de la seva finalitat, de l'origen de les dades, de com les ha aconseguit, dels teus drets, de qui són les persones destinatàries de la informació, de la identitat del responsable i de la seva adreça.
- Sempre que algú reculli les teves dades, hi han de figurar clarament els drets dels que hem parlat. Llegeix-los atentament amb els teus pares. Al final de cada formulari hauries de trobar frases com aquestes:

«Les dades personals es recolliran i es tractaran al fitxer [...], la finalitat del qual és [...], inscrit en el Registre de Fitxers de Dades Personals de l'Agència de Protecció de Dades de [...], i es podran cedir a [...], a més d'altres cessions previstes a la llei. L'òrgan responsable del fitxer és [nom i adreça]».

FITXER amb les meves
dades personals

Són correctes

Són errònies, incompletes
i inadequades

Dret d'accés

Dret de cancel·lació

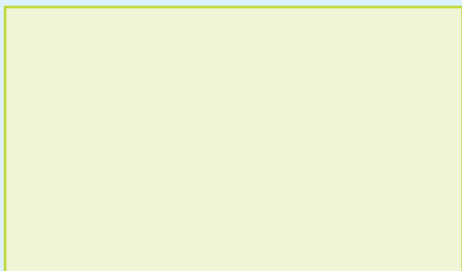
Dret de rectificació

Et proposem ara un exercici pràctic per aplicar aquests drets, a partir de l'estudi d'un cas trobat a Internet.

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

FITXA D'INSCRIPCIÓ

Foto actual, amb indicació del 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:

Ètnia:

Malalties o al·lèrgies:

Religió:

Condicó sexual (heterosexual o homosexual):

Estaries disposat o disposada a:

- | | | | |
|---|----|----|-------|
| • tenyir-te els cabells? | SI | NO | DEPÈN |
| • tallar-te els cabells? | SI | NO | DEPÈN |
| • desfilat amb roba de bany? | SI | NO | DEPÈN |
| • fer nus parcials (topless)? | SI | NO | DEPÈN |
| • ser enregistrat o enregistrada durant el dia sense que sàpigues quan? | SI | NO | DEPÈN |
| • Consentiries l'emissió d'aquestes imatges enregistrades seleccionades per la productora Globo Tour RTV? | SI | NO | DEPÈN |

Aficions:

.....

.....

.....

.....

Indica si t'has presentat abans a algun altre concurs de televisió i en quina cadena

.....

.....

.....

.....

Una vegada acabades les proves de selecció, es publicarà a la nostra pàgina web el nom, el DNI i l'adreça de correu electrònic de cadascuna de les persones seleccionades per l'empresa Globo Tour RTV, S.A., Barcelona.

Una vegada hagi llegit la fitxa d'inscripció del càsting, contesta aquestes preguntes:

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

.....

.....

2. Quina és la finalitat principal d'aquesta empresa quan demana aquestes dades?

.....

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

.....

.....

4. Si facilites aquestes dades, quines creus que haurien d'estar especialment protegides?

.....

.....

5. Ja saps que les teves dades personals es poden guardar de manera manual o en un fitxer informàtic. Quin nivell de seguretat ha de tenir l'empresa?

.....

6. Hi ha una llei de protecció de dades personals. Si s'infringís, qui en seria el responsable?

.....

7. Imagina't que, al cap d'un mes del càsting, algú vinculat al programa es presenta a casa d'un concursant per vendre-li equips de música i karaokes. Què hauria d'haver demanat el propietari de l'empresa Globo Tour RTV, S.A. a aquest concursant per poder utilitzar aquestes dades amb altres finalitats?

.....

.....

8. Imagina't que vols denunciar la productora per haver fet un mal ús de les dades de què disposa.

.....

.....

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

4.2 SOM PERSONES

La Convenció Internacional dels Drets de l'Infant estableix que tots els nens i les nenes tenen drets que han de ser respectats i promoguts per totes les persones.

Alguns d'aquests drets són els següents:

- Dret a la protecció contra qualsevol forma de maltractament (article 19).
- Dret a un nivell de vida adequat al seu desenvolupament físic, mental, espiritual, moral i social (article 27).
- Dret al descans i l'esbarjo, al joc i a les activitats recreatives pròpies de la seva edat (article 31).
- Dret a ser protegit contra qualsevol forma d'explotació que sigui perjudicial per a qualsevol aspecte del seu benestar (article 36).



Capítol 5

CONSELLS PER A PARES I MARES, EDUCADORS I EDUCADORES, O TUTORS

Internet pot ser un lloc excepcional perquè els nois i les noies aprenguin, s'entretinguin, parlin amb els amics de l'escola o l'institut, o, simplement, es relaxin i explorin. Però, de la mateixa manera que el món real, la xarxa pot ser especialment perillosa per a ells. Abans de deixar que el vostre fill o filla s'hi connecti sense la vostra supervisió, assegureu-vos d'establir un conjunt de regles que tots pugueu acceptar.

En l'estudi elaborat hem detectat algunes dades preocupants pel que fa a la facilitat dels joves d'aquesta edat a facilitar les seves dades personals. Prop del 35 % ho fan sense problemes per ingressar en un club virtual o per fer un càsting, un percentatge que se supera quan es tracta de donar l'adreça de correu electrònic o el número de telèfon mòbil. I, a més, aquestes dades augmenten amb l'edat fins als 17 anys.

Si no sabeu per on començar, a continuació us oferim algunes idees que podeu comentar amb els vostres fills per ensenyar-los a utilitzar Internet d'una manera segura.

DE CARÀCTER GENERAL

1. Intenteu estar al dia en qüestions d'Internet i del telèfon mòbil. Com més informació tingueu sobre aquestes tecnologies, millor podreu ajudar els vostres fills a fer-ne un bon ús.
2. Mantingueu-hi un diàleg fluid sobre el que fan a Internet, amb qui hi parlen o quines pàgines web visiten més. Establiu entre tots unes regles bàsiques d'ús i consum de les tecnologies. Gaudiu d'Internet tots plegats.
3. És recomanable situar l'ordinador en un lloc comú de la casa. No s'aconsella que tinguin l'ordinador en una habitació sense control.
4. Controleu el temps que passen els vostres fills a Internet o amb el telèfon mòbil. Establiu uns horaris d'ús que s'adaptin al temps d'estudi.
5. Aviseu-los que no han d'acordar una cita «en persona» amb amics coneguts per Internet o pel telèfon mòbil. Expliqueu-los que els amics en línia potser no són el que diuen que són.

SOBRE L'ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ

6. Instal·leu un antivirus, un tallafocs i programes de filtratge de correu brossa a l'ordinador, i assegureu-vos d'actualitzar-los periòdicament.
7. Prepareu diferents inicis de sessió personalitzats per a cada fill o filla.
8. Configureu el vostre compte com el d'administrador de l'equip, per controlar el que pot fer i no pot fer cada usuari de l'ordinador.
9. Si els vostres fills envien missatges o visiten sales de xat, juguen a videojocs en línia o fan altres activitats a Internet que requereixin un nom d'inici de sessió per identificar-se, ajudeu-los a triar-lo i comproveu que fan servir contrasenyes segures, que no les comparteixen amb ningú i que no revelen cap altra informació personal. Al mercat hi ha una àmplia varietat de programes amb més opcions de seguretat i de filtratge de continguts.
10. Estigueu al corrent dels jocs que es baixen o intercanvien amb els amics. Assegureu-vos que el contingut és l'adequat a la seva edat i no inclou cap tipus de violència.
11. Acompanyeu els vostres fills quan es baixin programes, música o arxius, encara que siguin legals. Ensenyeu-los que, si comparteixen arxius o copien textos, imatges o dibuixos d'un web, ho han de fer sense infringir les lleis de drets d'autor.

SOBRE LA PROTECCIÓ DE DADES PERSONALS

12. Parleu amb els vostres fills sobre la importància de protegir les dades personals. En aquest manual recollim els drets que ens emparen com a ciutadans, que es recullen a la legislació de protecció de dades de caràcter personal, tant estatal com autonòmica.
13. Ensenyeu als fills adolescents que mai no han de facilitar informació personal sense el vostre permís quan utilitzen el correu electrònic, les sales de xat o la missatgeria instantània, quan emplen formularis de registre i de perfils personals, o quan participen en concursos en línia.

Capítol 6

CONSELLS PER A ESTUDIANTS

SOBRE L'ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ

Per navegar per la xarxa sense problemes, hauries de seguir les recomanacions següents:

1. Tingues una contrasenya secreta que no faciliti informació personal. No facis servir mai el teu nom real. Si utilitzes missatgeries o entres en xats privats, fes-ho només amb els teus amics. Mai no parlis amb persones desconegudes!
2. Aprèn a utilitzar i mantenir actualitzat un antivirus i altres bloquejadors. Així evitaràs que entrin a l'ordinador espies que podrien tenir accés a la informació que hi guardes.
3. No obris fitxers ni missatges de persones desconegudes, ni et baixis programes que no coneixes.
4. Si obres un bloc o tens un espai personal a la xarxa, convida-hi només els teus amics. Si no és així, les teves dades poden anar a parar a les mans de qualsevol persona!
5. No donis mai les teves dades personals a persones desconegudes: el nom i els cognoms, on vius, el nom d'usuari de Messenger, el número de telèfon (mòbil), etc.



Recorda que has d'utilitzar l'ordinador i el telèfon mòbil seguint els consells dels teus pares, tutors o professors. Consulta amb ells qualsevol dubte que tinguis.

SOBRE LA PROTECCIÓ DE DADES PERSONALS

Imagina't que a la teva escola o institut hi ha una empresa que selecciona els millors dibuixants de la teva classe per il·lustrar un llibre de contes. Els més originals tindran com a premi un reproductor de música d'última generació. Juntament amb els dibuixos, et demanen que emplenis un formulari amb les teves dades personals. Recorda quines coses ha de fer aquesta empresa:

6. T'ha d'informar sobre la finalitat amb la qual s'utilitzaran les dades, i també sobre els teus drets en aquest tema: dret d'accés a les dades que té sobre tu, de rectificació (si són inexactes o excessives), de cancel·lació i d'oposició.
7. T'ha de demanar el teu consentiment per poder utilitzar-les o tractar-les. Si ets més petit de 14 anys, ho han de fer per tu els teus pares o tutors.
8. T'ha de demanar únicament les dades necessàries per a la finalitat perseguida. Per exemple, per ingressar en un club esportiu no t'han de preguntar sobre els teus gustos musicals, no trobes?
9. T'ha d'assegurar que les dades estaran segures i es mantindran en secret.

Recorda que hi ha organismes com ara l'Agència Espanyola de Protecció de Dades, així com les agències autonòmiques (de Madrid, Catalunya i el País Basc), que sempre et poden ajudar gratuïtament davant qualsevol tema que no coneguis.

SOLUCIÓ A L'ACTIVITAT DEL PROBLEMA 4

Nom d'usuari: marta lopez fernandez

Contrasenya: aa oe eae

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

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

EUSKADI

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

EXTREMADURA

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

MADRID

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



**Comissió
de Llibertats
i Informàtica**

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