INTERNET SEGUR@

Avui en dia els nens i adolescents utilitzen cada dia molta estona les noves tecnologies, tant a casa com a l'escola. Per això és important que siguin conscients dels seus drets i deures a la xarxa i de les mesures de seguretat que cal prendre a l'hora d'utilitzar les noves tecnologies.

Amb els dispositius mòbils o els ordinadors els nens i nenes i els joves tenen la facilitat i rapidesa d'obtenir gran quantitat d'informació, de comunicar-se per mitjà de les xarxes socials o aplicacions, i intercanviar informació amb les amistats o familiars. Alhora, són especialment vulnerables a determinades activitats delictives relacionades amb el contingut de la informació. Poden ser víctimes si accedeixen a continguts il·legals, inadequats o nocius com: pornografia infantil, anorèxia i bulímia, jocs en línia.

Per poder ajudar als vostres fills o filles, és bo que els pares i educadors:

- Us familiaritzeu amb l'ús d'Internet, les aplicacions i les xarxes socials que puguin utilitzar els menors.
- Feu conscients els menors dels beneficis i dels riscos d'internet.
- Eduqueu-los perquè sàpiguen navegar i utilitzar les xarxes socials de manera responsable.
- Doneu-los estratègies perquè puguin protegir-se sols dels possibles perills de la xarxa.
- Parleu obertament amb els menors com actuar davant dels continguts inapropiats que es poden trobar a Internet o de les situacions que els incomodin, els violentin o si pateixen algun frau.
- Navegueu per la xarxa amb els vostres fills i filles i/o alumnes i informeu-vos de les eines de control.
- Feu-los conscients de les implicacions i dels riscos que pot suposar compartir informació personal, documents, imatges, vídeos o àudios a les xarxes socials o amb persones que no coneixen personalment.
- Responsabilitzeu-los de no apuntar-se a cap xarxa social sense el vostre consentiment i supervisió.
- Estabiu regles de seguretat, de temps i d'ús a la llar i al centre educatiu.
- Utilitzeu les eines de control parental.
- Eviteu deixar a la vista comptes d'accés a pàgines d'adults.
- Pregunteu en el centre educatiu quines polítiques de seguretat segueixen.
- Jugueu o utilitzeu amb els vostres fills o filles als jocs tecnològics; a més d'acompanyar-los, podreu valorar si s'adeqüen a la seva edat.
- Expliqueu la importància que no facin ostentació de l'ordinador i que cal que tingui cura dels llocs on l'exhibeix.
- És aconsellable que en cas de fer-ne ús a la via pública es prenguin precaucions i no es perdi de vista l'aparell. En la mesura del possible només fer ús a l'escola i si es pot és millor deixar-lo en els llocs que tingui habilitats el centre.

Utilitzar i configurar l'ordinador amb seguretat

Quan adquiriu un nou dispositiu:

Seguiu aquests consells per als diferents dispositius: ordinador de sobretaula, ordinador portàtil, tauleta...

- Protegiu el dispositiu amb un PIN, una contrasenya o un patró gràfic de desbloqueig ((No només protegireu l'accés a la informació del dispositiu, també podràs realitzar algunes accions abans que una altra persona accedeixi al dispositiu).
- Bloquegeu l'accés amb una contrasenya, pin o patró gràfic per accedir al dispositiu.
- Assegura't que les contrasenyes que introdueixis no siguin fàcils d'endevinar.
- Protegiu el vostre ordinador de virus i altres programes maliciosos que poden revelar les vostres claus.
- És recomanable disposar d'una aplicació "antirobatori" que permeti esborrar les dades i localitzar el dispositiu un cop sostret.
- Guardeu la factura de compra i anoteu el número de sèrie de l'ordinador (el número de sèrie és necessari per identificar-lo si es recupera després d'un robatori).

En el dia a dia... / **A fora de casa...**

- Tingueu especial cura de l'ordinador i els dispositius en llocs públics com bars, cafeteries, parcs, etc.
- És millor deixar els l'ordinador a l'institut o a l'escola, on disposen d'espais de seguretat adients per guardar-lo.
- Eviteu presumir d'ordinador. Quan sigueu fora de casa o de l'escola, porteu-lo sempre en un lloc segur (motxilla o funda) i no el perdeu mai de vista.
- És aconsellable que en cas de fer-ne ús a la via pública es prenguin precaucions i no perdeu de vista l'aparell. Tingueu cura i vigileu on deixeu el vostre portàtil o tauleta.
- No expliqueu que porteu un ordinador.
- Tingueu especial cura dels dispositius en llocs públics com bars, cafeteries, parcs.

Per assegurar el dispositiu i el contingut...

- Sigueu curosos i eviteu que algú tingui accés visual al dispositiu quan introduïu la contrasenya o el patró gràfic de desbloqueig.
- Comproveu que l'antivirus, el sistema operatiu i els navegadors estan sempre actualitzats.
- Activeu les notificacions automàtiques d'aparició de noves versions i així podem actualitzar-les immediatament.
- Si cerquem als buscadors les darreres actualitzacions poden donar resultats no legítims; és preferible usar enllaços d'actualització de les pàgines oficials dels fabricants dels programaris o des de les opcions que us ofereix el programari.
- Enteneu quins permisos esteu autoritzant quan instal·leu aplicacions i quan navegueu.
- Reviseu que els connectors (plugins) per als navegadors (complements per obrir o llegir informació que el navegador, amb la configuració bàsica, no pot; és el cas de Flash, Java, Quicktime o altres funcionalitats afegides als navegadors) no comprometen la seguretat del dispositiu i que estan actualitzats.
- Feu còpia de seguretat de la informació continguda al dispositiu.
- Eviteu connectar-vos a xarxes wi-fi desconegudes o obertes (sense contrasenya d'accés); quan us connecteu a Internet amb aquestes xarxes algú pot accedir i tenir control a les pàgines que navegueu i les operacions que hi realitzeu, tenir control de les sessions a les xarxes socials a què accediu o al vostre correu electrònic.
- Eviteu aparellaments amb *bluetooth* amb dispositius desconeguts.
- Reviseu l'ús que fan els vostres fills o filles fan dels dispositius i pacteu unes condicions o l'horari d'utilització.

Controls parentals

- Activeu mesures de control parental per evitar que els infants accedeixin a continguts perillosos o també per fer el seguiment de l'ús que fan d'Internet.
- El control parental és un sistema de seguretat de protecció infantil que permet gestionar, bloquejar o restringir l'accés a determinada informació ofensiva per als nens.
- Informeu-vos del seu funcionament i de com aplicar-ho al vostre ordinador.
- Navegueu per pàgines web que siguin segures i davant del dubte defugiu de pàgines que no us generin confiança.
- Acordeu quines pàgines es poden visitar.
- Feu el seguiment de l'ús que fan d'internet.
- Controleu els accessos a continguts d'adults i no deixeu comptes oberts que puguin tenir contingut inadequat pel vostre fill/a o alumne/a.
- És aconsellable utilitzar l'ordinador en llocs comuns i evitar espais privats com pot ser l'habitació.

Càmera web

- Apagueu i tapeu la càmera quan no l'utilitzeu.
- Assegureu-vos que els vostres fills són conscients del que fan quan la tenen engegada.
- Recomanacions:
    - Desconfieu dels desconeguts
    - No obriu trucades ni missatges de persones desconegudes.
    - Sigueu prudents i conscients del que es fa davant de la càmera, un cop fer se'n perd el control.

Navegar i descarregar arxius

Quan navegueu per Internet...

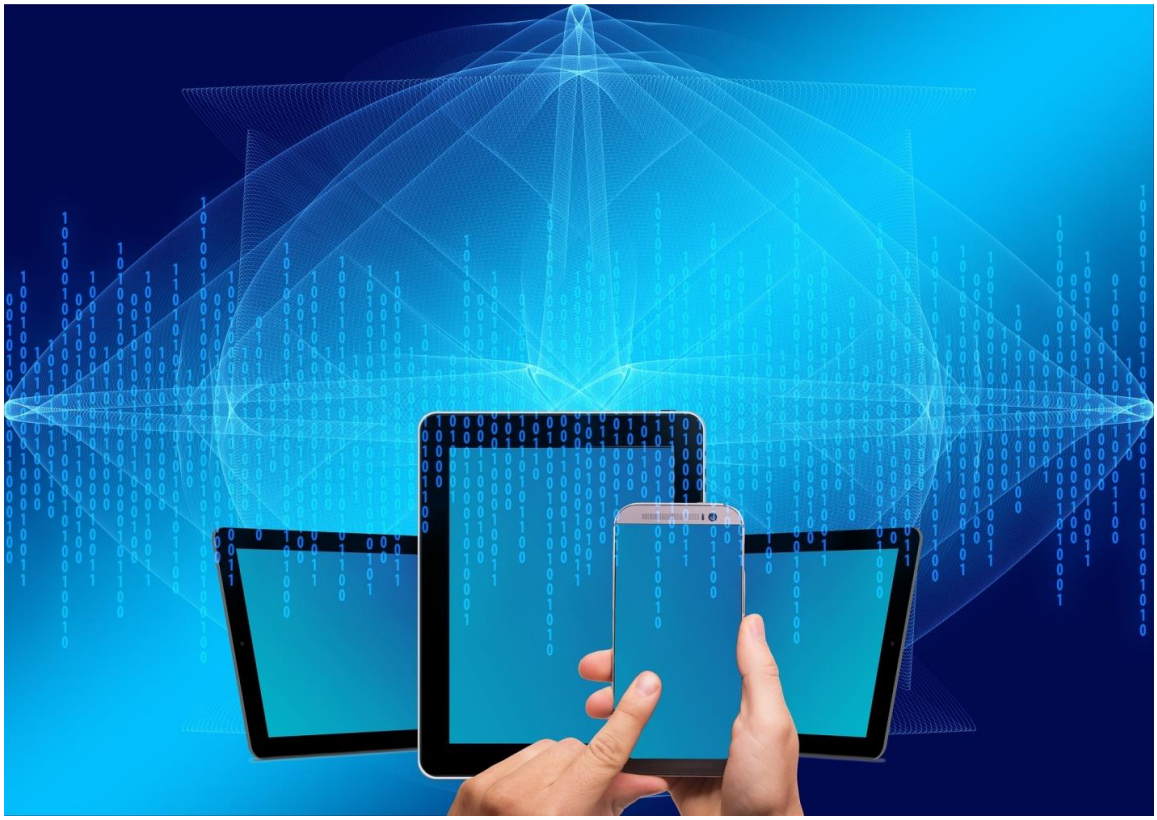
- Navegueu per webs segures i de confiança.
- Navegueu per la xarxa amb els vostres fills i filles i/o alumnes i informeu-vos de les eines de control.
- Eviteu desactivar l'antivirus i el tallafocs, us arrisqueu que infectin el dispositiu, copiïn informació o robin les dades personals.
- Feu atenció si apareixen finestres emergents quan visiteu una pàgina web o instal·leu programari per evitar que instal·lin programes o continguts no desitjables en el dispositiu.
- No faciliteu les vostres dades personals ni les d'altres persones quan visiteu webs de poca confiança.
- Amb els missatges de correu electrònic obriu només aquells que us enviïn persones de confiança.

Amb la descàrrega d'arxius...

- Feu atenció als arxius adjunts, ja que poden contenir virus.
- Eviteu obrir arxius adjunts de remitents desconeguts.
- Si descarregueu o intercanvieu fitxers, feu-ho només en aquells llocs o amb persones de confiança.
- Tingueu present que les descàrregues P2P i de procedència desconeguda o no confiable poden ser una via d'accés a virus, troians, cucs, etc.
- Respecteu els drets d'autor dels continguts.

Quan descarregueu aplicacions...

- És important que llegiu sempre bé abans d'acceptar unes condicions o la instal·lació d'un contingut determinat.
- Verifiqueu si l'aplicació ofereix els ajustaments de seguretat:
    - la navegació segura (https)
    - avisos per SMS o correu electrònic quan iniciem les sessions
    - recollida els dispositius reconeguts per entrar al compte (ordinador de casa, portàtil, mòbil, altres dispositius...)
    - recollida de les sessions actives (ubicacions –casa, wi-fi oberts, escola...- i tipus de dispositiu)



Virus

- Iniciar o reiniciar els ordinadors perquè siguin efectives les actualitzacions preventives que han estat fent el cap de setmana els corresponents serveis tècnics.
- No obrir un correu (ni els fitxers adjunts, ni els enllaços que contingui) del qual no en reconeixem l'origen.
- Apagar l'ordinador (o desconnectar de la xarxa) si detectem que es comporta anòmalament i, tot seguit, contactar amb el servei d'atenció a l'usuari de la nostra organització.
- No connectar a la xarxa l'ordinador de feina que haguem tingut a casa durant el cap de setmana i també contactar amb el servei d'atenció a l'usuari per demanar suport per revisar-lo i connectar-lo.

Com prevenir els virus en general

Un virus pot provocar la destrucció de les dades del dispositiu o la manipulació d'aquestes.

És convenient instal·lar antivirus i tallafocs als vostres dispositius; tingueu-los actualitzats.

Una de les formes més habituals d'infecció són les fotografies, jocs, descàrregues de programari o obrint correus electrònics de persones desconegudes. Aquesta última és la més perillosa.

Analitzeu els arxius amb un antivirus abans d'obrir-los (tant si els heu baixat d'internet com si us el faciliten per correu electrònic o en un llapis de memòria).

Fotografies i vídeos

- Sigueu prudents i conscients de les fotografies o vídeos que pengeu i les que pengen els vostres fills o filles.
- És convenient que assessoreu els vostres fills sobre els riscos que es poden trobar i com actuar si algú publica fotografies o vídeos sense el seu consentiment.
- Cal demanar autorització als pares dels menors de 14 anys per publicar fotografies seves.
- Configureu el vostre perfil (xarxes socials, webs, aplicacions, etc.) de manera que només les persones que vosaltres vulgueu tinguin accés a les imatges que publiqueu.
- Un cop pengem una fotografia o vídeo a la xarxa, en perdem el control; qualsevol persona pot descarregar-los, copiar-los o fer-ne una captura de pantalla, modificar-la i reutilitzar-la sense el nostre consentiment.
- Si voleu publicar fotografies on surti més gent, demaneu-los permís.
- Eviteu etiquetar altres persones si no heu obtingut el seu consentiment.
- Recordeu que les fotografies no han de vulnerar la intimitat de les persones ni la seva dignitat.

Xarxes socials

Els joves d'avui es troben i es relacionen a les xarxes socials de forma natural; s'envien missatges, xategen, tenen perfils a les xarxes socials, blocs, pengen fotos i les comenten, comparteixen arxius... I aprenen ràpidament a utilitzar qualsevol nova xarxa social o prestació dels dispositius que tenen o que hi ha a casa.

Les xarxes socials no són ni bones ni dolentes; tot depèn de com s'utilitzin. Els pares i mares i els docents, per als quals de vegades és un entorn força nou, heu d'educar-los també per fer un ús responsable i segur de les xarxes socials.

Per poder ajudar als vostres fills o filles, és bo que els pares i educadors:

Us familiaritzeu amb el funcionament de les xarxes socials i en concret amb les que utilitzen els vostres fills i filles.

Parleu amb els vostres fills per saber quin ús fan d'Internet i de les xarxes i quines pàgines visiten, conèixer amb qui xategen i quina informació publiquen...

Feu-los conscients de les implicacions i dels riscos de tenir perfils a les diferents xarxes socials. I, en definitiva, que no facin a les xarxes socials el que no farien en la seva vida real.

En el moment de crear comptes o perfils nous

- No permeteu que obrin un compte si no tenen l'edat mínima requerida per la xarxa.
- Creeu una adreça de correu electrònic específica per utilitzar-la només amb les xarxes socials.
- En el moment d'inscriure's en una xarxa estigueu amb ells per evitar que donin dades compromeses i assegurar-vos que es garanteix el nivell de privacitat desitjat.
- Demaneu que us acceptin a vosaltres o a un germà gran en la seva llista de contactes, amics o seguidors dels seus comptes a les xarxes socials.
- Acostumeu-los a llegir les condicions d'ús o els permisos de les aplicació abans de descarregar-les per conèixer les dades personals a les que poden tenir accés les diferents aplicacions.
- En el cas de xarxes relacionades amb vídeos o fotografies (com ara Youtube) assegureu-vos que indiquen correctament la seva data de naixement, ja que hi ha continguts que no són accessibles per als menors d'edat.

En el dia a dia...

Assegureu-vos que saben mantenir el nivell de privacitat adequat:

- Contrasenyes segures.
- Repassar sovint la configuració de privacitat de les diferents xarxes.
- Evitar donar informació personal (adreça, telèfon...) o mostrar fotos privades compromeses.
- Evitar publicar fotos o vídeos d'altres persones sense el seu consentiment.

Ajudeu-los a seguir unes pràctiques adequades:

- Utilitzar xarxes sense fils segures.
- Ajudeu-los a valorar quines informacions posen a la seva pàgina.
- Cal reflexionar abans de donar qualsevol dada personal, imatges o dades d'altres persones.
- Evitar crear una identitat falsa amb dades inventades.
- Evitar els contactes amb desconeguts.
- No trobar-se en persona amb gent que han conegut a la xarxa.
- Desconfiar de missatges rebuts de persones desconegudes; no s'han de contestar mai.

Amb les persones desconegudes:

- Evitar agregar persones que no coneixen.
- Cal ser conscient que donar accés a persones desconegudes pot ocasionar que donem accés també al contingut del nostre ordinador.
- Cal relacionar-se amb altres persones amb respecte.

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

Si algú fa un ús abusiu de les xarxes notifiqueu-ho als administradors.

Recordeu-los que si tenen dubtes ho poden consultar amb els pares o mares o amb els educadors.

En cas de robatori o pèrdua... denuncieu-ho a la policia

- Expliqueu als fills que si els prenen l'ordinador els primers que han de tenir coneixement són els pares i després l'escola. Cal informar sempre dels fets succeïts.
- Si us el prenen per la força, no us enfronteu. Comuniqueu-ho als pares i a l'escola i denuncieu-ho a la comissari més propera.
- Si heu vist qui us l'ha pres cal que doneu el màxim de dades, les característiques físiques d'aquesta persona, i el lloc i les circumstàncies en què s'ha produït el robatori.
- Cal tenir en compte que:

    - Els menors d'edat han d'anar acompanyats dels pares o tutors quan presentin la denúncia.
    - Cal que porteu el DNI o un document d'identificació.
    - Si disposeu de la documentació del portàtil cal que la porteu (factura, nº de sèrie, etc...)
    - En cas de que el vostre fill/a hagi vist l'autor dels fets cal que doneu el màxim de dades quan feu la denúncia.
    - Presentar denúncia falsa / simulació de delicte està penat per les lleis.
    - Les dependències policials ofereixen servei les 24 hores del dia, els 365 dies de l'any.
    - Per a urgències truqueu al telèfon gratuït 112.