
A INTERNET
POSA-HI SENY!!
You
Tube
Descar
35%

CONSELLS GENERALS DE SEGURETAT

Quan naveguem per Internet o usem el mòbil (parlem amb els amics a través de xats, utilitzem les xarxes socials o compartim imatges, vídeos i arxius) hem de fer-ho amb seguretat per evitar problemes.

Cal estar alerta quan naveguem per la xarxa perquè Internet és un mitjà que també utilitzen els delinqüents per cometre fraus, robar dades, assetjar, etc.

A continuació et donem una sèrie de consells perquè la teva experiència a Internet sigui positiva.

NAVEGANT PER INTERNET... AMB SEGURETAT

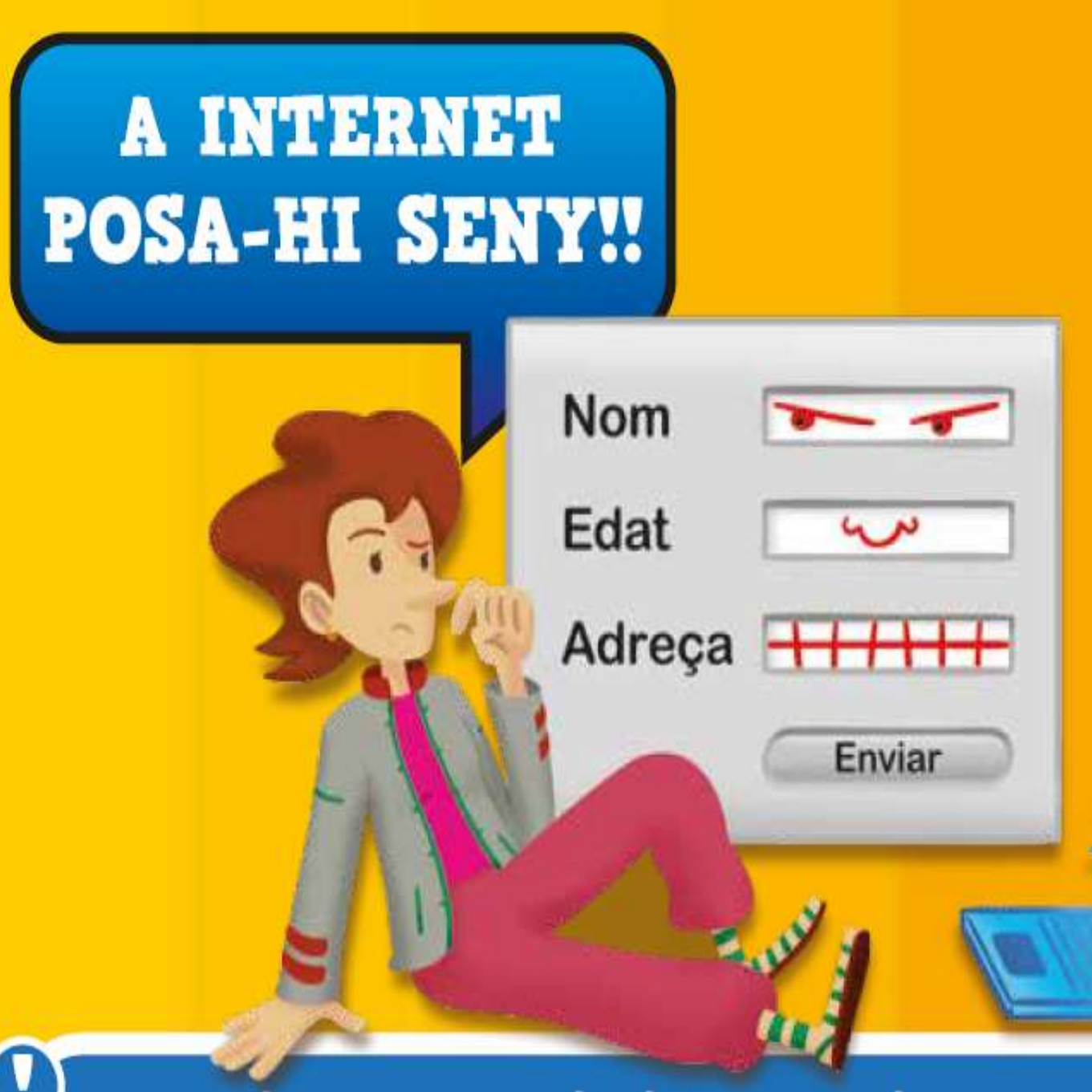
Internet és un lloc ple d'oportunitats on pots aprendre, comunicar-te amb amics arreu del món, jugar... i divertir-te d'allò més. Cada cop tenim més continguts de qualitat pensats expressament per a les teves necessitats i que esperen que els descobreixis.

Cada dia hi ha nous riscos a Internet. Si n'ets una víctima o t'han advertit gràcies a algun avís, cal que ho comparteixis amb els teus amics i familiars. D'una banda, si ho expliques a algú més experimentat et podrà ajudar amb bones solucions, i de l'altra, si és algú més novell a Internet el prevens del que li pot passar.

Aquesta és una guia de recomanacions perquè gaudeixis de la xarxa de forma més segura.

I RECORDA... A INTERNET, POSA-HI SENY!

A INTERNET POSA-HI SENY!!



NAVEGANT PER INTERNET

• Intenta sempre navegar per pàgines segures i de confiança. No tothom té bones intencions a la xarxa, per això has de fixar-te en les indicacions que et fan navegadors i els antivirus sobre el risc de la pàgina que obres.

• No desactivis l'antivirus ni el tallafocs en cap moment. Ho poden aprofitar per infectar el teu dispositiu[1], copiar la teva identitat o informació, i fins i tot es poden fer passar per tu o pots perdre tot el que hi tens guardat.

• Usa contrasenyes complicades que siguin llargues, barregin lletres, majúscules i minúscules, nombres i símbols especials per registrar-te com a usuari en un lloc web. Mai facis servir el nom, la data de naixement, el telèfon o el DNI com a contrasenya. Són massa fàcils de descobrir.

• Obre només els correus electrònics de les persones que coneguis. Esborra els missatges sospitosos i no et descarreguis els arxius que sovint s'hi adjunten perquè poden incloure virus.

• No facilitis les teves dades personals ni les d'altres persones quan visitis webs de poca confiança. Quan deixis les teves dades, assegura't perquè les volen.

• No te'n refiïs de tot allò que trobis o llegeixis a Internet. Intenta verificar-ho, i si tens algun dubte demana l'ajuda dels pares o els tutors.

1 Són dispositius: l'ordinador de sobretaula, el portàtil, la tauleta tàctil, el mòbil, els telèfons intel·ligents (*smartphone*)...

SI FAS SERVIR MÒBIL O TAULETA TÀCTIL

A LES XARXES SOCIALS

Les xarxes socials et permeten conèixer gent i tenir amics arreu del món. Pots compartir fàcilment molta informació amb tots els teus contactes i te n'arriba molta altra de persones que no coneixes a la vida real. Les més usades són Facebook, Twitter, Google+ o Tuenti però n'hi ha altres: Bebo, hi5, Instagram, ask.fm, Tumblr, Taringa,...

Hem de saber que l'ús massiu i de forma desinhibida de les xarxes socials fa que hi hagi persones que les usen per fer malifetes (estafes, fraus, suplantació, assetjaments,...). Per això cal estar alerta si no en volem ser víctimes:

• No acceptis "amistats" de desconeguts. A Internet és molt fàcil dir mentides i fer veure que ets una altra persona.

• Publicar informació a les xarxes socials és molt fàcil i ràpid, però un cop publicada no saps quin ús en poden fer. Allò que inicialment pensem que tindrà un ús privat pot arribar a ser desastrós si algú ho fa públic.

• Fes servir un àlies (*nick*) que només coneguin els teus amics quan obris un compte en una nova xarxa social (així evites que qui no et coneix et busqui pel teu nom i cognom).

• Si algú et molesta o t'assetja en algun xat o grup, surt del grup i avisa els teus pares o els tutors. Sigues tu també respectuós amb totes les persones del grup.

• No comparteixis dades com el telèfon, l'adreça o el teu nom i cognoms. No enviïs mai les teves fotos ni donis les teves dades personals a cap desconegut. Només fes servir les teves dades personals quan confirmis que tens el control de qui pot arribar a veure-les.

• A Internet no tothom és amic. No hauries de quedar amb les persones que coneguis a la xarxa. I si al final et trobes amb algú, avisa els teus pares o algun amic que t'acompanyi i queda sempre en un lloc públic.

• Compte amb els enllaços d'arxius de persones que coneguis al xat perquè podrien incloure algun virus. Fins i tot les cançons o les fotos que t'envien poden ser perilloses.

SI FAS SERVIR MÒBIL O TAULETA TÀCTIL

• La missatgeria instantània és molt popular en els mòbils: Whatsapp, Line, BlackBerry Messenger, Skype, Hangouts,... No hem de perdre de vista que moltes de les coses que ens podem dir amb text poden ser més valorades si es comuniquen cara a cara.

• Perquè no te'l prenguin evita exposar-lo davant els amics i protegeix el desbloqueig amb un patró gràfic, un pin o una contrasenya.

• Sospita de trucades i SMS de desconeguts i ocults. No donis dades personals sense estar del tot segur de qui hi ha a l'altre costat de la línia.

• Descarrega't només les aplicacions de mòbil que estan als *markets* oficials (Iphone, Android, Blackberry,...) per evitar que incloguin virus, siguin fraudulentes o espiïn les teves dades.

• Evita l'ús de xarxes wi-fi obertes de les quals no coneixes el propietari. Algú pot tenir control de les sessions a la teva xarxa social o al teu correu electrònic quan l'obris des del mòbil.

• Hem de configurar les opcions de l'aparell perquè respecti la nostra privacitat. Hem de vigilar quan donem permís per connexions de proximitat amb altres dispositius (Bluetooth) i la nostra geolocalització (GPS) que demanen diferents serveis (Google Maps, Twitter, Foursquare, Instagram,...).

• Abans de compartir una notícia o publicar una fotografia o vídeo pensa-t'ho bé. No facilitis o publiquis dades, informació, fotografies o vídeos d'altres persones sense que t'hagin donat el seu permís.

• Cal vigilar la gran difusió que poden arribar a tenir les imatges amb contingut sexual que poden ser gravades i compartides en grups de missatgeria instantània.

• Si omples formularis amb les dades personals o per fer compres des del mòbil assegura't d'usar comunicació segura https i amb el 3G actiu.

DESCARREGANT ARXIUS

• Si descarregues o intercanvies arxius fes-ho només en llocs segurs i de confiança. No t'inscriguis en pàgines insegures.

• Has de saber que intercanviar música, vídeos i pel·lícules a través de programes P2P infringeix els drets de propietat intel·lectual si el seu autor no ho autoritza expressament.

• Si no coneixem bé l'origen d'un arxiu (tant d'un llapis de memòria com d'una baixada) ens exposem a què tingui algun virus maliciós (*malware*), per això cal analitzar-lo amb un antivirus abans d'obrir-lo.

• No utilitzis les xarxes P2P per difondre continguts ofensius, degradants o humiliants per a altres persones. Et poden denunciar per fer-ho.

JOCS EN XARXA I AL MÒBIL

• Quan juguis en línia amb els teus amics vigila les pàgines on accedeixes i no donis mai dades personals (nom, adreça, telèfon,...) ni dades bancàries.

• No realitzis mai cap compra a través de la xarxa sense estar acompanyat dels teus pares o tutors.

• Controla el temps que dediques al joc. L'evasió que provoquen molts jocs ens fan caure en l'addicció o ens fan oblidar de les coses importants.

RECOMANACIONS PER A PARES I EDUCADORS

• Reviseu l'ús que fan del dispositiu i pacteu unes condicions (horari d'utilització, tipus de serveis autoritzats i límits de consum) abans de lliurar-los-hi.

• Comproveu que l'antivirus, el sistema operatiu i els navegadors estan sempre actualitzats i operatius. Activeu mesures de control parental que evitin que el menor accedeixi a continguts nocius i/o perillosos o per fer el seguiment de quin ús fan d'Internet.

• Expliqueu als menors la importància de les dades personals i especifiqueu quines dades poden facilitar i quines no.

• Acordeu quines pàgines es poden visitar (agregant-les a la llista de favorits) i reviseu junts l'historial de navegació que queda enregistrat a l'ordinador.

• Estigueu alerta amb les noves amistats que poden fer a les xarxes socials i parleu amb ells si veieu algun comportament estrany.

• Acordeu els horaris de connexió, l'ús que poden fer dels diferents dispositius i assegureu-vos que no descuiden les activitats escolars i que realitzen altres activitats (esport, quedar amb els amics, etc.).

1 . ANTIVIRUS

Són programes que actuen com a guardaespatlles del nostre ordinador. Estan alerta davant possibles virus que puguin atacar els nostres aparells (vegeu virus).

2. CIBERASSETJAMENT *(cyberbullying)*

És una forma d'assetjament a un individu o grup i consisteix en atacs personals difosos mitjançant les tecnologies de la informació i la comunicació (Internet, telèfon mòbil, etc.). L'assetjament engloba qualsevol tipus de maltractament psicològic, amenaces, xantatges, insults, menyspreus, etc.

3. CONTRASENYA SEGURA

És aquella que altres persones no poden determinar fàcilment endevinant-la o utilitzant programes informàtics. Per crear una contrasenya segura que puguis recordar fàcilment però que sigui difícil de determinar per terceres persones intenta una de les tècniques següents:

- No utilitzis contrasenyes que siguin paraules presents a qualsevol diccionari o noms (el de l'usuari, personatges de ficció, membres de la família, mascotes, marques, ciutat on vius,...).
- Tria una contrasenya que barregi caràcters alfabètics (majúscules i minúscules), numèrics i símbols. Ha de tenir com a mínim 8 caràcters o més.
- Estableix contrasenyes diferents per a sistemes diferents. Pots usar una contrasenya base i certes variacions lògiques d'aquesta per a diferents llocs. Això permet que si et roben una contrasenya no perdis també els accessos a tots els altres llocs on tens compte.

4. CONTROL PARENTAL

És qualsevol eina que permet els pares o els tutors supervisar i/o limitar l'ús que el menor fa de l'ordinador o d'Internet. Aquests controls ajuden a seleccionar els jocs i els programes que poden usar els menors, així com els llocs web que poden visitar i quan poden fer-ho.

5. CORREU BROSSA O *SPAM*

Els missatges no sol·licitats, habitualment de tipus publicitari, enviats de forma massiva. La via més utilitzada és el correu electrònic, però pot presentar-se per programes de missatgeria instantània o per telèfon mòbil.

6. CIBERASSETJAMENT A MENORS O *GROOMING*

Es refereix a l'assetjament de caràcter sexual a un menor. Les accions dutes a terme tenen l'objectiu d'establir una relació i un control emocional sobre un/una nen/a per a després abusar-ne sexualment. A diferència del ciberassetjament aquest tipus d'assetjament té un objectiu explícitament sexual. (Vegeu ciberassetjament)

7. DADES PERSONALS

Són les informacions escrites, gràfiques o imatges relacionades amb una persona i que serveixen per identificar-la, contactar-la i/o localitzar-la. Es consideren dades personals, doncs, el nom, l'edat, l'adreça, el número de telèfon, el número del carnet d'identitat, les contrasenyes i el números de comptes bancaris, entre d'altres. Internet ha fet que sigui més fàcil recopilar aquest tipus d'informació i fer-ne un mal ús.

8. MISSATGERIA I NSTANTÀNIA

És un sistema que permet conversar de forma escrita entre dues o més persones en temps real per Internet.

Els programes usats permeten guardar una llista de contactes o grups i, si es troben disponibles, es pot fer xat i intercanviar imatges o música.

9. *PHUBBING*
Situació en què algú no presta atenció perquè està pendent més del seu mòbil enlloc d'escoltar les persones que l'acompanyen (al cas de converses o de piulades -*twitt*-, juguen a jocs, trien música,...).

10. PROGRAMARI MALICIÓS O *MALWARE*
És un programari que té com a objectiu infiltrar-se en el sistema i danyar l'ordinador sense el consentiment de l'usuari. (Vegeu virus i troians).

11. *RANSOMWARE*
És un *malware* que uns criminals instal·len en el teu ordinador sense consentiment des d'una ubicació remota i bloqueja el teu equip. Presenten una finestra emergent (fent-se passar per un organisme oficial) amb l'avís de què no podràs desbloquejar-lo fins que paguis un rescat amb una transferència de diners a un compte. No heu de pagar mai.

12. ROBATORI D'IDENTITAT O *PHISHING*
És una forma d'enganyar els usuaris perquè revelin informació personal o financera mitjançant un missatge de correu electrònic o un lloc web fraudulent. El missatge adreça els destinataris a un lloc web fraudulent, on se'ls demana que proporcionin les seves dades personals, com per exemple un número de compte o una contrasenya. Després, amb aquesta informació poden suplantar-te la identitat.

13. *SEXTING*
És l'enviament de contingut sexual, principalment fotografies i/o vídeos produïts pel mateix remitent, a d'altres persones per mitjà del telèfon mòbil. En aquest cas s'ha d'anar amb precaució per la gran difusió que arriba a tenir Internet. Un cop a la xarxa l'usuari perd el control de la difusió de l'arxiu que penja.

14. TROIANS
Són programes informàtics que aparenten ser programari útil però que posen en perill la seguretat de l'ordinador. Habitualment s'utilitzen per espiar en instal·lar-hi programari d'accés remot que permet monitorar el que fa l'usuari a l'ordinador.

15. XARXES P2P
Són sistemes d'intercanvi d'arxius. És una forma legal de compartir arxius de forma similar a com es fa en el correu o en missatgers instantanis, si bé més eficient i, generalment, més ràpida.

16. XARXES SOCIALS
Conjunt de persones vinculades a un mateix grup d'Internet que tenen com element de cohesió el fet de compartir diferents tipologies de continguts: textos, fotografies, vídeos, música, enllaços,...

17. VIRUS
És un codi informàtic que s'adjunta a un programa o arxiu per propagar-se d'un equip a un altre. Infecta, amb gran facilitat, a mesura que es transmet. Els virus poden danyar i esborrar el programari (*software*), perjudicar el maquinari (*hardware*) i els diferents arxius que inclou l'ordinador infectat.

18. VIDEOCONFERÈNCIA
A partir de portàtils amb *webcam* o d'un *smartphone*, és la combinació de l'àudio, el vídeo i les xarxes de comunicació perquè individualment o en grup els usuaris es trobin cara a cara en temps real per interaccionar. Actualment Skype, Hangouts o algunes aplicacions per mòbil ho permeten de forma fàcil.

centre internet +segura

Segueix les nostres aventures a:

A Internet posa-hi seny

@internetambseny

Consulta i descarrega't els nostres recursos sobre seguretat a Internet al web

www.internetsegura.cat

INFÀNCIA RESPON
900 300 777

Posa't en contacte amb les nostres línies d'atenció si necessites assessorament o ja t'has trobat amb algun incident.

Co-founded by:

Generalitat de Catalunya