Adingabeak heztea Internet arriskurik gabe erabil dezaten

Gurasoentzako gida

Vitoria-Gasteiz

Vitoria-Gasteiz
Hiri Hezitzailea
Ciudad Educadora

Ayuntamiento
de Vitoria-Gasteiz
Vitoria-Gasteizko
Udala

Adingabeak heztea Internet arriskurik gabe erabil dezaten

Gurasoentzako gida

Ayuntamiento
de Vitoria-Gasteiz
Vitoria-Gasteizko
Udala

Argitaratzailea: Vitoria-Gasteizko Udala
Egilea: Udaleko Hezkuntza Saila
Bilduma: Hezkuntza
Testuak: Mintza S.L.
Itzulpena: Saretik
Diseinua eta maketazioa: La Debacle S.L.
Inprimatzailea:
L.G.: VI-
www.vitoria-gasteiz.org

Aurkibidea

Sarrera

Gizarte industrialaren ondoren, gaur egun informazioaren gizartean bizi gara; haren ezaugarri nagusiak informazioaren eta komunikazioaren teknologiek izan duten ezohiko hedapena da eta, bereziki, Internetek izan duena. Gizarte-eredu horren baitan, Informazioaren eta Komunikazioaren Teknologiekin (IKT) lotuta dagoen orok funtsezko rola betetzen du. Teknologia horiek izan duten ezohiko hedapena ezinbesteko tresna bihurtu da herriek banaka zein modu kolektiboan garapena lortu ahal izateko.

Herri-administrazioek, ezinbestean, kultura mailako aldaketa hori babestu dute. **Avanza Plana**k, esate baterako, beste hainbat neurriren artean, informazioaren eta komunikazioaren teknologiak hedatzeko eta erabiltzeko dauden oztopoak desagerraraztea, eta informazioaren gizarte berrian herritarren eskubideak bermatzea helburu dute araudiak hartzea aurrez ikusi du.

↘ Informazioaren gizarteko zuzendaritza nagusia
www.mityc.es/dgdsi/es-ES/Paginas/index.aspx

Euskadin, **2010eko Euskadi Informazio Gizartean Plana: Euskadiko Agenda Digitala** izeneko plangintza dago abian eta haren helburua Informazioaren eta Ezagutzaren Gizartea sendotzea da Euskadi berrikuntza arloan Europako erreferente bihurtzeraino aurrera egiteko.

↘ Euskadi informazio gizartean
www.euskadi.net/eeuskadi/new/eu/index.html

Informazioaren Gizartearen Goi-bilerako printzipioen adierazpenaren arabera (2004/05/12), "hezkuntza, ezagutza, informazioa eta komunikazioa ezinbestekoak dira gizakien aurrerapenerako, ekimenerako eta ongizaterako. Historia osoan lehen aldiz, IKTek ohiko oztopoak gutxitzeko (bereziki denbora eta distantzia mailakoak) eskaintzen dituzten gaitasunek teknologia horiek mundu osoko milioika pertsonaren mesedetan erabiltzea ahalbidetzen dute".

↘ www.itu.int/wsis/index-es.html

Bestalde, **Vitoria-Gasteizko Udalak**, gure hiria Hiri Hezitzaile gisa sendotzeko zeregina bere gain hartuta, seme-alabek informazioaren eta komunikazioaren teknologiak behar bezala erabiltzearen inguruan gurasoek duten ardura partekatzen du, horiek behar bezala ez erabiltzetik erator daitezkeen arriskuak ekidinda.

Gida hau argitaratu izanaren asmo nagusiak, helburu hauek betetzea izango da:

- Adingabeen gurasoak hezten laguntzea informazioaren eta komunikazioaren teknologiek eskaintzen dituzten aukeren inguruan, eta adingabeekin duten harremanean erabilgarriak izan daitezkeen edukiak eskaintzea eta erronkak proposatzea.
- Informazioaren eta komunikazioaren teknologien arriskuen inguruan ohartaraztea, fobia teknologikorik sorrarazi gabe. Konfiantza lortzea ezagutzak eskuratuta.
- Biztanleria teknologia horiek modu seguruan erabiltzearen, ezagutzearen, bideratzearen eta bultzatzearen inguruko erabilgarritasunaren inguruan kontzientziatzea. Jardunbide seguruak eta Interneteko ohitura osasuntsuak bultzatzea.
- Estrategiak ikastea informazioaren eta komunikazioaren teknologietara sartzeak biltzen dituen arrisku nagusiei aurre egin ahal izateko.

Informazioaren eta Komunikazioaren Teknologiak (IKT)

Kontzeptuak finkatzea

Informazioaren eta komunikazioaren teknologiek gure bizitzako ia alderdi guztietan eragin nabarmena dute. Teknologia horien bilakaera azkarrak garapen maila altuagoak lortzeko aurrekaririk gabeko aukerak eskaintzen ditu.

Euskadik IKTekin lotuta duen egoera, etengabe eguneratuta, sakontasunean ezagutu daiteke Euskal Administrazioetako web atariek eskaintzen duten informazioari esker.

➘ www.euskadi.net/eeuskadi/new/eu/esi_tic.html

Adingabeek IKTetara sartzeko erabiltzen dituzten sarbide-sareak (lantzen ari garen gaiari dagokionez garrantzi handiagoa dute) telefonia-sareak (finkoak eta mugikorrak) eta banda zabaleko sareak dira, ordenagailu pertsonaletatik Interneterako kalitate handiko konexioak ahalbidetzen dituztenak.

Bide horien bidez adingabeek gehien eskatzen dituzten zerbitzuak hauek dira: komunitate birtualak (sare sozialak, foroak, blogak eta abar), edukiak partekatzeko Peer To Peer (P2P) zerbitzuak eta Interneteko nabigazioa.

Internet erabiltzen duten adingabe gehienek aisialdirako tresnatzat hartzen dute (txateatzeko, jolasteko, musika bilatzeko), baina alde nabarmenak antzematen dira ikasketa mailen artean. Esate baterako, Lehen Hezkuntzako ikasleak dira Internet informazioa bilatzeko gehien erabiltzen dutenak; DBHko ikasleek batez ere txateatzeko erabiltzen dute Internet, eta Batxilergoko ikasleek funtsean harremanak egiteko eta jendea ezagutzeko tokia bilatzen dute sarean.

➘ Haurren segurtasuna eta adingabeen ohiturak Interneten
www.asociacion-acpi.org/seguridad%20y%20costumbres.htm

Adingabeek gaurko teknologiekin lotuta dituzten ohiturak

Adingabeek teknologia horietara sartzeko dituzten ohiturak sakon aztertu dituzte ekimen hauen bidez, besteak beste:

"Haurrek eta nerabeek IKTak segurtasunez erabiltzeko ohiturei buruzko azterketa eta gurasoen e-konfiantza" INTECOko (Komunikazioaren Teknologietako Institutu Nazionaleko) Informazioaren Segurtasuneko Behatokiak egindakoa.

www.inteco.es

"Haurren segurtasunari eta adingabeek Interneten dituzten ohiturei buruzko azterketa" ACPI (Haurren Pornografiaren Aurkako Ekintza) eta Madrilgo Komunitateko adingabeen defentsarako PROTÉGELES erakunde independenteek egindakoa.

www.protegeles.com/es_estudios5.asp

Internet erabili ohi duten adingabeei (laurdena inguru) buruzko emaitza esanguratsuenen artean hauek aipatu behar dira:

— Adingabeak etxetik sartzen dira Sarean batez ere eta, kasu gehienetan, iragazketako sistemarik ez duten ordenagailuetatik. Heren batek "Internetera maiz konektatzeko beharra sentitzen duela" aitortzen du.

— Haurrek mezu elektronikoak igorri eta jasotzeko, artxiboak deskargatzeko eta informazioa bilatzeko erabiltzen dute Internet. Erabilera horien atzetik, berehalako mezularitzak eta txatak ere erabilera-tasa altuak dituzte. Maiz konektatzen diren adingabeen laurdenak jolasteko egiten du.

— Adingabeak lehen aldiz Internetera sartzen direnean duten batez besteko adina 10 edo 11 urte ingurukoa da. Adingabeak oso maiz sartzen dira Interneten: erdia egunero konektatzen da Internetera eta herena baino gehiago astean 2 edo 3 egunetan sartzen da.

— Gurasoen ia % 80k dio beren seme-alabek Interneten pasatzen duten denbora normala dela, normaltzat hartuta "inguruko beste adingabe batzuk ematen dutenaren baliokidea".

— Adingabeen **erdiak ez du** Internet erabiltzeko oinarrizko segurtasun arauei buruzko **inolako informaziorik jaso**.

— Adingabeen **laurdena** webgune **pornografikoetan**, **indarkeria** ikus daitekeen webguneetan (hor ehunekoa altuagoa izango da seguru asko) edo **eduki arrazista edota xenofoboa** duten webguneetan sartzen da.

— Mahai gaineko ordenagailuaren ondoren (% 88), adingabeek gehien erabilitako ekipo teknologikoak DVD-irakurgailua (% 72), telefono mugikorra (% 64) eta MP3 edo MP4 (% 53) dira.

— Espainiako 10 eta 16 urte arteko adingabeen artean **telefono mugikorrak** txertatze maila altua da: bi heren inguruk telefonia mugikorreko terminal propioa du. Telefono mugikorraren jabetza areagotu egiten da adinaren arabera eta 15 eta 16 urteko neska-mutilen artean orokorra dela esan dezakegu, % 89k badu.

— Adingabeek erabiltzen duten telefono mugikorreko kontratu motari dagokionez, % 50 aurreordainketakoak dira, eta gainerako % 50 kontratuko telefonoak; aurreordainketa da adin txikieneko neska-mutilen artean gehien sistemarik ohikoena.

— Etxeen % 41en **bideo-jokoen kontsolak** egon ohi dira, eta % 19n bideo-jokoen kontsola eramangarriak. On lineko bideo-jokoen erabilera, bideo-jokoen kontsolen edo ordenagailuen bidezkoa, Espainiako adingabeen % 30ekoa da.

— Internet erabili ohi duten adingabeen **% 30ek telefono-zenbakia eman du** noizbait konektatu denean eta inkestari erantzundako adingabeen **% 16k helbidea eman** edota **hitzordua egin du** ezezagun batekin Internet bidez.

— Internetera maiztasunez konektatzen diren adingabeen ia **erdiak** dio Sarean autore-eskubideen bidez **babestutako materialak** bilatzen dituela eta joera horrek gora egiten du adinarekin.

— Gurasoen artean kezka gehien sortzen duena **mendekotasun-arriskua** edo **gehiegizko erabilera** da, gainerako egoerekin alderatuz gero, askoz ere kezka handiagoa, gainera: malware motako sistema informatikoaren mehatxuak, sexu-jazarpena, ezezagunekiko elkarrekintza, iruzurrak eta eduki desegokietarako sarbidea.

"Informazioaren eta komunikazioaren teknologiak ez dira inolako panazea, ezta formula magikoa ere, baina planetako biztanle guztien bizitza hobetu dezakete"

(Kofi Annan, NBEko idazkari nagusia, Geneva 2003).

Abantailak ulertzea

Sareko sarbideek egun eskaintzen dituzten aukerek banakoen ohiturak aldatu dituzte. Eskuragarri daukagun eta etengabe eguneratzen den informaziorako sarrerak gizartea aberastu eta pertsonen artean harremanak izateko aukerak eskaintzen ditu, duela zenbait bosturteko imajinatu ere ezin zirenak.

Garrantzitsua da ulertzea arazoa ez dela teknologia bera (etikoki neutroa), haren inguruan egiten den erabilera baizik. Babesgabeenak diren kolektiboen kasuan (batez ere, adingabeak), **tresna horien erabileran jardunbide egokien erantzukizuna gurasoena eta hezitzaileena da**; haiek beren ezagutzekin eta sen onarekin IKTen erabilera egokia bultzatu behar dute.

Erakunde publikoek adingabeen hezkuntzaz arduratzen diren guztiei jarduteko ildo fidagarriak eta seguruak emateko aukera eta betebeharra dute, haiek, era berean, gazteei hauen moduko alderdi garrantzitsuen inguruko prestakuntza eman diezaien: informazioaren kalitatea bereizten jakitea, ezezagunekin harremana izateak dituen arriskuak edo gure pribatutasuneko sarbidea kontrolatuta izateko beharra.

Informazioaren eta komunikazioaren teknologiek eskaintzen dituzten abantaila nagusien artean hauek aipa daitezke adibide modura:

— **Webguneen bidez** aukera hauek ematen dituzte: hezkuntzako eta kulturako baliabideak bilatzea (on lineko entziklopediak, erreferentziazko lanak, irudiak, podcast-ak, bideoak eta abar), informazioaren gaurkotasunera sarbidea, gehien interesatzen zaizkigun gaietan sakontzea ahalbidetzen duen dokumentazioa lortzea, bakarka edo beste batzuekin jolastea eta abar.

— **Posta, txat eta mezularitza elektronikoaren bidez** aukera hauek eskaintzen dituzte: pertsona kopuru mugagabearekin komunikatzea, haiekin ideiak eta iritziak partekatzea eta interesetako komunitateetan parte hartzea, informazioa partekatzea eta adituekin harremanetan jartzea.

— **Blog eta sare sozialen bidez**, sarean lankidetzan jarduten laguntzen, teknologia horiek hobeto erabiltzen erakusten, argitaratutako edukien gaineko erantzukizuna hartzen eta, azken batean, lan-merkatuan gero eta gehiago eskatzen diren gaitasunak eskuratzen laguntzen dute.

Adingabeentzako Sareko arrisku garrantzitsuenak honela sailka daitezke:

- **Neurriz kanpoko erabileraren eta mendekotasunaren** arriskuak.
- **Jabetza intelektualeko eskubideen urraketarekin** lotutako arriskuak.
- **Eduki desegokietara** sartzeko arriskua.
- **Beste pertsonek zelatatzeko eta haiekin elkarregiteko** arriskua.
- **Sexu-jazarpena** jasateko arriskua.
- **Pribatutasuna mehatxatzeko** arriskua.

Arriskuak ulertzea

Egungo teknologiek etengabeko garapena dute eta abantaila sozial eta pertsonal handien iturri dira: informaziorako sarrera, komunikazioaren hobekuntza, ezagutzak trukatzea, harremanak erraztea eta abar. Hala ere, gero eta gehiago dira beste jarduera batzuen kaltetan (eskolakoak edo jolaserako beste ekintza tradizional batzuk esaterako) nerabeek tresna horiek gehiegi erabiltzen dituztela ohartarazten dutenak.

Interneten erabilera konpultsiboak, alor pribatua agerian jartzeak edo telefono mugikor berriek eskaintzen dituzten zerbitzuetarako sarrera mugagabe eta bereizi gabeak kezka sortu dute guraso, hezitzaile eta psikologoen artean. Enrique Echeburúak, Euskal Herriko Unibertsitateko Psikologia Klinikoko katedradunak, gaiari buruzko argitalpen interesgarriak ditu, hala nola: *"Drogarik gabeko menpekotasunak? Menpekotasun berriak"*.

➘ www.ehu.es/echeburua/index.asp

Adingabeentzat, informazioaren eta komunikazioaren sareak erabiltzea oso baliagarria eta atsegingarria izan ohi da, baina ez dugu ahaztu behar gatazkak sor ditzaketen egoerak eragin ditzaketela, esaterako: eskatu gabeko eduki desatsegineko mezuak jasotzea, hainbat hizketakideren artean irainak botatzea edo pertsona ezagunen edo ezezagunen mehatxuak (modu agerikoan edo ez hain agerikoan) sufritzeko aukera.

Orain arte ohikoak izan ez diren informazio mailetara sartzeko gaitasun horrek eragin sozial handiko arazoak sor ditzake, modu masiboan edo bereizi gabe eginez gero. Hemeroteka guztiek horri buruzko frogak ematen dituzte:

"Ertzaintzak Internet bidez harremanetan jarri ondoren adingabeenganako hainbat jazarpen sexual gertatu direla ohartarazi du"

(Deia.com) 2009-03-24

"Adingabeei erasotzeko Internet erabiltzen zuten eta beren ordenagailu pertsonaletan haurpornografia deskargatzen zuten hiru anaia atxilotu ditu gaur Polizia Nazionalak"

(El Pais.com) 2009-12-19

"Euskadiko nerabeen % 62 asteko egun guztietan konektatzen da Internetera eta % 40k sarean ezezagunekin harremanetan jarri izana aitortzen du, Euskadiko Adingabeen Segurtasunari buruzko bigarren Azterketako datuen arabera"

(El Mundo.es) 2009-12-17

Oinarrizko segurtasun kontzeptuak

Zer da firewalla (suebakia)?

Ekipo informatikoa nahi ez ditugun kanpoko intrusioetatik babestea xede duen softwarea. Ordenagailuetako segurtasun-sistemako oinarrizko osagaia da. Ordenagailuaren eta sarearen arteko informazioaren trafikoa ahalbidetzen edo mugatzen du, arau multzoan eta bestelako irizpideetan oinarrituta.

Zer dira Sistema Eragilearen eguneraketak?

Ordenagailuko sistema eragilean sortutako arazoak konpontzeko edo etorkizunean arazoak saihesteko fabrikatzaileak iradokitako aldaketak. Sistema eragile guztiek eskaintzen dituzte (Windows, Linux, Mac OS eta abar). Etengabe eguneratutako sistema eragilea funtsezkoa da ordenagailuaren segurtasunerako eta fidagarritasunerako.

Zer esan nahi du malwareak?

➘ http://es.wikipedia.org/wiki/Malware#Clasificaci.C3.B3n

Jabeak jakin gabe ordenagailuko sistema eragilean sartzea xede duen softwarea da. Programak sistema eragileetako kode-erroreak (bugs edo zuloak) aprobetxatzen ditu sartzeko. Sistema eragileetako eguneraketak errore horiek prebenitzen edo eragozten ahalegintzen dira. Ahultasun (edo zaurgarritasun) hitza ere maiz erabiltzen da softwarearen diseinuko, konfigurazioko edo funtzionamenduko edozein errore aipatzeko. Erasotzaileak topatzen dituenean, sistemaren segurtasuna mehatxa dezaketen baimendu gabeko sarrerak gerta daitezke.

Hauek dira malware nagusiak: birus informatikoak (gehien ezagutzen direnak), harrak, troiarrak eta spyware-a.

Zer da biruskontrakoa?

Ordenagailuan intentzio txarreko eragiketak antzemateko, blokeatzeko, ezabatzeko eta, ahal izanez gero, saihesteko diseinatutako aplikazio informatikoa da. Segurtasun-sistemetan firewallaren nahitaezko osagaia da. Malware mota desberdinak dauden arren, egun erabiltzaileek aplikazio bakarrarekin asmo txarreko software mota guztiei aurre egiteko osatuta dauden informatikako programak izan ditzakete.

2010. urteko biruskontrakorik onenen prezioen eta ezaugarrien alderaketa eguneratua helbide honetan topatuko duzu: www.pcasalvo.com

Zer da hackinga?

Jabeak jakin gabe norbait zuzenean sistema informatikoan sartzea da. Horretarako, ahultasunak aprobetxatzen ditu.

Hacker-en asmoak askotarikoak izan daitezke: aplikazio informatikoaren diseinuko erroreak azaleratzea (haiek ezabatzeko adabakia sortzea ahalbidetzeko xedearekin) edo softwarearen errore horiek erabiltzea biktimentzako helburu kaltegarriekin edo erasotzaileen mesedetan.

Zer da spama?

Spam-a edo "nahi ez den posta elektronikoa" edo "zabor-posta" eskatu gabeko mezu multzoa da eta masiboki igorriz gero, hartzailea nolabait kaltetu dezakete. Gehien erabilitako sistema posta elektronikoa da, baina berritaldeak, blogak, foroak eta telefono mugikorrak testu-mezuen bidez ere "zabor-postaren" helburu izan dira.

2009ko apirilean, segurtasuneko irtenbideetan espezializatutako Sophos http://esp.sophos.com konpainiak, "Dirty Dozen" zerrenda ospetsuaren egileak ("Los doce del patíbulo" film ospetsua gogora ekarrita), adierazi zuen Espainia zortzigarren postuan dagoela spamaren eragina jasatzen duten herrialdeen artean (lehenengo postuan Estatu Batuak daude).

Zer dira ateratzen diren elementuak (pop-up)?

Nabigatzailean, ikusten ari garen orrialdearen gainean, zabaltzen diren leiho txikiak dira, informazioa gehitzeko, edo, maiz gertatzen den moduan, nabigazioan zehar publizitatea sartzeko edo eduki sexual esplizituko materiala erakusteko balio dute.

Segurtasun-arazorik sortzen ez duten arren, oso deserosoak edo desegokiak izan daitezke; hori dela eta, nabigatzaileek erraz konfiguratu daitezkeen "elkarrizketa-elementuen blokeatzaileak" jartzen dituzte.

Zer da cookiea?

Webgune jakinak bisitatzean, orrialdearen egileak hala eskatuta, gure disko gogorrean metatzen den testu arruntaren itxura duen informazio zatia da. Bisitarien kontrola eramateko eta erabiltzaileen nabigazio-ohiturei buruzko informazioa lortzeko erabiltzen da.

Ez dute segurtasun-arazorik sortzen, baina pribatutasunean sartzea ekartzen dutenez, nabigatzaileek baimena emateko edo ukatzeko aukera dute.

Zer da ziurtagiri digitala?

Besteak beste, jabea identifikatzen duten datuak dituen dokumentu digitala da. Nahasmenik sortu gabe, Interneten identifikatzea eta beste pertsona batzuekin informazioa trukatzea ahalbidetzen du, informaziorako sarbidea zuk eta zure hizketakideak soilik izango duzuela bermatuta.

Zer da wi-fi konexioa?

Ordenagailuak Internetera "kablerik gabe" konektatzea ahalbidetzen duen sistema da (haririk gabe). Abantaila ugari du, baina zenbait arrisku ere izan dezake. Gida honetako Segurtasun neurriak eta tresnak atalean horri buruzko aholkuak topatuko dituzu.

Zer da konexio segurua?

Encriptatzeko metodoen bidez egindako konexioa da (normalean "SSL protokoloaren" bidez –Secure Sockets Layer edo Konexio seguruko geruzaren protokoloa–). Ordenagailu pertsonalaren eta konektatutako zerbitzariaren artean trukatutako informaziora sartzea (konfidentzialtasuneko bermea) edo, atzemanez gero, manipulatzea (segurtasuneko bermea) eragozten du.

Adingabeekin lotutako segurtasun arazoak

Interneteko inguruneak, zalantzarik gabe, abantaila ukaezinak ditu, baina denborarekin delinkuentzia teknologikoa ekarri du, Sarean ezer desegokirik topatzea espero ez zuen erabiltzaile askoren fede onari esker neurri batean.

Malware-a, oro har, programa informatikoen ahultasuna eta zabor-posta (spam) ordenagailuetako erabiltzaile guztiak mehatxatzen dituen segurtasun-arazoa da, bereziki sarearen bidez beste erabiltzaile batzuekin elkarreragiten dutenean.

Dena den, badira IKT modernoen erabiltzaileentzako are kezkagarriagoak diren beste mehatxu batzuk. Adingabeekin lotuta arriskutsuenak diren mehatxuak landuko ditugu.

Haurren behatokia
www.observatoriodelainfancia.msps.es

Posta elektronikoaren eta berehalako mezularitzaren arriskuak

Berehalako mezularitzako programak (eta txata) eta posta elektronikoa (e-maila) Interneten garapen maila handia lortu duten komunikaziorako zerbitzuak dira. Haien arrakasta eta erabilera maila dela eta, software gaiztoak eta eskatu gabeko edukiak hedatzeko gehien erabilitako euskarriak dira; ondorioz, egileentzako abantaila hauek izaten dituzte: hedapena masiboa eta kostua txikia izaten da.

Teknologia horien erabilerarekin lotutako arriskuak hiru motatakoak dira batik bat:

— **Helbide elektronikoen bilketa**, helbideak "lortzeko programak" (harvesting) erabilita, esaterako. Horiek ondoren eskatu gabeko komunikazioen igorpen masiboa (spam) egitekoedo albiste faltsuak zabaltzeko erabiltzen dira , pertsonen multzoari gezurrezkoa edo beharrezkoa ez den zerbait benetakoa edo beharrezkoa dela sinestarazteko asmoz (hoax).

— **Identitatea ordezkatzea**, oro har, ez baita igorlearen eta hartzailearen nortasuna finkatzeko sistema fidagarririk edo informazioaren trukean konfidentzialtasuna bermatzen duen mekanismorik erabiltzen. Ziur al zaude mezuak beti zure ustezko hartzailearekin trukatzen dituzula?

— **Software gaiztoen instalazioa** mezu elektronikoei erantsitako dokumentuetan malware-ak sartuta egiten da maiz. Datuak babesteko bulegoan www.agpd.es "Interneteko erabiltzaileei zuzendutako gomendioak" bilatu.

Mehatxu pertsonalak: Grooming-a, Ziberjazarpena eta Sexting-a

Sareko mehatxuek (beste norbaiten aurkako irainak eta aipamen iraingarriak) garrantzi berezia hartzen dute, idatziz egiten direlako eta hartzailearengan babesgabetasun-sentsazio handia sortzen dutelako. Efektu hori are kaltegarriagoa da hartzailea adingabea denean.

Eskola jazarpenaren aurrean laguntzeko egitasmoa
www.acosoescolar.info/index.htm

Segurtasunari eta hezkuntzari buruzko mundu mailako Wiredsafety www.wiredsafety.org sareko ekimenaren zuzendari exekutiboak, Parry Aftabek, honela dio: "Ziberjazarpena haurren aurkako arriskurik ohikoena da".

Atal horretan sartzen dira hauek ere: iritzi-delituak, terrorismoaren apologia eta delituak egitera bultzatzea; jarrera horiek Internet bidez eginez gero, legeari dagokionez larriagoak izaten dira.

Segurtasun-arazo larrienen artean sexu-askatasunaren aurkako delituak nabarmendu behar dira: jazarpenetik hasi eta exhibizionismora edo probokazio esplizitura artekoak.

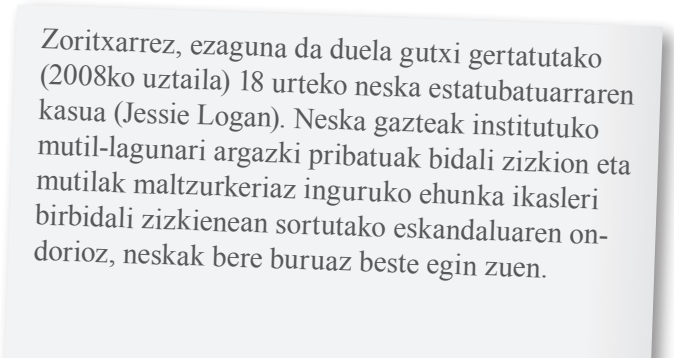
1. **Grooming-a** [*limurtzea*] www.internautas.org/html/5349.html
   Pederastek eta pedofiloek internauta adingabeen konfiantza eskuratzeko erabilitako prozedurak (lotura emozionalak finkatzea, datu pertsonalak lortzea, eduki erotikoa edo pornografikoa duten irudien igorpena edo eskaera eta ondorengo xantaia) izendatzeko erabiltzen den termino anglosaxoia da.

2. **Ciberbullying** [*ziberjazarpena*] www.ciberbullying.net
   Ziberjazarpena deitzen zaio komunikazio-sarean (Internet, telefono mugikorrak eta bestelako teknologia telematikoak) adingabeen artean egiten den jazarpena eta zirikatzeari. Gazte batzuek beste gazte batzuen aurka egindako **mehatxuak**, **mespretxuak**, **xantaiak**, **isekak** edo **irainak** izan ohi dira. Anonimotasuna, sortutako benetako kaltea ondo ez ulertzea eta Sarean askotan gezurrezko rolak eskuratzea direla eta, ziberjazarpena arazo larria da.

↘ Zer egin mehatxuen aurrean?
www.ciberfamilias.com/conflictos1.htm

↘ INTECO-ren webgunetik 'Ziberjazarpenari eta grooming-ari buruzko gida' deskarga daiteke.' www.inteco.es

3. **Sexting** [*hitz-jokoa da eta horren itzulpena hau izan daiteke: 'sexua igortzen'*]
   www.sexting.es
   Sexting-a eduki **sexualak bidaltzea da** (argazkiak eta bideoak, batez ere). Oro har, igorleak berak sortzen ditu edukiak eta **telefono mugikorren bidez** beste adingabe batzuei igortzen dizkie. Ekintza horren atzean arrazoi hauek daude, besteak beste: "adiskideen" presioa, ezagun bihurtzeko gogoa, arreta jasotzeko beharra, heldutasunik eza eta adin jakinetan ohikoak diren beste arrazoi batzuk.


Zoritxarrez, ezaguna da duela gutxi gertatutako (2008ko uztaila) 18 urteko neska estatubatuarraren kasua (Jessie Logan). Neska gazteak institutuko mutil-lagunari argazki pribatuak bidali zizkion eta mutilak maltzurkeriaz inguruko ehunka ikasleri birbidali zizkienean sortutako eskandaluaren ondorioz, neskak bere buruaz beste egin zuen.

Iruzurraren arriskua

Iruzurra IKTetan sartu da, nola ez. Funtsean, iruzurgileentzako "aukera" berria eskaintzen duten komunikaziorako tresnak dira.

Iruzurrekin lotutako mehatxu larrienek ez diete adingabeei eragiten, zorionez; izan ere, konfidentzialtasun berezia eskatzen duten zerbitzuak dira (banku elektronikoa, merkataritza elektronikoa, administrazioko izapideak eta abar).

Adingabeen eta sarearen arteko elkarrekintzan iruzurra sortzen duen elementu nagusia identitatea ordezkatzea izaten da (ikusi gidako Pribatutasuna eta segurtasuna atala). Adin-talde horretan, ohikoa da gehiegizko konfiantza eta, ondorioz, kolektibo hori ahulago bilakatzen da.

➘ www.osi.es/Segurtasunaren_ABCa/Iruzurra_gizarte_ingeniaritza/

Pribatutasuna eta segurtasuna

Informazio pribatua edo konfidentziala publikoki azaltzeak dakarren arriskua (helduek ulertzeko ere zaila izaten da zenbaitetan) areagotu egiten da adingabeen kasuan, datu pertsonalak emateko garaian inuzenteagoak izaten baitira (beren datuak zein senideei edo lagunei buruzkoak ematen dituzte).

Bizitza pribatuaren aurkako delituak, oro har, beste batzuen datu pertsonalak haien baimenik gabe eta kaltea eragiteko xedearekin erabiltzearekin lotutakoak izaten dira. Telefonoa edo helbidea ematea, argazkia erakustea edo elkarrizketa pribatuak ikusgai jartzea izan daiteke.

Ingeniaritza soziala (ingelesez Social Engineering) deitzen zaie manipulazio-estrategien bidez pertsonei buruzko informazio konfidentziala lortzera bideratutako ekintza edo jarrera guztiei. Pertsona bati buruz bere bitartez informazioa lortzea da helburua, baina hura "isilpekoa izan daitekeen informazioa" ematen ari dela ohartu gabe. Funtsean, segurtasun-sistemetako elementurik ahulena aprobetxatzen da: gizakia.

Pertsonak kaltetzea edo arriskuen edo jazarpenen aurrean jartzea ahalbidetuko lukeen informazioa lortzea edo informazio-sistemetarako sarrera edo pribilegioak lortzea da horren helburua.

Gure datuak zuzenean lortzeko modua da, ondoren, horien erabilera interesatua egiteko. Legedian "sekretuen aurkikuntza eta ezagutaraztea" moduan espresuki jasotako jarrera izango litzateke eta hainbat kartzela-urte ekarriko lituzke.

➘ www.privacidad-online.net

"Egun on, jauna: Hedapen handiko enpresaren marketin-zerbitzutik deitzen dizugu. Gure bezero onenei eskaintza berezia egiten ari gara. Zuk aukeratutako telefono finko nazionalerako deiak doan izango dituzu urte osoan.

Eskaintza hori eskuratzeko, hainbat datu egiaztatzea eskatzen dizugu, mesedez...

Sareko iruzurrak

Webgune faltsuak dira horren erakusgarri. Existitzen ez diren zerbitzuak eskaintzeko (ondoren entregarik gabeko ordainketa-zerbitzua, adibidez) edo webgune ofizialak ordezkatzeko (banku-erakundeen, saltokien edo administrazio publikoen webguneen itxura imitatzen dute) erabiltzen dira, erakunde horiekin trukatu ohi den informazioa lapurtzeko helburuarekin.

Kasu arruntena phishing izenekoa da. Posta elektronikoa erabiltzen da horretarako eta lehen begiratuan egiazko erakundeak igortzen duela dirudien arren, orrialde faltsura eramaten duen esteka izaten du; bertan gure datuak sartuz gero, iruzurgileak eskuratuko lituzke. Pharmingaren kasua konplexuagoa eta askoz ere arriskutsuagoa da. Erabiltzailea orrialde faltsura igortzen da, nahiz eta webgunearen helbidea akatsik gabe idatzi. Guardia Zibilaren webgunea sistema horren bidez eraso zuten 1999. urtean. Helbidea www.guardiacivil.org behar bezala idatzi arren, erabiltzailea eduki sexualeko orrialdera bideratzen zuten.

Iruzur mota hori saihesteko modu onena mezu iruzurtiak ezagutzen ikastea eta izapideak on line egiteko gomendioen berri izatea da.

➘ www.osi.es/Babes_zaitez/Lineako_izapideak/Iruzurrezko_mezuak_antzematea/

Eduki desegokietara sartzea

Ezerk ezin du ordezkatu seme-alabak Interneteko eduki desegokien aurrean babesteko gurasoek egiten duten zaintza- eta heziketa-lana.

Internet, egun ezagutzen dugun moduan, erabiltzaileei bi noranzkoetan zabaldutako sistema da. Alde batetik, erabiltzaileek nabigazioan topatutako edukien etekina ateratzen dute eta, bestetik, edukien eskaintza aberasten lagun dezakete. Sarean partekatutako informazioaren eta artxiboen eskaintza hain handia denez, ezinezkoa da horien guztien gaineko kontrol orokorra egitea; hortaz, haietarako sarbidearen zaintza, azken finean, erabiltzaileen desioaren eta inplikazioaren mende dago.

Interneten nabigatzean, adingabeak bere adinerako desegokiak diren edukiak aurki ditzake bila ibili beharrik gabe, esaterako, **sexu esplizitua** eskaintzen duten orrialdeak edo **indarkeria duten edukiak**, **hizkuntza desegokia** edo **intentzio txarreko informazioa** duten orrialdeak.

Badira adingabeentzako desegokiak diren edukiak kontrolatzea errazten duten tresnak, WOT kasu (webgunera sartu aurretik, hara eramaten duten estekei lotutako kolore-kodea erabilita, konfiantzari buruz ohartarazten duen luzapena da Mozilla Firefox eta Internet Explorer nabigatzaileetarako), baina **ezerk ezin du ordezkatu seme-alabak Interneteko eduki desegokien aurrean babesteko gurasoek egiten duten zaintza- eta heziketa-lana**.

↘ www.mywot.com/es

Artxiboak partekatzearen arriskuak

Artxiboak trukatzeko (musika, bideoak, softwareak eta abar) programa espezifikoak (P2P) milioika erabiltzailek erabiltzen dituzte sarean egunero. Programa informatikoa instalatzea eta interesatzen zaiguna bilatzeko eskatzea bezain prozedura erraza da eta, oro har, doakoa eta erraz sartzeko modukoa.

Informazioak abiadura handian bidaiatzea ahalbidetzen du sistemak eta fitxategien kopuru handia parteka daiteke informazioa bilduko duen ordenagailu bakarraren beharrik gabe; izan ere, karga, bai banda zabalerarena, bai disko gogorreko espazioarena, parte-hartzaile guztien artean banatzen da.

Praktika horren arriskuak handiak dira. Deskargatutako materialaren autore-eskubideak urratzeko aukera dago, baina ez hori bakarrik, material hori maiz malwarearekin infektatuta egoten da eta arretarik gabeko erabiltzaileak ordenagailuko eduki guztia erraz jar dezake intentzio txarreko pertsonen eskura.

2009ko irailean, G Data enpresak www.gdata.es ohartarazi zuen xede horiekin asko bisitatzen zen webgune jakineko artxibo exekutagarrien % 90 malware motaren batekin infektatuta zegoela.

➘ www.ftc.gov/bcp/edu/pubs/consumer/alerts/salt128.shtm

Sare sozialen arriskuak

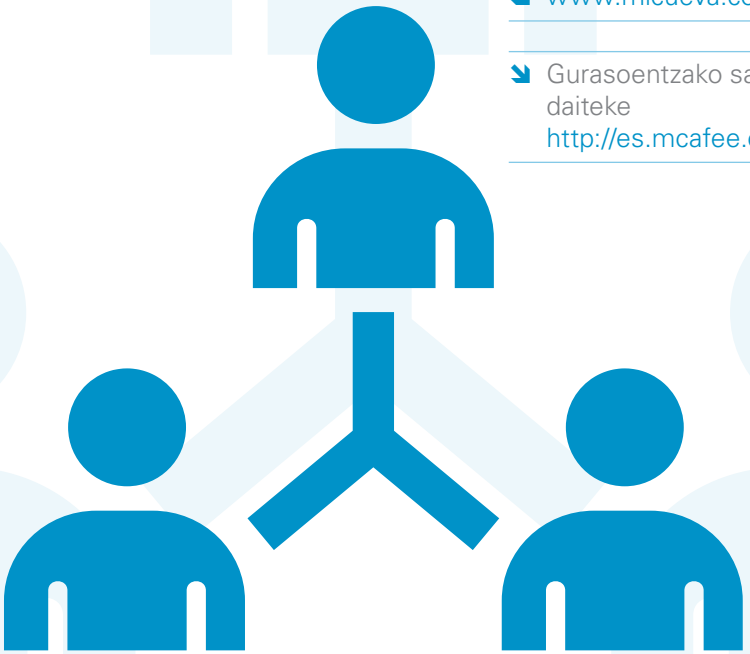
Sare sozialak interakzio sozialerako sistemak dira eta informatikako sistemen bidez pertsonen arteko harremana errazten dute. Izaera irekiko sistema oso dinamikoak dira eta partaidetza aktiboa, edukien trukea eta, oro har, komunikazioa eta topaketa bultzatzen dituzte. Sare horiek oso ezagunak dira adingabeen artean, orrialde pertsonala sortzeko, askastasunez adierazteko eta lagunekin loturak finkatzeko aukera eskaintzen baitiete.

Sare horiek adingabeen segurtasunean eragin dezakete, hautaketa-irizpideak erabiltzea zailtzen duten aukera asko eskaintzen dituztelako, automatismo ugari dituztelako (segurtasunezko sentsazio faltsua) eta hain trebeak ez diren erabiltzaileen segurtasuna zalantzan jar dezaketen aukerak eskaintzen dituztelako (...baina nik ez nekien hori egiten ari nintzenik!).

Gure helburua ez da hain baliagarriak diren sare sozialak satanizatzea, haien ekarpenak, arriskuak eta haiekin jarduteko modu egokiak ondo ezagutzea baizik. Interneten ekimen bikainak daude. PROTÉGELES erakundeak sortu eta bultzatutako adingabeentzako Mi cueva sare soziala horren adibidea da eta bertan segurtasunak eginkizun garrantzitsua du.

- www.micueva.com

- Gurasoentzako sare sozialei buruzko gida berrikustea interesgarria izan daiteke
  http://es.mcafee.com/es/local/docs/SocialNetworkinge-guide.pdf



Segurtasuna telefono mugikorrean

Aurrerapen teknologikoei esker, terminal horiek erabilera tradizionalez gain beste erabilera batzuetarako erabil daitezke (mezu laburrak igortzeko (SMS), jolasteko, argazkiak egin eta bidaltzeko, artxiboak deskargatzeko eta abar). Telefono mugikor modernoek Internetera konektatzeko teknologia dute. Telefono mugikorren (oinarrizkoak edo aurreratuak -Smartphone eta PDA-) erabilera segurua egiteko beharrezkoa da funtzioak ezagutzea eta konpainia guztiek aparatuaren dokumentazioan eskaintzen dituzten erabilera-aholkuak arretaz irakurtzea.

PROTÉGELES erakundeak Madrilgo Komunitateko Adingabeen Defentsaria-rentzako egindako *"haurren segurtasuna eta adingabeek telefono mugikorra erabiltzeko ohiturei"* buruzko azterketan argi azaltzen da adingabeek teknologia horren bidez aurre egin beharreko arrisku-egoerak dagoeneko Interneten topa ditzaketen bezainbeste direla.

Deigarria da jakitea adingabeek ez dutela mugikorra erabiltzen besteekin denbora errealean ahots bidez komunikatzeko. Izan ere, askoz ere maizago erabiltzen dute SMSak bidaltzeko ahozko elkarrizketak izateko baino. Adingabeen % 24k soilik erabiltzen du mugikorra egunero telefono deiak egiteko.

www.protegeles.com/es_estudios2.asp

Segurtasun neurriak eta tresnak

Sistemaren segurtasuna ahultasun nagusiak non dauden ezagutu eta horien zuzenketa egitean oinarritzen da. Ez dago aditua izan beharrik horretarako; nahikoa da beharrezko informazioa ezagutzea, eskuragarri dauden bitartekoez baliatzea eta sen ona erabiltzea.

Dena den, ez dugu ahaztu behar sistema informatikoaren **segurtasun-tresna nagusia** ez dela adituen azken aurkikuntza, software garestia edo tresna konplexuen erabilera; **sarean konektatzeko ohitura egokiak izatea** (Konexio segururako gomendioak kapitulua ikusi) eta beharrezkoak ez diren arriskuak saihestea baizik.

Ordenagailuan

SEGURTASUNEKO oinarrizko ZORTZI aholku:

1. Ekipo informatikoa lehenengo egunetik hasi zaintzen. Sistema eragile berria instalatzean edo ordenagailu berria estreinatzean, harekin elkarreragiteko hasi **eguneraketa** guztiak deskargatzen, **biruskontrako** softwarea instalatzen eta **firewalla** konektatzen. ondoren, egin sistema guztiaren **segurtasuneko kopia**. Sistema eragile modernoek lan horiek egiteko tresna bikainak dituzte, biruskontrako softwarea salbu; hori banaka instalatu behar da.

   Adibidez: avast! (doakoa) hemen www.avast.com/es-es/index

2. Egin astero lanean sortutako informazio guztiaren **segurtasuneko kopia** (backups), datu garrantzitsuak betiko galtzea saihesteko. Aplikazio informatikoak berriro instalatu daitezke, baina haiekin sortutako artxibo pertsonalak ez. Zaila iruditzen bazaizu edo sistema eragileek eskainitako aukerak erabiltzea nekagarria iruditzen bazaizu, erabili zure izenean egiten duten doako programak.

   Adibidez: Cobian Backup helbide honetan www.educ.umu.se/~cobian/cobianbackup.htm

3. **Eguneratuta** mantendu ekipo informatikoa (sistema eragilea eta biruskontrako softwarea batez ere) eta horretarako erabili programek eskaintzen dituzten eguneraketa-aukerak. Erabili bermea, euskarria eta eguneraketak eskaintzen dituzten legezko softwareak.
   Nabigatzaileen kasuan, Internet Explorer (Microsoften nabigatzailea) sistema eragilearen mekanismo berarekin eguneratzen da, hau da, eguneraketa automatikoak aktibatuta. Mozilla Firefox www.mozilla-europe.org/es eta Safari www.apple.com/es/safari automatikoki eguneratzen dira, besterik zehaztu ezean.

4. Internetera haririk gabe (Wi-Fi) konektatzean, **modu seguruan** egin. Erabili nabigatzaileek eskainitako babes-sistemak eta aprobetxatu **gurasoen kontrolak** eskaintzen dituen aukerak. Erabili WPA motako enkriptatzea (edo hobe WPA2 motakoa sistemak onartzen badu), igorritako datuak kapturatzea saihesteko.
   INTECOren webguneak *"Etxeko haririk gabeko konexioa babesteko gida"* deskargatzeko aukera ematen du. www.inteco.es

5. **Fidatu, baina ez izan inuzentea**. Interneten irakurritako guztiak ez du egia izan beharrik. Erabili konfiantza ematen duten konfiantzazko iturriak eta egiaztatu informazioa beste iturri batzuetan zehaztasunik gabeko edukiak eta gezurrak saihesteko. Ez eman informazio pertsonalik telefonoz. Ez fidatu mezu deigarriak edo oso asaldagarriak dituzten orrialdeekin. Zenbait kasutan, birusak zabaltzen dituzten asmo txarreko orrialdeetara bidaltzeko zure arreta lortzen saiatuko dira. Webguneetako edukien arriskua aztertzeko doako tresnak daude; hala nola Mc Afee SiteAdvisor (nabigatzeko aholkularia).
http://es.mcafee.com/root/product.asp?productid=sa

6. Hartu ohitura **pasahitz egokiak** erabiltzeko. 8 karaktere baino gehiago erabiltzea komeni da; letra maiuskulak eta minuskulak, zenbakiak eta ikurrak ausaz konbinatzea aukera ona izaten da. Aldatu zure pasahitzak aldian behin.
Horri buruzko aholkuak ikus ditzakezu Microsoften segurtasun-zentroan www.microsoft.com/latam/athome/security/default.mspx edo Mcafeeren webgunean http://es.mcafee.com/es/local/docs/FamilySafetyPlan.pdf. Gogora ezinak diren pasahitz oso seguruak erabiltzea eta, gero, horiek gordetzeko doako enkriptazio softwarea instalatzea ere ideia ona izan daiteke.

Adibidez:
LoginControl helbide honetan www.pandreonline.com/productos/logincontrol

7. Babestu asmo txarreko softwareak dituzten deskargen aurrean. Programaren bat deskargatu behar duzunean, orrialde ofizialetatik egin beti, edo, bestela, **konfiantzazko orrialdeetatik**. Deskargatutako guztia biruskontrakoarekin aztertu exekutatu aurretik.

8. Erabili web-edukiak **iragazteko programak**. Adingabeentzako desegokiak diren edukietarako sarbideak blokeatzeko gai diren kontrol- eta monitorizazio-tresnak dira. Eduki horietarako sarrera eragozteko erabilitako sistemak askotarikoak izan daitezke (helbide jakinen blokeoa, sarrera-orduen kontrola, eduki jakineko orrialdeetarako sarbidea desgaitzea eta abar). Hori da Espainian Telefónica konpainiak www.telefonica.es etxebizitza/Internet/segurtasuna/zerbitzuak atalean merkaturatzen duen Canguro Net produktuaren kasua edo Archivos PC www.archivospc.com atariak Protección PC atalean eskaintzen dituen iragazteko doako programen kasua.

Telefono mugikorretan

Telefono mugikorretarako segurtasuneko hainbat gomendio eskaintzen dizkizugu. Komunikazioaren Teknologietako Institutu Nazionaleko (INTECO) webgunean doan eskura daitekeen *"Telefono mugikorra babesteko eta modu seguruan erabiltzeko gidarekin"* osa dezakezu informazio hori.

↘ www.inteco.es

— Telefono mugikorra ez bistatik galdu leku publikoetan, gaizkileentzat oso erakargarria izan baitaiteke manipulatzeko edo lapurtzeko. Ez utzi telefono mugikorra ezezagunei. Lapurtzen saiatuz gero, zure segurtasun fisikoa zaindu eta uko egin telefonoari.

— Aktibatu **PIN kodea** (telefonoko SIM txartelera sartzea ahalbidetzen duen edo eragozten duen kode pertsonala) eta leku seguruan gorde **PUK kodea** (PIN kodea hiru aldiz oker sartuz gero telefonoa desblokeatzea ahalbidetzen duen segurtasun-kodea).

— Terminala **blokeatzeko** aukera aktibatu desblokeatzeko pasahitza eskatuta. Telefonoak deiak egiten uzten ez badu ere, datuetara sartzen utz dezake (informazio pertsonala).

— **Pasahitz** seguruak eta sendoak erabili beti sarbidea eta konexioak babesteko (ikusi horri buruzko pasahitzen konfigurazioa -25 horrialdea- ordenagailuari buruzko atalean).

— Telefonoko tarifan **kontsumoa** zaindu eta edozein irregulartasunen aurrean berehala informatu. Adingabeen kasuan, oso gomendagarria da aurreordainketako txartelen sistema erabiltzea.

— Igorlea ezezaguna bada, ez zabaldu **mezu elektronikorik** eta ez onartu artxiborik. Ez erantzun ezezagunen irudiak dituzten **SMS**ak. Software originala instalatu beti; horrela, laguntza eskatu ahal izango diozu fabrikatzaileari.

— **Bluetooth**a ez utzi inoiz piztuta erabiltzen ari ez bazara. Bluetootha datuak eta ahotsa transmititzeko teknologia bikaina da (autoko esku libreko telefonoa), baina segurtasun maila ez da hain bikaina (erabiltzaileak egiten duen erabilera egokiaren mende dago). Nolanahi ere, baimena eskatu konexio bakoitzerako eta desaktibatu telefono mugikorra besteentzako ikusteko moduan agertzea ahalbidetzen duen aukera.

— Ohitura hartu eta adingabeak ohitu lagunei edo ezagunei argazkiak atera aurretik **baimena eska dezaten**. Ikastetxeetan, gimnasioetan edo igerilekuetan telefono mugikorrarekin argazkiak ateratzea debekatuta dago.

— Ez erantzun inoiz eduki mehatxagarria duten **SMS**ei. Mugikorraren bidez mehatxuak jasoz gero, gomendagarria da deiaren ordua apuntatzea, mezua gordetzea eta ikastetxeko zuzendaritzari edota poliziari horren berri ematea (ikusi Ikuspegi legala kapitulua).

— Aldian behin egiaztatu seme-alaba adingabeen telefono mugikorrean **gordetako telefono-zenbakiak**.

Gainera, Telefónica, Orange, Vodafone eta Yoigo konpainiek 2007ko abenduaren 12an kode hau hitzartu zuten: "Adingabeek Espainiako komunikazio elektroniko mugikorretako edukien zerbitzuez erabilera arduratsua egin dezaten bultzatzeko operadore mugikorrentzako jokabide-kodea". Hemen ikus dezakezu:

↘ www.gsmeurope.org/documents/eu_codes/spain_codigo.pdf

Zenbait galdera eta erantzun

Sekulako garrantzia du adingabeei lehen urratsetan laguntzea eta gure ohiturak haientzat erakusgarri bihurtzea.

Zein da Sarean elkar eragiten hasteko adin egokia?

Kontuan izan Internetera konektatzeko moduak adingabearen adinak baino garrantzi handiagoa duela. Sarea gero eta adingabe gehiagok erabiltzen du eta hori gero eta goizago gertatzen da. Hezkuntza-sistemak, hain zuzen, sarean konektatzea sustatzen du eskolako orduetan.

Sekulako garrantzia du **adingabeei lehen urratsetan laguntzea** eta gure ohiturak **haientzat erakusgarri** bihurtzea. Adingabeek konektatuta egoteko irizpiderik ez dutenez, lehen hurbilketa horiek garrantzi berezia dute. Hasieran, **eseri beraiekin batera** konektatzen direnean. Egiaztatu nabigazio seguruaren oinarrizko printzipioak ulertu eta erabiltzen dituztela. **Aurrea hartu** etxetik kanpo jasoko duten informazioari.

"Microsoften Babes Zentroan: haurren segurtasuna", esaterako, zure zalantzen erantzunak topatu ahal izango dituzu *"Gurasoentzako on lineko segurtasunari buruzko gida"*.

www.microsoft.com/latam/athome/security/default.mspx

Adingabeak Internet-adikto bihur al daitezke?

Internet gazteentzako tresna interesgarria da, batik bat ezagutza informatikoak dituztenentzat, autoestimua areagotzen lagun baitiezaieke. Hala ere, gehiegizko erabilerak besteengandik edo bestelako jardueretatik (eskolako lanak, ariketa, atsedena edo lagunekin egoteko denbora) are gehiago isolatu ditzake lotsatiak diren haurrak.

Edozein motatako mendekotasuna edo adikzioa jokabidearen gaineko kontrola galtzea ekartzen duen jarrera da. Bestelako jarduera atsegingarrien inguruko interesa galtzea ekartzen du gainera, eta bizitzan interferentzia nabarmena eragiten du.

Teknologia horien gehiegizko erabilerak **sintoma** kezkagarriak sor ditzake eta gurasoek horiek ezagutzen ikasi behar dute:

— Sentsazio atsegina edo **euforia** konektatuta dagoen bitartean eta egoera emozional nahasia (**antsietatea**, **ezinegona**, **suminkortasuna**...) jarduera eteten denean.

— Jokaera errepikatzeko desio sakona, **konexio-denbora pixkanaka luzatuta** eta norberaren jokabidea ukatzea edo minimizatzea.

— Harreman sozialak eta familiako harremanak kaltetzea. **Isolamendua**. Eskolako errendimenduaren beherakada.

— Lo-faltagatik eta ariketa fisikorik ez egiteagatik eratorritako arazo fisikoak (**nekea**, **ahultasuna**, **logura**...).

Gorabehera horietakoren bat sumatuz gero, edo zalantzarik izanez gero, kontsultatu espezialistari.

↘ www.microsoft.com/latam/athome/security/default.mspx

Egokia al da adingabeek beren posta elektronikoko kontuak izatea?

Haur txikiek familiako posta elektronikoa partekatu behar dute, beraiena izan ordez. Hazten diren heinean eta independentzia gehiago nahi duten neurrian, helbide propioa eman diezaiekezu baina denbora horretan **gaiari buruzko informazioa jaso behar dute**. Mezuek familiako sarrerako ontzian egoten jarrai dezakete. Internet zerbitzu-hornitzaileari (ISP) galdetu familiako posta elektronikoko kontuetarako zein aukera eskaintzen dituen, nahi ez den postarik, eskatu gabeko mezurik, edo iruzur egiteko igorpenik ez jasotzeko.

Adingabeak konektatzen direnean zer webgune bisitatu duten jakin al dezakegu?

Horretarako aukera ugari dago, baina errazena nabigatzaile guztiek beren menuetan eskaintzen duten Interneteko konexioen historiala berrikustea da. Nabigazioko Historialak bisitatutako webguneak erregistratzen ditu. Nabigatzaileek zerbitzu hori eskaintzearen arrazoi nagusia aurretik bisitatutako webguneen araberako bilaketako iradokizunak eskaini ahal izateko duen erabilgarritasuna da. Dena den, kontuan izan historiala edozein unetan ezaba dezakeela adingabeak.

Zer egin behar dut seme-alaba on line jazartzen badute?

Edozein jazarpen-egoera edo haren edozein susmo larrialdia da. Nerabeen arteko ziberjazarpeneko arazoak gero eta ohikoagoak dira (ikusi Adingabeekin lotutako segurtasun arazoak kapituluko Mehatxu pertsonalak: Grooming-a, Ziberjazarpena eta Sexting-a atala).

Jazarpena gertatuz gero, mezuak bidaltzen dituen pertsona **blokea** dezakezu posta elektronikoko eta berehalako mezularitzako programa gehienek eskaintzen dituzten blokeo-aukerekin. Gorde jazarpena biltzen duten posta elektronikoko mezuak eta bidali posta elektronikoko zerbitzuen hornitzaileari. Hornitzaile gehienek jazarpena debekatzen duten erabilera egokiko araudiak izaten dituzte.

Arazoa berehala konponduko ez balitz, modu erabakigarrian esku hartu eta **salatu** jarrera maltzur hori (ikus salatzeko sistemak atala Ikuspegi legala kapituluan).

Funtzionatzen al du iragazteko softwareak?

Iragazteko tresnak erabilgarriak izan daitezke gazteen kasuan gurasoen gainbegiraketa osatzeko (sekula ez ordezkatzeko). Dena den, iragazkiak eta blokeatzaileak ez dira erabat seguruak edo hutsik gabeak izaten eta, batzuetan, ez dute ezegokia den material guztia

Seme-alabak babesteko modurik onena haiek heztea da Sareak eskaintzen dituen aukera guztiak modu arduratsuan eta seguruan erabil ditzaten

blokeatzen. Gainera, baliteke gehiegizko arreta dela eta, haurrek beren eskolako etxeko lanetarako behar izan ditzaketen eduki erabilgarri ugari ere blokeatzea. Automatismoak erabiltzearekin lotura duten arazoak izan ohi dira; haien funtzioa gurasoei laguntza ematea da, ez haiek ordezkatzea.

Ez dago asmo txarrak dituzten erabiltzaileengandik adingabea erabat babes dezakeen iragazkirik. Beti izango dira segurtasun-neurri horiek gainditzeko modua aurkitzen saiatzen diren pertsonak. Horregatik, **seme-alabak babesteko modurik onena haiek heztea da** Sareak eskaintzen dituen aukera guztiak modu arduratsuan eta seguruan erabil ditzaten.

Seme-alabak txikiak direnean iragazkiak erabilgarriak izan daitezkeen arren, hazten diren neurrian, **on lineko portaera segurua eta arduratsua** garatu behar dute.

Zer da gurasoen kontrola? Nola funtzionatzen du?

Gurasoen kontrola oso tresna erabilgarria da erantzukizunpean adingabeak dituzten gurasoentzat. Horren bidez, ahal den neurrian, adingabeak desegokiak diren Interneteko edukietara sartzea eragotzi nahi da.

Horretarako, adingabeak sar daitezkeen edukietan **iragazkiak** aplikatzen dituzte eta, horien bidez, sarbidea eragozten edo baimentzen zaie. Adingabea webgune batera konektatzen denean, nabigatzaileak aurrez ezarritako erabiltzaile-izena eta pasahitza eskatuko dizkio (saio bakoitzaren hasieran). Datu horiek sartutakoan, guneaen katalogazioa egiaztatzen da eta adingabearentzat baimenduta ez dagoenean, sarbidea eragozten zaio.

Iragazketa-sistema pertsonaliza daiteke eta zure telefono-konpainiarekin kontrata dezakezu.

Horren inguruan, interesgarria izan daiteke Komunikazioaren Teknologietako Institutu Nazionalaren Segurtasuneko Behatokiak argitaratutako *"Nola aktibatu eta konfiguratu sistema eragileen gurasoen kontrola"* gida ikustea:

➘ www.inteco.es

Gure seme-alaba nerabeak on line egin nahi du erosketa. Nola jakin dezaket gunea segurua den?

Seme-alaba nerabeari kreditu-txartela on line erabiltzen utzi aurretik, on lineko erosketen inguruko irizpide argi batzuk eta transakzioak seguruak izan daitezen eta babestuta egon daitezen kontuan izan beharko dituen argibideak eman beharko dizkiozu.

Webgune batean erosi aurretik, gutxienez, hauek bilatu beharko dituzue:

— Orrialdearen beheko ertzean giltzarrapo itxiaren ikonoa; hauxe adierazten du horrek: egindako transakzioak erabiltzaileak eta webguneak soilik ikus ditzakete.

— Esploratzaileko helbideen taulan ikusgai egoten den webgunearen helbidearen hasieran, http**s** bat ("s" horrek segurua dela adierazten du).

Aurreko elementuak faltsifika daitezke; hori dela eta, garrantzitsua da seme-alabei on line erosketak egin aurretik zuri galdetzeko esatea. Horren bidez, zeu bihurtuko zara webgunea segurua den ala ez den zehazteko amaierako epailea.

Nola eragotz ditzaket nire ordenagailuan ateratzen diren elementuak?

Ateratzen diren elementuak (pop-up izenekoak) eragozteko modurik errazena horiek blokeatzen dituen softwarea erabiltzea izaten da. Internet Explorer, Mozilla Firefox eta Safari nabigatzaile modernoek ateratzen diren elementu horiek blokeatzeko zuzeneko sistema izaten dute eta hori menu honen bidez konfigura dezakegu: Tresnak>Aukerak.

➘ http://support.mozilla.com/es/kb/Ventanas+emergentes

➘ http://windows.microsoft.com/es-es/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions

Sistema eragilearen eguneratze automatikoak aktibatu edo desaktibatu egin behar ditut?

Oso komenigarria da sistema eragileek eskaintzen duten Eguneratze automatikoak aukera **aktibatuta mantentzea** eta kalitatezko birusen aurkako softwarea izatea. Eguneraketak softwarearen osagarriak izan ohi dira eta ordenagailuan arazoak ekiditeko edo erroreak (ahultasunak) zuzentzeko balio izaten dute haiek aurkitzen dituzten neurrian. Horri esker, ordenagailuak egonkortasun handiagoa lortzen du eta sistemaren segurtasun handiagoa berma dezakegu.

➘ www.consumer.es/web/es/tecnologia/software/2009/08/24/187121.php

Zenbat urterekin izan beharko lukete adingabeek telefono mugikorra?

Telefono mugikorraren erabilera oso bizkor hedatu da adingabeen artean; neurri batean, horretan eragina izan du teknologia hori eskuragarri izatearen berezko interesak, baina bestetik, ez dugu ahaztu behar telefoniako konpainiek egiten duten presioa. Izan ere, konpainia horientzat, biztanleriaren segmentu hau etorkizunerako aukera garrantzitsua da.

Urrats hori eman aurretik serioski egin beharko zenuke gai horren inguruko hausnarketa eta biltzen dituen arriskuak eskaintzen dituen onurekin alderatu beharko dituzu (galdetu hau zeure buruari: zertarako behar du telefono mugikorra X urteko neskak edo mutilak?). Edozein kasutan, adingabeak gailu horren inguruan egingo duen erabilerarekin lotutako **oso arau zorrotzak ezarri**.

Konexio segururako gomendioak

Internet adingabeen prestakuntzarako eta aisialdirako aukera garrantzitsua da, baina segurtasuneko ohitura onak izan behar dira erabat goza dezaten.

Oro har, oso erabilgarria izaten da Sareko konexioetarako **familiako arauak** adostea, ordenagailutik gertu gordeko dugun paperean idatziz jasotzea eta zehatz-mehatz errespetatzea. Hauek izan daitezke horren adibideak:

— Benetako datu pertsonalak biltzen dituen erabiltzaile-izenekin ez erregistratzea eta benetako nortasunaren inguruko informaziorik ez argitaratzea.

— Sekula ez jakinaraztea pasahitzak, helbidea edo telefono-zenbakia.

— Argazki desegokirik edo nortasuna agerian utz dezakeenik ez argitaratzea, eta erabiltzaile-izen probokatzailerik ez erabiltzea.

— Sarearen bidez ezagutu ditugun ezezagunekin sekula informaziorik ez partekatzea.

— Interneten bidez harremanetan jarritako ezezagunekin sekula ez elkartzea.

— Sekula ez irekitzea jatorri ezezaguneko fitxategi-eranskinik.

Webean modu seguruan nabigatzeko aholkuak

— Babestu ordenagailua saio-hasiera mugatzeko **pasahitzarekin**, guk horren berri izan gabe hirugarren bat saiora sar ez dadin. Pasahitzak, bistakoa denez, isilpean gorde behar dira eta ez zaizkio hirugarren bati jakinarazi behar edo eskuratzeko errazak diren tokietan idatzi behar.

— **Ez eman datu pertsonalik** nork jasoko dituen erabat seguru ez badakigu. Eta sekula ez beharbeharrezkoak diren horiek baino gehiago.

— **Sekula ez partekatu informaziorik** konexioa segurua ez bada. Oso erraza da konexio segurua ezarri dugun jakitea; izan ere, ordenagailuan, konektatu garen orrialdearen helbidearen hasieran, https jarriko du, http beharrean. Gainera, nabigatzailearen beheko zatian (egoera-barra) itxitako giltzarrapoa ikusiko duzu.

— Sistema eragileak eta nabigatzaileak haiek diseinatzen dituzten enpresek argitaratutako adabakiekin (gomendatutako eguneraketa automatikoak) **eguneratu**.

— Ez kontratatu zerbitzuak IP finkoko helbidea ematen duten Interneteko hornitzaileetan; izan ere, hori eginez gero, erraza litzateke adingabea kokatzea nabigatzen ari denean edo haren inguruko datu garrantzitsuak lortzea. Ahal denean, **kontratatu** Interneteko zerbitzuak IP dinamikoa duen helbidearekin. Ohikoena izaten da, baina egiaztatu.

— Egiaztatu ordenagailuak kalitateko **birusen kontrako** softwarea duela instalatuta eta egunero eguneratzen dela automatikoki.

— Erabili sistema eragileek, birusen kontrako programek eta web-nabigatzaileek izaten dituzten **gurasoen kontroleko** aukerak. Oso komenigarria da erabiltzen hasi aurretik segurtasuneko eta murrizketako aukerekin sistema eragilea eta nabigatzailearen softwarea konfiguratzeko denbora ematea. Horiek guztiak oso esplizituak izaten dira eta nabigatzaileetako Tresnak menuan eta sistema eragileetako Hasi menuan egoten dira erabilgarri.

— Fitxategiak deskargatu aurretik, hartu beharrezko neurriak; hori dela eta, deskargatu aurretik, egiaztatu **webgune horrek bermea** edo behar adinako konfiantza duela.

— Arreta jarri ordenagailuan **software gaiztoa** instalatu dela erakusten duten zantzuak hautemateko. Ordenagailuan software mota hori instalatuta dagoela adierazten duten ezaugarrietako batzuk hauek dira: orrialde nagusia edo nabigatzailearen konfigurazioko beste elementu batzuk aldatu egin dira, webgune batzuetara ezin gara sartu, bat-batean irekitzen diren leihoak etengabe ateratzen dira, tresna-barra berriak instalatu dira edo ordenagailua oso mantso dabil...

— Adingabeak bizi diren etxean familiaren **ordenagailuaren kokalekua** erabakitzea garrantzitsua da. Ordenagailua mugimendu handiko **familiako eremuan** jartzea eta haurrek ordenagailua erabiltzeko orduen kopurua mugatzea komeni da.

Posta elektronikoaren erabileraren inguruko gomendioak

— **Ez ireki** jatorri ezezaguneko posta-mezurik; ezabatu zuzenean. Susmorik txikiena izanda ere, ez egin klik mezuetan dauden esteketan.

— **Ez exekutatu** mezuaren testuan datorren fitxategi-eranskinik, batez ere jatorria ezezaguna bada edo oso mezu iradokitzaileak badira. Batez ere, ez ireki fitxategia birusen kontrako softwarearekin aztertu aurretik.

— **Ez parte hartu** mezuen kateetan edo, gutxienez, beharrezko neurriak hartu: ezabatu mezuaren ondoz ondoko bidalketetan sartu dituzten hartzaileen helbideak.

— Erabili **spam**aren aurkako **iragazkiak**. Iragazki horiek (besterik zehaztu ezean, posta elektronikoko programetan txertatuta egoten dira) Sarrerako erretiluan nahi ez dugun posta-mezu asko azaltzea eragozten dute.

— **Ez eman** sekula **erabiltzaile-izenaren** edo **pasahitzaren** inguruko daturik.

— Ahal den neurrian, **ez erabili** gorde pasahitza aukera; askotan, konexio berri bakoitzean pasahitza berriro sartzeko lana saihesteko eskaintzen da.

— **Ez eman** helbide elektronikoa "errazegi".

— **Konfiguratu** posta-programa **segurtasun mailarik handienean**. Beti aktibatuta izan defentsa proaktiboa duen biruskontrako on bat eta firewalla. Aktibatu erabiltzen duzun posta elektronikoko programak eskaintzen duen mezu baztergarriak bereizteko iragazkiak.

— Kontuan izan hartzaile ugariri posta-mezuak bidaltzen dizkiezunean haien posta elektronikoko **helbideak ere ematen ari zarela**. Helbide horiek Hartzailea edo Kopia (Cc) eremuetan azaltzen dira. Hori ekiditeko, mezuaren hartzaileen helbideak Ezkutuko kopia (Cco) eremuan sar ditzakezu. Horri esker, hartzaileek ezingo dute gainerako hartzaileen posta elektronikoko helbidera sartu eta mezua berdin-berdin iritsiko zaie.

Berehalako mezularitzako zerbitzuak eta txatak erabiltzeko aholkuak

— Webean nabigatzeko garaian zuzena denaren inguruan eta, batez ere, on lineko hizketaldi horietan (txatak) **arau finkoak eta adostuak ezarri**.

— Bide horietatik **sekula ez eman** isilpeko daturik: pasahitzak, erabiltzaile-izenak, helbidea, ikastetxea eta abar. **Sekula ez bidali** argazkirik txataren bidez ezagutu dituzunei.

— **Ekidin** susmagarriak diren edo ezezagunek emandako aretoak bisitatzeko egindako gonbidapenak. Kontu izan ezezagunekin hitz egitean edo kontaktu ezezagunak gehitzean.

— **Egiaztatu** seme-alabek ez dituztela ".alt" hizketaldirako aretoak erabiltzen adingabeentzat desegokiak diren gai alternatiboetan oinarrituta badaude.

— **Uko egin** "nahi ez dituzun" erabiltzaileei; hau da, haien mezurik jaso nahi ez duzunei. Zure kontaktuen zerrendan azaltzen diren pertsonekin soilik komunikatu.

— **Kontu izan** "nick" edo ezizena sortzeko garaian. "Ezizen" horrek ez luke informazio pertsonalik eman beharko (ez zuenean, ez zeharka).

— **Sortu barrera** nahi ez duzun berehalako mezularitzaren aurka. Ez eman ezezagunei zure ezizena edo posta elektronikoko helbidea eta saiatu horiek Interneteko direktorio handien edo on lineko komunitateko profilen moduko eremu publikoetan ager ez daitezen.

— **Sekula ez ireki** irudirik eta ez deskargatu bidaltzaile ezezagunek igorritako fitxategirik edo mezuetako estekarik.

— Ordenagailu publikoa erabiltzen ari bazara, **ez hautatu** Saioaren hasiera automatikoa aukera. Zure ondoren ordenagailu bera erabili behar dutenek zure nick ikusi eta konektatzeko erabil dezakete.

Operadore gehienek modu aktiboan lan egiten dute teknologia horiek biltzen dituzten arriskuen prebentzioan. Horretarako, gako-hitzak blokeatzeko edo izen ezberdinak erabiltzen dituzten erabiltzaileak detektatzeko tresna automatikoak erabiltzen dituzte. Kanal batzuetan, gainera, moderatzaileak ere izaten dira. Lasai galdetu zure telefonia-konpainiari horren inguruan zer politika duten.

P2P trukeko programen inguruko gomendioak

— P2P sareetara sartzeko, ezinbestekoa da **programa** (doakoa) **instalatzea**. Programa hori onartutako guneetatik deskargatu behar da beti eta, ahal den neurrian, programaren sortzailearen webgunetik.

— Programa instalatu aurretik, **sistemaren segurtasun-kopia** egitea eta, instalatu ostean, nahi dugun programa hori soilik instalatu dugula egiaztatzea komeni da. Izan ere, programa horietako batzuek, aldi berean, software gaiztoa ere instalatzen dute eta horrek gure sistema ezegonkorra bihurtu edo sakatzen ditugun teklak edo gure konexioak araka ditzake.

— Konexiorako **ataka ez-estandarra** ezarri programarekin administrazio mailako komunikazioa izateko (beti 1024 baino altuagoa).

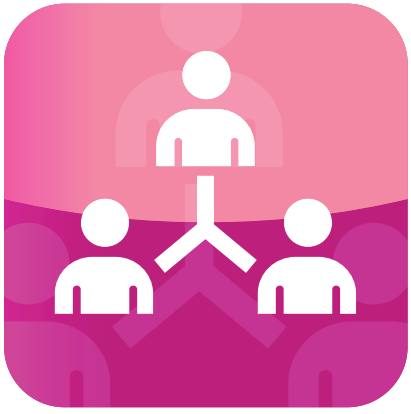
— Bezero-programak komunikazio irekia eguneko 24 orduetan mantentzeko gai dira. Gaur egungo tarifa finkoaren bidezko Interneten sarbideen erraztasunei esker, gero eta ohikoagoa da. Hori dela eta, oso komenigarria da ordenagailuko ataketara sarbidea mugatzen duen **suebakia instalatzea edo aktibatzea**.

— Ordenagailuan zerbitzaria instalatzeak berekin dakartzan **arriskuak aztertu** behar dituzu; izan ere, zure IP helbidea ezagutarazi beharko zenuke eta, horren bidez, jende askok jakingo luke ordenagailua non duzun eta zer software duzun. Ez duzu lortuko fitxategiak bizkorrago deskargatzea eta banda-zabaleraren kontsumoa asko handituko da.

— P2P programa instalatzean zure disko gogorraren zati bat beste batzuekin **partekatzen ari zara**; hori dela eta, han gordetako informazio osoa egongo da hirugarren batzuentzat eskuragarri. Kontuz aukeratu zer direktorio partekatu behar duzun eta saiatu sistema eragilearen kokalekutik desberdina den partizioan izatea. Ahal den neurrian, instalatu beste disko batean. Dena den, egokiena ordenagailu bat helburu horretarako soilik erabiltzea litzateke.

— **Kontuan izan balitekeela fitxategiak dioten hori ez izatea**. Fitxategiaren izenak ez du esan nahi barruan esaten duen hori duenik. Egokiagoa da ez deskargatzea fitxategi exekutagarriak (.exe amaiera dutenak) edo, deskargatuz gero, behar bezala eguneratuta dagoen biruskontrako on batek aztertu aurretik ez exekutatzea.

— **Ez baimendu seme-alabei fitxategiak modu librean deskargatzea**. Segurtasuneko urrats argiak ezarri eta horiek bere horretan mantendu.



Haririk gabeko konexioen inguruko gomendioak

— **Itzali sargunea** erabili behar ez duzunean. Ez konektatu ezezagunak diren sarguneetara, batez ere, erraza bada.

— **Desaktibatu zure Wi-Fi sarearen izena hedatzeko aukera** (SSID ere deitzen zaio) kanpoko ordenagailuek zure haririk gabeko sarearen datuak automatikoki identifika ez ditzaten.

— **Aldatu besterik zehaztu ezean datorren pasahitza**; izan ere, fabrikatzaile askok gako bera erabiltzen dute ekipamendu guztietarako.

— **Erabili WPA motako enkriptatzea** (edo hobe WPA2 motakoa sistemak onartzen badu), igorritako datuak kapturatzea saihesteko. WEP protokoloa soilagoa da eta enkriptatze ahulagoa eskaintzen du.

Internautaren Segurtasun Bulegoaren webgunean teknologien erabilerarekin lotutako ohitura erraz batzuk gomendatzen dituzte:

➘ www.osi.es/Babes_zaitez/

Bideojokoekin lotutako orientabideak

Bisitatu www.guiavideojuegos.es/index.htm webgune espezializatua; bertan deskargatu ahalko duzu PROTÉGELESek eta Asociación Española de Madres y Padres Internautas (AEMPI) elkarteak garatutako *"Bideojokoen inguruko gurasoentzako gida"* www.guiavideojuegos.es/guia.pdf.

Telefono mugikorren inguruko aholkuak

— **Ez eman telefono-zenbakirik** (finkokoa edo mugikorrekoa) horiek eskatu dizkizuen ezezagunei; izan ere, baliteke linearen ezaugarriak ezagutzen saiatzen aritzea.

— Okerreko telefono-deia izanez gero, bizkor **eten komunikazioa** zure telefono-linearen fakturara zordundutako deien desbideratze posiblea saihesteko.

— "Hiruko deia" izeneko modalitatea kontratatuta izanez gero, **arreta handia izan**; informatikako programa batekin araka dezakete linea eta bertan bidegabe sar daitezke nazioarteko deiak egiteko telefonoaren titularrari zordunduta.

— **Ez onartu** deia jasotzen duenak ordaintzeko deirik hori nork eskatu duen erabat ziur ez bazaude.

— Kontuan izan **sekula ez dela beharrezkoa** tarifikazio osagarriko aurrezenbakietara telefonoz deitzea.

Internet bidezko telefono-deiaren zerbitzuen (VoIP) inguruko OHARRA (Skype, esate baterako):

Ez dira zehatz-mehatz telefonia-zerbitzuak. Hori dela eta, ezin dute telefono tradizionala ordezkatu kalitateari edo prestazioei dagokienez. Baliteke, agian, larrialdiko zenbakietara (112, 091 eta abar) sarbiderik ez izatea edo behar dugunean ez funtzionatzea. Ez dituzte kalitateko gutxieneko maila batzuk bermatzen, fabrikatzaileak erabakitzen dituen horiez gain.

Aipatutakoa gogorarazteko: gomendioen dekalogoa

III

I. **Hezi** seme-alabak Sarean topa ditzaketen arriskuen inguruan. Horretarako, ikasi ordenagailuen eta Interneten inguruko oinarrizko funtzionamendua, eta ziurtatu informazio hori ulertu duzula; jarraian, **zure jokabidea erakusgarri bihurtu**. Jakinarazi adingabeei Interneten ateratzen den guztiak ez duela zertan egia izan behar, ustekabekoak har baitaitezke. Sarean ondo zer dagoen eta gaizki zer dagoen bereizteak duen garrantziaren inguruko (bizitza errealean bezalaxe) irizpideak eman seme-alabei. Partekatu seme-alabekin IKTen inguruko berrikuntzen inguruko ezagutzak.

II. **Lagundu** adingabeari nabigatzen ari denean ahal den guztietan. Gazteenek beti izan beharko lukete alboan heldu bat Sarearekin elkarreragitean. Gozatu Internetek eskaintzen dituen aukeraz seme-alabekin. Bultza itzazu haien zalantzak partekatzera. Saiatu seme-alabek Interneten ezagutu dituzten gauzak naturaltasunez konta ditzaten. **Denbora eman komunikazioko ohitura zuzenak bultzatzeko** (irakurketekin edo higiene pertsonalarekin egiten duzun moduan). Seme-alaben jarduera zibernetikoak positiboak direla bermatzeko modurik onena **haiekin hitz egitea izaten da**.

↘ www.privacyrights.org/spanish/pi21.htm

III. Adingabeari, informazio pertsonalari dagokionez, Interneteko nabigaziorako **segurtasuneko ohitura** zorrotzak barneratu. Informatikako aplikazioek (mezularitzako programak, bideojokoak, txatak eta abar) pasahitzak eskatzen dituztenean, lagundu behar bezala konfiguratzen. **Gurasoek arretaz zaindu** beharko lukete seme-alabek informazioa ez dutela ezezagunekin partekatzen. Internetek zirkulazioaren edozein aztarna gordetzen du; hori dela eta, garraiatutako informazioa araka daiteke.

IV. **Adingabeei irakatsi egin behar zaie** Internet bidez informazio pertsonalik ez ematen. Ohartarazi Sarean **informazio pertsonala ez partekatzearen** garrantzia (helbidea, telefonoa, ikastetxea edo non jolastea gustatzen zaien). Informazio hori ematea inoiz ez da beharrezkoa Sarean gozatzeko. Irakurri zure seme-alabek bisitatzen dituzten guneetako pribatutasun-politikak. Webgune onenek oso ondo azaltzen dute jasotako informazioa.

V. Estutu seme-alabak Sarean **jabetza errespeta** dezaten. Azal iezaiezu beste pertsonen lanak deskargatzea edo legez kanpoko kopiak egitea ez dagoela ondo edo legez kanpokoa dela. Beharrak asetzeko lehen aukera moduan, adingabea ohitu dadila Sarean **doako tresnak bilatzera**; izan ere, dibertigarria da, desafiatzailea eta sorpresa handiak ekartzen ditu. Doako tresnak bilatzeko hainbat aukera daude:

↘ www.softonic.com

↘ http://es.wikipedia.org/wiki/Portal:Software_libre

VI. **Azaldu** zein arazo ekar dezakeen eduki ez desiragarriak dituen komunikazioetan parte-hartzeak (hizketaldi probokatzaileak, arrazistak, iraingarriak, erradikalak…) edo gaizki sentiarazten dietenetan. **Jokabide oneko arauak errespetatzearen beharra** nabarmendu, pertsonen arteko elkarrekintzaren moduan. Internet pertsonen arteko komunikazio-sistema da; horregatik, arretaz eta

beste aldean dagoenarekiko errespetuz jokatuz erabili behar da.

VII. **Jarri arreta Sareko lagunei**, presentziazko adiskideei bezala. Norbaitekin harremanetan jartzean, hari buruz ahalik eta gehien jakitea da onena. Adingabeak ulertu behar du Interneten hizketakide duen pertsonak konfiantzazkoa dirudien arren, inoiz ezin dela jakin nor dagoen beste aldean, hortaz, **ahalik eta zuhurren jokatu behar da**.

VIII. **Arau xumeak jarri**, betetzeko errazak direnak eta lehenengo unetik ohitura bilakatuko direnak. Ziurtatu familiako guztiek betetzen dituztela. Erakutsi adingabeari Sarean zure bilaketetan parte har dezan utziz. **Irakatsi zure "egiteko modua"** eta esaiozu berdin egiteko.

IX. Zaindu adingabeak Interneten **konektatuta ematen duen denbora**, beste jarduera batzuk albo batera utzi ez ditzan. Kontrolatu telefonoko fakturak. "Lineako gastuetarako" aurrekontuak finkatu eta betetzen direla gainbegiratu. Egiaztatu aldian behin seme-alabek ordenagailua zertarako erabiltzen duten. Ordenagailua partekatutako lekuan jarri, baina ez estutu adingabea etengabeko ikuskapenekin eta disuasio-betebeharrekin, seguru asko etxetik kanpoko tokietara aldatuko baitu konektatzeko lekua. Behar izanez gero, erabili konexio-denbora kontrolatzeko tresnak. Interneteko Kalitate Agentziaren (IQUA) Internet segurua webgunean *"Kontrolerako tresnen zerrenda"* topa dezakezu.

➘ www.internetsegura.net Pestaña Recomendaciones

X. Sortu adingabea sistema eragilean sartzeko **mugatutako erabiltzaile kontua**. Oso komenigarria da ordenagailuetara sarbide pertsonalizatua sortzea, sistema eragile guztiek eskaintzen duten Erabiltzaile kontuaren sorrera aukeraren bidez. Adingabeak Internet bidez sartuko dira mugatutako edo murriztutako erabiltzaile-kontuen bidez; ordenagailura "administratzaile" moduan sartzeko aukerarik eskaintzen ez duten kontuen bidez, alegia.

➘ http://windows.microsoft.com/es-XL/windows-vista/What-is-a-user-account

Komunikazioaren Teknologietako Institutu Nazionalaren webgunean *"Gurasoentzako adingabeak Interneten gida"* topatuko duzu.

➘ www.inteco.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiapadresymadres.pdf

I

- **Zure jokabidea erakusgarri bihurtu**
- **Hitz egin seme-alabekin**
- **Irakatsi seme-alabei informazio pertsonalik ez ematen**
- **Arau xumeak jarri**

II

IV

Ikuspegi legala

"Delitu informatikoaren" kontzeptua konplexua da. Arazoaren inguruan Europa mailan egindako hurbilketa-lana da Europako Kontseiluak 2001eko azaroan adostutako "*Ziberdelinkuentziari buruzko hitzarmena*"; Espainiak oraindik ez du lan hori berretsi.

↘ www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Legediari dagokionez, dena den, alor penaletik kanpo hazten ari den legezko zerbitzua dago eta Informazioaren Gizarteko hainbat alderdi arautzea du helburu:

— **Haurrak eta Nerabeak Zaintzeko eta Babesteko Legea** [EHAA 2005-03-30]

— **Jabetza Intelektualari buruzko Legea** [BOE 1996-04-22]

— **Datuak Babesteko Lege Organikoa** [BOE 1999-12-14]

— **Izaera pertsonaleko datuak dituzten fitxategi automatizatuen segurtasun-neurrien araudia** [BOE 1999-06-25]

— **Informazioaren Gizarteko Zerbitzuen eta Merkataritza Elektronikoaren Legea** [BOE 2002-07-12]

— **Telekomunikazioetako Lege Orokorra** [BOE 2003-11-04]

— **Sinadura Elektronikoaren Legea** [BOE 2003-12-20]

— **Herritarrek Zerbitzu Publikoetan sartzeko bide Elektronikoak erabiltzeari buruzko Legea** [BOE 2007-06-23].

— **Komunikazio Elektronikoetako Datuak Kontserbatzeari buruzko Legea** [BOE 2007-10-19]

— **Informazioaren Gizartea bultzatzeko Neurrien Legea** [BOE 2007-12-29]

Norbaitek Interneten legez kanpoko irudiak aurkitu dituela uste badu, salatu egin dezake "*Europako Batzordearen Interneteko Segurtasun programa*" osatzen duen Interneteko Zuzeneko Lineen Nazioarteko Elkartearen [INHOPE] bidez.

↘ http://inhope.org/en/index.html

Iruzurren biktima izanez gero, edo legez kanpoko bestelako edozein aztarnaren aurrean, hauetara jo dezakegu:

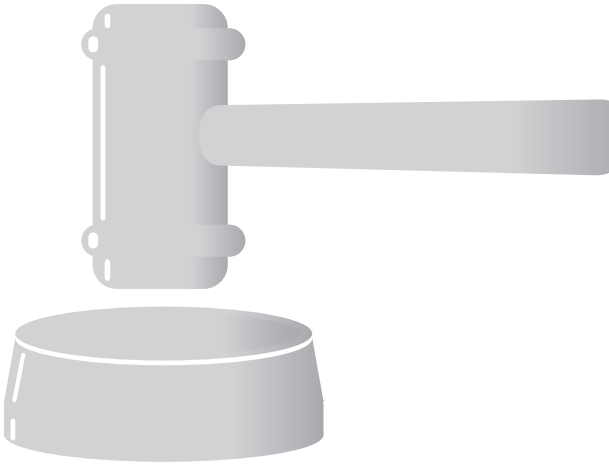
— **Ertzaintza**; "Informazioaren teknologietako delituen atal zentrala" (SCDTI) du eta webgunearen bidez jar zaitezke harremanetan www.ertzaintza.net ("on lineko zerbitzuak" erlaitza), edozein komisariatara joanda edo posta elektroniko bidez delitosinformaticos@ertzaintza.net.

— **Guardia Zibil**aren Unitate Eragile Zentraleko (UCO) Delitu Telematikoen Taldea (GDT) www.gdt.guardiacivil.es, gaiari buruzko informazio interesgarri ugari biltzen du eta salaketak egiteko inprimakia deskargatzeko aukera ematen du www.gdt.guardiacivil.es/denuncias.php.

— **Polizia Nacional**aren (CNP) Ikerketa Teknologikoko Taldearen (BIT) webgunean www.policia.es edo helbide elektroniko hauen bidez:

- **Iruzurrak telekomunikazioetan**: delitos.telecomunicaciones@policia.es
- **Haur pornografia**: denuncias.pornografia.infantil@policia.es
- **Interneteko iruzurrak**: fraudeInternet@policia.es
- **Birusak**, **erasoak**, **segurtasun logikoa**: seguridad.logica@policia.es
- **Pirateriaren aurka**: antipirateria@policia.es

Adingabeen eskubideen aurkako gai espezifikoetarako www.protegeles.com atariaren on lineko salaketa-sistema ere nabarmendu behar da.



Glosarioa

"BLOGA" edo BITAKORA: komunikazio-tresna oso berria da. Internauten eskura jartzen du webgunean edukiak modu librean sartzeko eta ezagutza partekatzeko aukera. Autoreek bidalitako testuak kronologikoki biltzen ditu; azkena bidalitakoa agertuko da lehenengo. Oro har, irakurleek oharrak idatz ditzakete, autoreek haiei erantzun eta, horrela, elkarrizketa sortu. Badira bereziki mugikorretarako eta blogak eguneratzeko eta kontsultatzeko WAP, SMS eta MMS sarbiderako diseinatutako mota horretako webguneak.

KRIPTOGRAFIA: informazioa zifratzea (kode moduan idaztea) eta deszifratzea ahalbidetzen duen teknologia; horrela, partekatutako mezuak zuzendutako pertsonek eta deszifratzeko bitartekoak dituztenek soilik irakur ditzakete.

IP HELBIDEA: Internetera konektatutako ordenagailu bakoitza identifikatzen duen zenbakia da. Beti zenbaki bera (IP finkoa) izan daiteke edo denborarekin automatikoki alda daiteke (IP dinamikoa). Etxeko ingurunean, IP dinamikoaren erabilera seguruagoa da.

FOROA: idatziz eta modu ordenatuan "elkarrizketa-lerroen" bidez gai bati buruzko parte-hartzaile guztien iritziak biltzea ahalbidetzen duen web-aplikazioa. Wikien kasuan ez bezala, ezin dira beste kideen ekarpenak aldatu, baimen bereziak izan ezean, moderatzaileei edo administratzaileei esleitutakoak kasu.

HARDWAREA: ordenagailuaren ikusizko zatia osatzen duten osagai elektriko, elektroniko, elektromekaniko eta mekanikoak. Automatizatutako lanerako gaitasun handia du, baina softwarea beharrezkoa du harekin elkarreragiteko.

IRC berriketa-zerbitzua edo "TXATA" (elkarrizketa denbora errealean)**:** bi pertsona edo gehiagoren arteko Internet bidezko ia aldibereko idatzizko komunikazioa; modu publikoan, txat publiko delakoen bidez (horien bidez edozein erabiltzaile sar daiteke elkarrizketan) edo txat pribatuen bidez egiten da. Hizketaldiak gai berdinei buruz interesatutako hainbat erabiltzailek bat egiten duten areto ekin eta kanalekin lotzen dira. Txatek zerbitzu bikaina eskaintzen dute, baina arriskutsuak izan daitezke adingabeek behar ez bezala erantzuten badute elkarrizketan. Parte-hartzaileen anonimatua bultzatzen dute identifikatzeko nickak sortuta (ezizena, goitizena).

"SAREA": Interneti buruz hitz egiterakoan, elkar konektatutako sareen multzoa dela esaten da batik bat. Sare horien bidez gaur egungo gizartean interes handikoak diren zerbitzu berezietara sar gaitezke: webguneetan nabigatu,

posta elektronikoko mezuak trukatu, denbora errealeko elkarrizketa pribatuak edo publikoak eduki eta abar.

BEREHALAKO MEZULARITZA: posta elektronikoaren antzeko on lineko komunikazio-metodoa. Hori, ordea, denbora errealean egiten da eta funtzio osagarriak eskaintzen ditu (ahozko elkarrizketak izatea eta irudiak ikustea ahalbidetzen du, esaterako). Arazorik gabe ahalbidetzen ditu taldeko elkarrizketak eta artxiboak trukatzea. Txataren oso antzekoa da, baina parte hartu ahal izateko beharrezkoa da nickaz gain, posta elektronikoa jartzea.

↘ Yahoo! messenger, Windows live messenger, Google talk

WEB NABIGATZAILEA: webguneko informazioa ikusteko aukera ematen duen softwarea. Internetekin elkarreragiteko modurik arruntena eta erabiliena da. Nabigatzaileak webgunea idatzita dagoen kodea interpretatu eta pantailan erakusten du; jarraian, erabiltzaileari edukiarekin elkarreragitea eta Sareko beste leku batzuetara nabigatzea ahalbidetzen dio, esteken edo hiperesteken bidez.

"PEER TO PEER" (P2P): informazioa zuzenean trukatzea eta edozein formatuko edukiak partekatzea ahalbidetzen duten eta elkarren artean (bitartekorik gabe) konektatuta dauden ordenagailuez osatutako sareak. "Kidekoen arteko" sareen interes nagusia materiala bi noranzkoetan trukatzeko aukera ematea da; fitxategiak deskargatzen diren heinean, gainerako sarearen eskura jartzen dira aurretik deskargatutako fitxategiaren zatiak.

"PODCASTING": aldez aurretik izena emanda fitxategiak deskargatzeko (nahi denean entzuteko edo ikusteko) aukera ematen duen edukiak zabaltzeko sistemaren bidezko audio- edo bideo-edukien banaketa (irrati-programak, elkarrizketak, hitzaldiak eta abar). Apple Computer-en iTunes software famatuan, esaterako, ordenagailura deskargatu ahal izateko audio-formatuko informazio-ildo ugaritarako sarrera eskaintzen da.

SARE SOZIALA: lagunekin harremanetan jartzeko eta lagun berriak egiteko aukera eskaintzen duen web-aplikazioa.

SISTEMA ERAGILEA: ordenagailuaren (hardwarearen) eta erabiltzailearen artean lotura egiteko diseinatutako softwarea. Ordenagailua piztean automatikoki kargatzen den lehen programa informatikoa.

SOFTWAREA: makinarekin (sistema eragilearekin) ulertzea eta zeregin es-

pezifikoak (testua idaztea, filma ikustea, birus kaltegarrien sarrera ekiditea eta abar) egitea ahalbidetzen duen programa multzoa (aplikazio informatikoak).

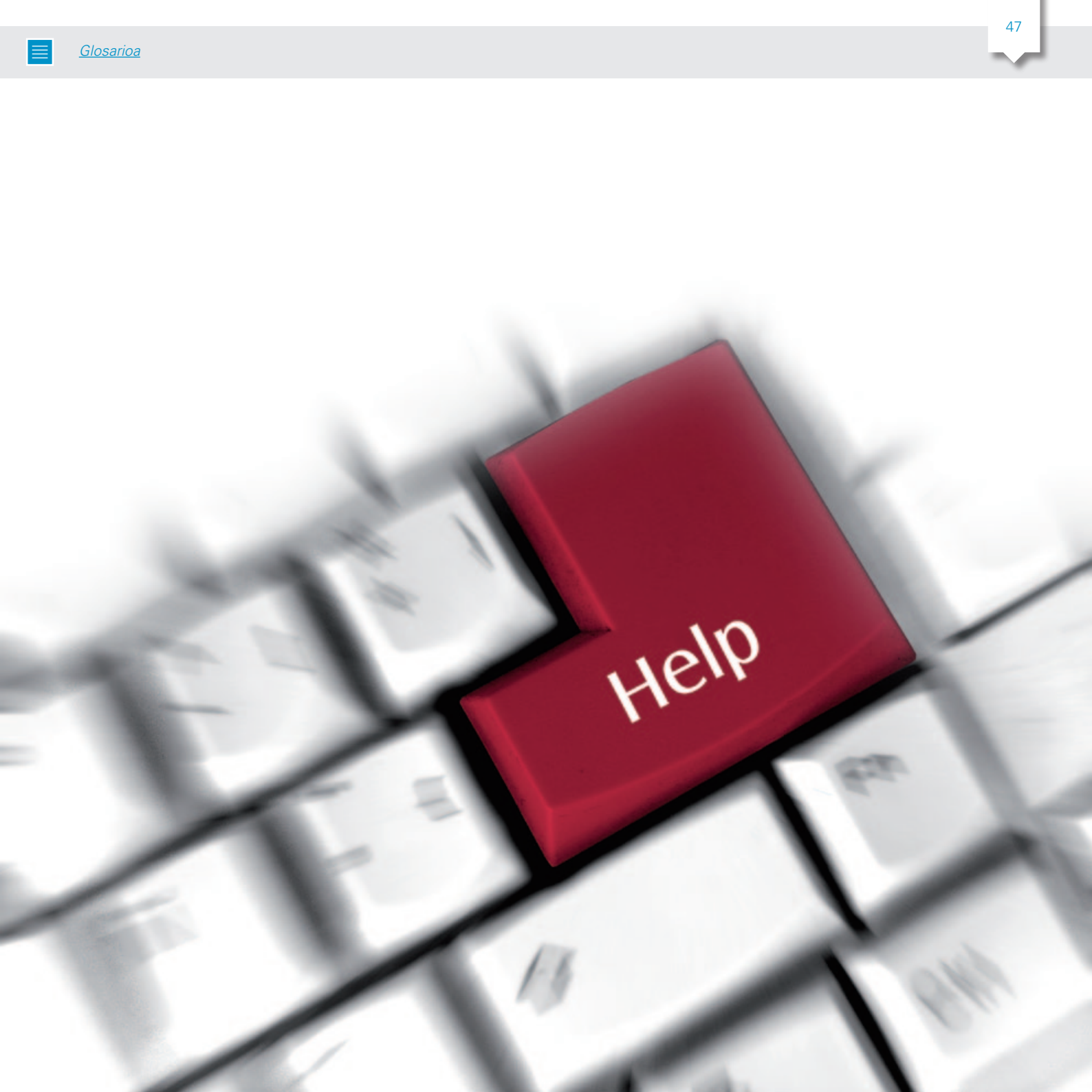
IP GAINEKO TELEFONIA: telefoniaren funtzio berriak; horien artean "ahotsa Internet bidez" transmititzeko (VoIP) aukera nabarmentzen da. Sistema horren bidez, ahotsa sarean transmiti daitekeen datu-pakete bihurtzen da; hala nola bideo-fitxategiak, testu-dokumentuak edo argazkiak. Horren (Jingle edo Skype) arrakastaren arrazoia Konmutatutako Telefono Sare Publiko tradizionalak sortzen duen gastua (batez ere, distantzia luzekoa) saihestea da. Telefonia tradizionalarekin alderatuta, abantailak handiak dira: askoz ere merkeagoa da (doakoa tarifa finkoa izanez gero) eta erabiltzailearen kokapen fisikoa kontuan izan gabe telefono-deiak egitea ahalbidetzen du. Telekomunikazioen Merkatuko Batzordeak telefonia tradizionaletik bereizi du; beraz, telefono-zerbitzuari buruzko arauek ez diote eragiten.

BIDEOKONFERENTZIA: elkarren artean urrun kokatutako pertsona taldeen artean bilerak egitea ahalbidetzen duen bi noranzkoko aldiuneko audio- eta bideo -komunikazioa. Informazio grafikoak edo irudi finkoak trukatzeko eta fitxategiak transmititzeko zerbitzuak ere eskain ditzakete. Audio- eta bideofluxuak denbora errealean modu digitalean konprimitzeko aukera teknikoan oinarritzen dira.

2.0 WEBGUNEA (web soziala)**:** Interneteko komunikazioaren bilakaera teknologikoa. Funtsean webgunearekin zuzenean elkarreragiteko aukeran oinarritzen da; hau da, noranzko bakarreko sistema estatikoa izatetik bi noranzkoetan trukatzea ahalbidetzen duen sistema izatera pasatzen da (edukia irakurtzen dut, baina sortu ere egiten dut). Sare sozialak, blogak eta wikiak komunikazioaren filosofia berri horren zati dira.

↘ Flickr, Gmail, Delicious, Wikipedia, Plaxo, Googledocs, Wikispaces, Doodle

"WIKIA": web-nabigatzailea soilik erabilita hainbat boluntariok aldi berean editatu ditzaketen webguneak. Parte-hartzaileek partekatzen duten testua sortu, aldatu edo ezabatu egin dezakete.


Help

Informazio iturriak: webgune interesgarriak

Interes handiko informazio-iturritzat jotzen dira:

- Komunikazioaren Teknologietako Institutu Nazioala
  www.inteco.es
- Euskadi Informazioaren Gizartean
  www.euskadi.net/eeuskadi/new/eu/index.html
- Ziberfamiliak (Gurasoak eta hezitzaileak biltzeko lekua)
  www.ciberfamilias.com/index.htm
- Pantaila lagunak
  www.pantallasamigas.net
- Gazteak. Hau da gure Webgunea
  www.chaval.es
- Interneteko Erabiltzaileen Elkartea
  www.aui.es
- Gazteriaren Erakundea
  www.injuve.migualdad.es/injuve/portal.portal.action
- EDEX
  www.edex.es
- Internautaren Segurtasunerako Bulegoa
  www.osi.es/Internautaren_segurtasun
- WIREDSAFETY (ingelesez)
  www.wiredsafety.org
- Datuak Babesteko Espainiako Agentzia
  www.agpd.es/portalweb/index-ides-idphp.php
- Arartekoa. Herriaren defendatzailea
  www.ararteko.net
- Madrilgo Komunitateko Adingabeen Defentsaria
  www.defensordelmenor.org
- Andaluziako Komunitateko Adingabeen Defentsaria
  www.defensordelmenor-and.es
- Administrazio Elektronikoaren Kontseilu Gorena
  www.csae.map.es

- Internauten elkartea
  www.seguridadenlared.org/menores
- Telekomunikazioetako erabiltzaileen arretarako bulegoa
  www.usuariosteleco.es
- Interneteko Kalitate Agentzia (IQUA)
  www.Internetsegura.net.
- Guraso Internauten Elkarte Espainiarra (AEMI)
  www.aempi.com
- Mc Afee segurtasun alerten zentroa
  http://home.mcafee.com/advicecenter/default.aspx
- Panda Security-Ko Segurtasunari buruzko informazioa
  www.pandasecurity.com/spain/homeusers/security-info
- Bitdefender Babes zentroa
  www.bitdefender.es/site/virusinfo
- PROTÉGELES
  www.protegeles.com
- Haur Pornografiaren Aurkako Ekintza Elkartea
  www.asociacion-acpi.org
- Moneta eta Tinbreen Fabrika Nazionaleko CERES Proiektua
  www.cert.fnmt.es
- Interneteko Kalitate Agentziaren Internet Segurua (IQUA)
  www.iqua.net
- Telebistako Edukiak eta Haurtzaroa Autoerregulatzeko Kodea
  www.tvinfancia.es/default.htm
- UNICEF
  www.unicef.org/spanish
- Jolasak
  www.secukid.es
  www.navegacionsegura.es/home/triviral.html

Ikaskuntzako hainbat leku

KZguneak

KZgunea Internetera sartzeko eta prestakuntzako doako zentroen sarea da. Eusko Jaurlaritzak Vitoria-Gasteizko Udalarekin lankidetzan jarri zuen abian.

KZguneetan hauek topatuko dituzu:

— Interneti eta administrazio elektronikoari buruzko **oinarrizko ikaskuntza-ikastaroak**.

— Interneten erabilera praktikorako **gaikako ikastaroak eta mintegi aurreratuak** (on lineko bankua, bidaiak, erosketak, segurtasuna, familia, posta elektronikoa...).

— **Mikroenpresei zuzendutako ikastaroak**, eguneroko kudeaketa IKTen erabilerara egokitu dezaten.

— Teknologia berrien oinarrizko gaitasunetako **ziurtagiria eskuratzeko** azterketak (IT Txartela).

KZguneak **gizarte-etxe** hauetan daude: Aldabe, Arriaga, El Pilar, Hegoalde, Ibaiondo, Iparralde eta Lakua.

Informazio gehiago nahi izanez gero, kontsultatu webgunea: www.kzgunea.net

Saregune

Gasteizko Alde Zaharrean dagoen zentroa da eta Eusko Jaurlaritzak eta Vitoria-Gasteizko Udalak batera finantzatu dute. Bertan ordenagailuak doan erabili daitezke **nabigatzeko** eta **posta begiratzeko**. Horrez gain, herritarrei mota guztietako aplikazio informatikoak erabiltzen irakasteko **ikastaroak** eskaintzen dituzte. 2.0 webgunearekin zerikusia duen guztian espezializatuta daude. Arduradunen taldeak hainbat hizkuntza hitz egiten du eta erabat interkulturala da. Zentroaren egitekoa auzoko herritarrei (hirian behartsuenetakoak) teknologia berriek eskaintzen dituzten aukerak ulertaraztea da.

Santa Maria kantoia 4, behean kokatuta dago eta hau da helbide elektronikoa: www.saregune.net

Internet Zuretzat

Herritarren alfabetizazio digitala sustatze aldera, Internet Zuretzat ekimenak (Eusko Jaurlaritzaren Hezkuntza, Unibertsitate eta Ikerketa Sailaren mendekoa) ikastetxeetako **ikasleen senideei zuzendutako trebakuntza-ekintzak** jartzen ditu abian. Ikastaro horiek ikastetxean bertan eskaintzen dituzte adituek. Edozein kontsulta egiteko orrialde honetara sartu: www.internetzuretzat.net. Edo 945 01 61 49 telefonora deitu. Informazio gehiago hemen: formatec@kzgunea.net

Prestakuntza-ikastaroak

Vitoria-Gasteizko Udalaren Sustapen Ekonomikoko eta Planifikazio Estrategikoko Sailak antolatutako trebakuntza-ekintzak dira. Ekintza horiek lan-merkatuan txertatzeko aukerak hobetzeko, laneko profila aldatzeko edo haien jarduerarekin lotutako gaietan ezagutzak zabaltzeko interesa duten langileei zein langabezian daudenei zuzenduta daude. Bi ikastaro mota eskaintzen dira: presentziazkoak eta e-learning ikastaroak (urrunekoak). Informazio gehiago nahi izanez gero, kontsultatu webgune hau: www.vitoria-gasteiz.org/formacion

Informatikaren hastapenerako ikastaroak. Montehermoso

Montehermoso Kulturuneak taldeentzako, elkarteentzako eta kolektiboentzako **informatika arloko hastapenerako ikastaroak** eskaintzen ditu. Informatika eta komunikazioaren teknologiak baliabidetzat erabilita, ikasleei egokitutako programak prestatu ohi dituzte, gehien interesa dakizkiekeen gaiak azpimarratuta: Internet, segurtasuna sarean, ordenagailuaren erabileraren hastapenak, edukien bilaketa.... Helburua informazioaren teknologiak herritarrei hurbiltzea da, horretarako, ezagutzak behar errealetara egokituta. Taldeak mugatuak dira (gehienez 12 pertsona) eta ikastaroen iraupena taldeko arduradunak planteatutako helburuei jarraiki finkatzen da. Informazio gehiago 945 16 18 59 telefono-zenbakira deituta edo www.montehermoso.net webgunean.

Bibliografia

- AFTAB, P. *"Internet con los menores riesgos"*. ISBN: 84-9726-310-3. Edex. 2005
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *"Guía de seguridad de datos"*. NIPO: 052-08-003-6. 2008
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Recomendaciones a usuarios de internet"*. NIPO: 052-08-007-8. 2009.
- FARRAY, JI. *"Cultura y educación en la sociedad de la información"*. ISBN: 84-9745-027-2. Netbiblo. 2002
- ALMUZARA, C. *"Estudio práctico sobre la protección de datos de carácter personal"*. ISBN: 84-8406-582-0. Editorial Lex Nova. 1ª ed. 2005
- ASENSIO, G. *"Seguridad en internet"*. ISBN : 84-9763-293-1. Nowtilus ed. 2006
- GARCÍA SANZ, RM. *"El derecho de autor en internet"*. ISBN: 84-7879-939-7. Colex. ed constitución y leyes. 1ª ed. Madrid. 2005
- GRALLA, P. *"Cómo funciona internet"*. Anaya multimedia. Madrid. 1º ed. 2007
- OCDE - MAP. *"Directrices de la para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad*. NIPO: 326-04-035-2. 2004
- INTECO (INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN). *"Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres"*. Marzo 2009.
- JOYANES, L. *"Las redes sociales: de la mensajería instantánea a los weblogs"*. Sociedad y utopía: Revista de Ciencias Sociales, 24: 93-122 (2004)
- PROTÉGELES (CANOVAS, G). *"Cibercentros y seguridad infantil en internet"*. Noviembre 2002.
- PROTÉGELES (CANOVAS, G). *"Seguridad infantil y costumbres de los menores en el empleo de la telefonía móvil"*. Mayo 2005.
- PROTÉGELES (CANOVAS, G). *"Seguridad infantil y costumbres de los menores en internet"*. Noviembre 2002.
- PROTÉGELES (CANOVAS, G). *"Videojuegos, menores y responsabilidad de los padres"*. Diciembre 2005.
- WEBSENSE SECURITY LABS. *"State of internet security Q1-Q2"*. 2009