

ÚS SEGUR D'INTERNET

MESURES A ADOPTAR PELS PARES, RESPECTE DELS SEUS FILLS

- Cal establir unes regles d'ús i les seues conseqüències.
- Adaptar els seus horaris escolars i d'estudi a la utilització d'ordinadors.
- Controlar els temps d'ús.
- Ensenyar-los a no sol·licitar productes sense aprovació familiar.
- Ajudar-los, en la mesura que siga possible, a realitzar els seus treballs, estudis, busques, etc.
- Motivar-los perquè realitze les seues pròpies recerques sobre temes d'interès, tant per als seus treballs escolars com per a la pròpia família.
- Comentar-los els efectes perjudicials i beneficiosos que causa la intimitat en fer ús de la xarxa.
- Parlar-los dels perills del xat, i explicar-los que, en xatejar, cal parar especial atenció als suposats amics, que després resulten no ser-ho. I fer atenció als continguts sexuals.
- Controlar les factures telefòniques.
- Establir pressuposts per a despeses en línia i supervisar que es compleixen.
- Fer comprovacions periòdiques sobre l'ús que els fills fan de l'ordinador i, sobretot, de la xarxa.
- Educar els fills sobre les conseqüències d'infringir les lleis.
- Dedicar especial atenció als jocs que els fills solen rebre, intercanviar o copiar. No tots són divertits, n'hi ha de perillosos i violents.
- No us heu de deixar convèncer sobre els suposats avantatges econòmics que suposen les compres de còpies il·legals de jocs, programari, pel·lícules, etc.
- Intercanviar coneixements amb els fills sobre novetats informàtiques.
- Animar als adolescents que mostren un determinat interès per la informàtica a compartir aqueixos coneixements amb altres germans, familiars, amics, etc.
- Revisar els continguts que puguen ser perjudicials per a la seua educació i desenvolupament (temes pornogràfics, violents, racistes, etc.)
- Usar proveïdors solvents.
- Valorar la possibilitat d'instal·lar filtres i programes de control per a accés a determinades activitats.
- Consulte les pàgines especialitzades en mesures de seguretat.

MESURES A ADOPTAR PELS FILLS

- Aviseu els adults immediatament si aprecieu continguts que pugueu considerar perillosos o, simplement, si els veieu rars.
- No doneu les vostres dades personals, si no esteu segurs del destinatari o si considereu que no són necessàries.
- No envieu les vostres fotos o les de la vostra família, ni qualsevol informació sobre aquesta, sense autorització dels vostres pares.
- No entreu en pàgines de continguts no aptes per a la vostra edat.
- Si teniu trobades físiques amb algú que heu conegut en la xarxa, consulteu-ho

abans amb els vostres pares o tutors.

- No contesteu a missatges estranys; inclús, als que us adjunten fitxers que desconeu el seu origen, i eviteu obrir-los.
- No accediu a zones que sol·liciten diners, números de targetes de crèdit, inversions, etc.

PRECAUCIONS EN TRANSACCIONS ECONÒMIQUES

- No abandoneu les còpies dels resguards de compra en les proximitats dels Terminals de Punt de Venda (T.P.V.), perquè contenen informació sobre les targetes que pot ser utilitzada tant en Internet com fora de xarxa.
- No utilitzeu la targeta si l'establiment no mereix la seua confiança. Es coneixen casos en què el personal d'alguns establiments ha utilitzat el número de la targeta i el nom del seu titular.
- No introduïu el número de la targeta en pàgines de contingut sexual o pornogràfic, en les que se sol·licita com a pretext, per a comprovar la majoria d'edat.
- No facilitar més dades personals dels necessaris.
- En enviar informació, comproveu que, en la part inferior del navegador Explorer, apareix un cademat groc o un cademat tancat, en el cas de Netscape. Açò indica que les seues dades viatgen encriptats.
- Comproveu que els càrrecs rebuts es corresponen amb els realitzats.

PRECAUCIONS SOBRE EL CORREU ELECTRÒNIC.

- No obriu missatges de correu, d'origen desconegut. Elimineu-lo, directament.
- No executeu cap arxiu adjunt que vinga amb missatges suggeridors.
- Adopteu les mesures necessàries, quan li ofereixen "regals" substanciosos i, per a rebre'ls, heu de cridar per telèfon a prefixos 906.
- No faciliteu la direcció electrònica amb "massa" lleugeresa.
- Tingueu activat constantment un antivirus.
- Visiteu pàgines especialitzades sobre seguretat informàtica.
- Perquè les vostres dades viatgen segures, envieu els vostres missatges xifrats.

MESURES DE SEGURETAT PER A USUARIS PARTICULARS.

- No faciliteu dades personals si no hi ha una completa seguretat sobre qui els rebrà.
- No faciliteu més dades personals que els necessaris.
- Exigiu, sempre, "connexions segures". Assegureu-vos que, en transmetre dades sensibles, en la part inferior del navegador Explorer, apareix un cademat groc i, en el cas de Netscape, un cademat tancat.
- Comproveu els certificats de seguretat, en pàgines que requereixen dades personals.
- Utilitzeu un bon producte antivirus i actualitzeu-lo sovint.
- Extremeu la precaució en els arxius que rebeu en sessions de xat.
- Actualitzeu els sistemes operatius i navegadors, amb les actualitzacions que

publiquen les firmes especialitzades de programari.

MESURES A ADOPTAR PER PETITES EMPRESES.

- Canvieu les contrasenyes periòdicament.
- Exigiu contrasenyes de qualitat.
- No deixeu les contrasenyes guardades en el disc dur.
- Confieu la gestió de la xarxa a un responsable.
- Dissenyeu un protocol de l'ús de la xarxa.
- Controleu les operacions i transaccions, fora de l'horari habitual.
- Establiu una política adequada de còpies de seguretat.

MESURES A ADOPTAR PER GRANS EMPRESES.

- Confieu la Seguretat informàtica a un responsable qualificat.
- Tingueu un control sobre persones externes a l'empresa que, en determinades ocasions, tenen accés a equips informàtics per qüestions de reparacions, desenvolupament, manteniment, etc.
- Feu una actualització constant del programari.
- Consulteu amb empreses especialitzades del sector.

MESURES PER A EVITAR FRAUS TELEFÒNICS

- Controleu les factures, per a vigilar si la despesa facturada es correspon amb les comunicacions realitzades.
- Comproveu els números de telèfons a què s'ha cridat, per a identificar-los com coneguts. Es donen casos de facturacions de cridades no realitzades per l'interessat. En aquest cas, abans d'adoptar altres mesures, consulteu els usuaris.
- Davant la possibilitat de substracció de documentació, tingueu precaució amb la correspondència procedent de bancs i operadores telefòniques per a, en cas de no rebre informació puntual sobre consums comunicar-ho a la companyia, sol·licitant un duplicat i advertint del que succeeix.
- No facilitar els números de telèfon, tant fix com mòbil, a persones desconegudes que els sol·liciten, sota qualsevol pretext, ja que s'han detectat casos en què s'intenta conèixer les característiques de les línia per a possibles desviacions.
- Davant d'una telefonada equivocada, tallar la comunicació, ràpidament, per a evitar la possible desviació de cridades amb càrrec a la factura de la persona que rep la cridada.
- En el cas de tenir contractada la modalitat de "cridada a tres", extremar les precaucions, ja que, amb un programa informàtic, es pot rastrejar la línia i produir-se una intrusió a ella, per a realitzar crides internacionals, amb càrrec en titular del telèfon.
- No acceptar cridades de cobrament a destinació si no s'està absolutament segur de conèixer qui ho demana. Pot tractar-se d'una cridada fraudulenta i pagar despeses de centenars d'euros per l'engany.