

ADIN TXIKIKOAK SAREAN

HAUR jolasa ote?



PANDA
SECURITY

One step ahead.



2007an malwarea (birusak, spywarea eta beste hainbat kode maltzur) zazpi bider handitu zen aurreko urtearekiko. Horretaz gain, ziber-gaizkileek bide berriak urratu dituzte erabiltzaileak kutsatu eta euren isilpeko datuak lortzeko, berehalako mezularitza (MSN Messenger, Yahoo! Messenger etab.), fitxategien elkartruckerako programa (eMule edo Kazaa) edo blogen bidez.

Bestela esanda, arriskua Interneten handituz doa, eta adin txikikoak, eskarmentu eta prestakuntza eza direla eta, babesgabe eta zaurgarrienak dira.

Jarraian, Internetek haurrentzat gordetzen dituen arriskuak aztertuko ditugu, eta hauei aurrea hartzeko hainbat aholku azalduko ditugu. Hauetariko asko gurasoei zuzenduak daude, euren ardura baita txikienek Internet nola erabiltzen duten gainbegiratzea, teknologia berrien erabilera arduratsua eta segurua egin dezaten irakatsiz.

Datu esanguratsuak: Adin txikikoak Interneten



Espanian 10 eta 14 urte bitarteko neska-mutiletatik 7tik 10ek Internet erabiltzen dute. Internet haurren egunerokotasunean lekua hartu du. Horregatik, bai eurek nola euren gurasoek Interneten zelatan dabiltzan arriskuak ezagutu behar dituzte.

2004an Kleiner and Lewisek argitaratutako ikerketa baten arabera, 6 eta 10 urte bitarteko haurren %90ak Internet erabiltzen du maiztasunez Amerikar Estatu Batuetan. 2006an American Psychological Association (APA) elkarteak ikertutakoaren arabera, AEBko gazteen %75 eta %90 bitarteko kopuruak Internet erabiltzen du, txatetara sarbidea du edo berehalako mezularitzan jarduten da sarritan.

Europar Batasunean datuak ez dira oso bestelakoak. Eurobarometroak dio gazteen %64ak Internet erabiltzen duela Danimarka, Herbehereak eta Erresuma Batuan; Suedian %63ak, Finlandian %62ak eta Estonian %60ak. Batasuneko gainerako herrietan antzerako ratioak daude, Grezia (%15a), Zipre (%20), Eslovakia (%30a) eta Portugal (%31) salbu.

Espanian 10 eta 14 urte bitarteko neska-mutiletatik 7tik 10ek *Internet erabiltzen dute*. Katalunian kopurua handitzen da %88,5eraino.

Hau da, Internet haurren egunerokotasunean lekua hartu du. Ordu andana ematen dute konektaturik, bai eskolan nola euren etxeetan. Horregatik, bai eurek nola euren gurasoek Interneten zelatan dabiltzan arriskuak ezagutu behar dituzte.



Arrisku nagusiak

Haurrek gurasoen zaintzarik gabe Internet erabiltzen dutenean, izaera antzeko mehatxuen helburu izan daitezke, arrisku horietariko askok ondorio larriak ekar ditzaketelarik.

Azter dezagun gazteek zein eratan erabiltzen duten Internet eta horri lotzen zaizkion kalteak.

Berehalako mezularitza:

Berehalako mezularitza (MSN Messenger, Yahoo! Messenger, Google Talk, etab. bide direlarik) gazteen arteko komunikazio tresna nagusienetarikoa da. Erabilera zabaldu honek ez ditu ziber-gaizkileak epel uzten, eta tresna hauek euren ekintzetarako bitarteko lehendar bihurtu dute.

Arriskueta bat nortasunaren ordezkapenarena da, hau da, pertsona batek beste bat bailitzan bere burua aurkeztea. Programa hauetan identifikazioa posta helbide baten bidez, eta honi esleitutako pasahitz baten bidez ematen da. Horrela, norbaitek gure zerrendako kontakturen baten kontura sarbidea lortuko balu, ez legoke inolako arrastorik ordezkapen horren berri emango ligukeenik, beraz gure solaskidea uste dugun hori ez dela oharkabean pasako zaigu. Kontaktu horrekin partekatutako fitxategiak baditugu, erasotzaileak sarbide osoa izango du horietara. Horregatik da garrantzitsua isilpeko informaziorik ez ematea (datu pertsonalak, helbide fisikoa, identifikazio edo banketxe kodeak, pasahitzak, etab.) berehalako mezularitza gisako medio ez ziurren bidez.

Nortasunaren ordezkapenak dakartzan arriskueta beste bat -are larriagoa eta gizartea gutiz asaldatzen duena- pederastia da. Pedofiloek bide hauek erabiltzen dituztela agerian utzi duten hainbat kasuk oihartzuna izan dute hedabideetan, horien artean neskato asturiar batena, berekin harremanetan Messenger bidez jarritako pedofilo batek hertsatua izan zena, eta azken hiletan gertatutako beste hainbeste eredu. Erasotzaileek, behin adin txikikoen konfiantza bereganatuta, aurrez aurreko hitzorduak ezartzen edo eduki mineko argazkiak lortzen saiatzen dira. Gertutasun hori lortzeko pederastek euren burua gazte moduan edota euren argazkien bilduma egitean interesa duten puntako argazkilariak bailiran aurkezten dute, beste hainbat trikimailuren artean.

Arrisku horiengandik babesteko -bizitza errealean bezalaxe- ezezagunekin hitz egitea arriskutsua dela irakatsi behar zaie haurrei, eta behar besteko konfiantza helarazi, zalantza edo izuen aurrean guraso edo helduengana jo dezaten.

Birus eta kode maltzurren kutsadura beste arazo bat izan daiteke berehalako mezularitzari lotua. Urtearen lehen seihilabetekoan PandaLabs-ek hautemandako harren %58,6k baino gehiago (euren kabuz zabaltzeko gai diren kode maltzurak) erreminta horien bidez barreiatzeko diseinatuak izan ziren. Haietariko batzuk sareko banketxeetako pasahitzak kopiatzeko eginak ziren. Infekzio kasuetan beraz, arriskua ez da ematen soilik adin txikikoetan, baizik eta hauen gurasoengan ere, zerbitzu hauen behar ez bezalako erabilerak gurasoen hitz gakoan lapurreta, eta diruarena halaber, ekar baitezake.

Berehalako mezularitza bidez barreiatzen diren kode maltzurrei aurrea hartzeko honako aholkuak izan behar dira kontuan: bide



Berehalako mezularitzan identifikazioa posta helbide baten bidez, eta honi esleitutako pasahitz baten bidez ematen da. Horrela, norbaitek gure zerrendako kontakturen baten kontura sarbidea lortuko balu, ez legoke inolako arrastorik ordezkapen horren berri emango ligukeenik.



Berehalako mezularitza bidez barreiatzen diren kode maltzurri aurrea hartzeko honako aholkuak izan behar dira kontuan: bide honetatik heltzen zaigun fitxategirik ez zabaldu eta estekarik ez sakatu, behintzat, igorleak berak bidalia dela ziurtatu aurretik.

honetatik heltzen zaigun fitxategirik ez zabaldu eta estekarik ez sakatu, behintzat, igorleak berak bidalia dela ziurtatu aurretik.

Posta elektronikoaren erabilera hain arrunta eta ohikoa izanik hainbat dira sor ditzakeen arriskuak.

- Lehenik spama. Maiz iristen dira helbide elektronikoetara sareko joko-etxe edota sendagaien iragarkiak. Egoera horretan haurren eskarmentu gabezia dela eta, bertan datorren informazioa egiazkotzat jo dezakete, euren burua kaltetuz. Horrela, sareko joko-etxeetan dirua gal dezakete, jokorako menpekotasuna garatu edo jatorri zalantzarikoko botika zein drogak lortu, aizunduta badaude osasun kalte larriak eragin ditzakeena.
- Bigarren, lan eskaintza faltsuak ditugu. Nerabeekin txikienekin baino arazo larriagoa izan daiteke hau. Primerako lan eskaintzen berri ematen duten postak izan ohi dira. Erabiltzaileak diru mordo egin dezake trukean esfortzurik egin gabe. Kontu zenbaki bat eman beharko du, bertan diru kopuru jakin bat sartuko zaio ondoren beste kontu batera desbideratzeko, artesari baten truke. Horren erraza izanik, heldu orok hartuko luke eskaintza hori mesfidantzaz. Aurkan, dirua erraz gura duen gazte batek amua erraz irents dezake. Horrek delitu baten gaizkide izatea ekarriko dio, eragiketa horien helburua azpi-jardueretatik datorren dirua zuritzea izan ohi da eta.
- Hirugarren arriskua ordenagailua birus edo malware bidez kutsatzearena da. Gai erakargarriak amu moduan erabiliz (filmen trailerrak, pertsonaia ospetsuen irudi erotikokoak, sare bidezko jokoaren deskargak) erabiltzaileak esteka bat saka dezan edo fitxategi kutsakor bat saretik jaitsi edo exekutatu dezan saiatzean du oinarri, ondorioz sistema infektatuz. Gizarte ingeniariak izenaz ezagutzen da hau. Iruzurrean jausten diren helduak ugariak dira, beraz, are errazagoa izango da haurrak harrapatzea.

Arrisku hauek uxatzeko biderik onena, **haurrei jatorri ezezaguneko e-mailak zalantzan jarri behar dituztela irakastea da**. Barneratu behar dute bertan azaltzen dena sasi-egia izan daitekeela eta proposatutako esteka eta fitxategiak errefusatu behar dituztela.



Fitxategien elkartruckerako sareen arriskuak (Emule, Kazaa etab.)

Erabiltzaileen artean fitxategiak trukatzeko programak, Kazaa edo eMule kasurako, ordenagailuak kutsatzearen eragileetako bat dira halaber. Filmak edo programak izen erakargarriak mozorroturik ezkutatu ohi dira birus eta kode maltzurak –har bezala izendatuak direnak orokorrean- erabiltzaileen jakin-nahia piztu eta deskargatuak eta zabalduak izatera bultzatuz.

Arriskua gizarte ingeniartzaren antzekoa da –jarrera hori aurrekoaren aldaera litzateke- izen erakargarria amu moduan erabilia izan ohi da haurrek, nahigabea, ordenagailuan fitxategi maltzurra sartzeko.

Haurrek jakin behar dute sare hauetariko zein fitxategi deskargatu eta zein ez. Horrez gain **fitxategi horiek segurtasunerako euskarrien bidez aztertzea** ongi legoke lehen aldiz zabalduak izan baino lehen. Fitxategia exekutatzearan errorea adierazten duen mezua agertzen bazaigu non kodeka edo lizentziaren bat eskatzen den, zalantzarako arrazoiak izan daitezke, birusen bat barne duela adierazten baitu.

Sare sozialak eta blogak

MySpace edo Facebook bezalako sare sozialak argazkiak eta bideoak tartekatuzko, lagun berriak egiteko, txateatzeko eta abarrerako erabiltzen dira eta blog edo bitakorekin batera -maiz sareko eguneroko moduan erabiltzen direnak-, gazteek gehien ikuskatzen dituzten web guneen artean daude sailkatuta. Hauek erabiltzeko betekizuna profil bat sortzearena da, non izena edo adina besteren artean, agertuko diren.

Haurrei gogorarazi behar zaie orokorrean helbide elektronikoa eta ezizenarekin nahikoa izan ohi dela. Gazteek kontuan izan behar dute euren burua adin txiki moduan ezagutzera emango duen daturik ez argitaratzea, hala nola, euren bizileku edo ikas lekuaren berri ez emateko. Honenbestez, hobe da benetako izenik ez erakustea Interneten, ezizen edo "nick" a erabiltzea baizik.

Gainera, MySpace bezalako sare sozialetan fitxategiak parteka daitezke beste erabiltzaileekin. Arreta berezia izan behar dute haurrek fitxategi horietatik zeintzuk eta noekin tartekatzen dituzten. Ez dago arazorik argazkiak ipintzearekin, beti ere gako hitz baten bidez hauek elkartrukatzea lagun eta senitartekoetara mugatzen bada.

Gurasoek zerbitzu berri horien berri izan behar dute, hauen funtzionamendua eta arriskuak ezagutu behar dituzte eta euren seme-alabei horiek erabiltzeko bide ziurrena irakatsi.

Filmak edo programak izen erakargarriak mozorroturik ezkutatu ohi dira birus eta kode maltzurak erabiltzaileen jakin-nahia piztu eta deskargatuak eta zabalduak izatera bultzatuz.



Bluetooth bezalako funtzioekin edota Interneterako konexio bizkorragoen bidez, gailu hauek are zaugarriago egiten ditu.

Internetera sarbidea duten sakelako telefonoak: arrisku iturri berria

Frost & Sullivan etxeko ikerketa baten arabera, mugikorren berritze gorakorra dela eta, ziber-gaizkileek euren jardunerako esparru lehenetasunezkotzat izango dute hau datozen urteetan. Bluetooth bezalako funtzioekin –ari gabeko konexioak bideratzen dituen telefonoen artean, fitxategiak elkartrukatzea ahalbidetuz- edota Interneterako konexio bizkorragoen bidez, gailu hauek are zaugarriago egiten ditu.

Sakelako telefonoa egungo haur eta gazteentzat osagarri nagusienetakoa da. Ordenagailuetarako aipatu ditugun mehatxu bertsuak topatzen ditugu hauetan ere.

Ez da gauza berria berehalako mezularitza telefono mugikorretan. Gaztetxoek edonon txatea dezakete honakoen aurrean babesgabe egonik: nortasun iruzurra, komeni ez zaizkien pertsona eta egoerekin topo egiteak, sistemaren kutsatzea etab.

Bolo-bolo dabil spama mugikorretan ere. Mezu laburrak direla bide iritsi ohi da publizitatea, maiz pornografiarekin zerikusia izaten duena. Hau da, honek ez du haurren mugikorretan leku bat besterik hartzen, haurra jarraitzen du doan lekura doala.

Gurasoek euren seme-alabek sakelako telefonoa nola erabiltzen duten ere ikuskatu behar dute. Haur txikien kasuan arrisku iturri izan daitezkeen funtzioak ez dituzten tresnak topa ditzakegu, gazteen kasuan ordea, gailuen ganorazko erabilera gomendatu behar zaie, eta azpimarratu jatorri susmagarriko mezuei muzin egitea eta ezezagunekin aurrez aurreko hitzordurik ez burutzea.



Infektatua izatearen arriskua

Aurreko paragrafoetan ikusi dugu zein eratan izan daitezkeen erabiltzailerik gazteenak kutsatuak, baita hauen gurasoen ordenagailuak ere (mezularitza edo posta bidez heldutako estekak, infektatutako fitxategien deskarga...). Ordenagailuan kode maltzurra harat-honat izateak sor ditzakeen arriskuak ugariak eta anitzak izan daitezke.

Lehenik, aurrez aipatu dugun eran, hurrek gurasoen ordenagailu bera erabiltzen badute, behar ez bezalako erabilerak ordenagailua infektatzea ekar dezake, banketxeko kodeak ostuak izan daitezke helduek euren saioa hastean.

Arriskua ez da soilik gurasoen kalterakoa, hurrek eurek ere kalteak jasan ditzakete. Esaterako, adwarea instala dakieke. Kode maltzur hauek iragarkiak sar ditzakete erabileraren arunetan ari garenean banner edo bat-batean azaltzen diren leiho moduan. Helduentzat hauek enbarazua baino ez izatea eman daiteke –nahiz eta kontuan izan behar den horiekin, batzuek troiakoak sar ditzaketela sisteman-baina hurren kasuan are larriagoa izan daiteke horietako hainbat iragarkik eduki pornografikoa izan baitezakete barnean.



Hurrek gurasoen ordenagailu bera erabiltzen badute, behar ez bezalako erabilerak ordenagailua infektatzea ekar dezake.



Gurasoei aholkuak

- 1 Hitz egin ezazu zeure haurrekin:** Lehen urratsa da haurren babesean. Zein gune arakutzen dituzten, norekin dauden harremanetan edota zer duten gustuko jakitea komeni da, etxetik irteten direnean horren guztiaren berri izan nahi duzun bezalaxe. Internet erabiltzean ongi zein txarto ari diren ikuskatu behar da.
- 2 Informazioa eskuratu eta zeure haurrei aholkua eskaini iezaiezu:** Guraso askori ezezaguna zaie Internet. Badago informazioa bilatzeko, berriak irakurtzeko edo musika, filmak eta bestelakoak jaisteko erabiltzen duenik. Baina orokorrean seme-alabek erabiltzen dituzten zerbitzuak ezagun zaizkie. Horretarako urrats handia litzateke sareak haurrei eskaintzen dizkien erremintak eta hauen arriskuak, nola ekiditeko erak ezagutzea. Behin hori gaindituta haurrei aholkua emateko gai izango gara, gustukoen duten hori lan dezaten.
- 3 Internet erabiltzeko arau zurrunik ezarri:** Ordutegia, konexioen iraupena eta erabilera mota zehazteko oinarriak ezarri behar dira. Hauek betetzen direla ziurtatu behar duzu, batez ere gauzez egiten den erabilerari dagokionean. Kontuan izateko beste eragile bat bada ordenagailua etxeko zein gunetan kokatzen dugun: senitarteko guztiek ordenagailu bakarra erabiltzen badute, hobe da areto amankomunak aukeratzea, txikienaren logela baztertuz.
- 4 Galarazi ezazu adin txikikoez isilpeko informazioa zabaltzea:** Haurrei irakatsi behar zaie ezin dituztela euren izena, helbidea edota argazkiak sarean zehar barreiatu. Erakutsiezu ezizen eta pasahitz zuhurrak erabiltzen (zenbaki, hizki larri eta minuskulak tartekatzen dituztenak, kasurako) ziber-gaizkile edo erabiltzaile makurrek euren posta edo mezularitza kontuetara sarbidea izan ez dezaten.
- 5 Azaletik ez epaitzen irakatsiezu:** maiz, Interneten, urrutiko intxaurrak, gerturatzean lau: Ez da gauza berria kodea maltzurak itxuraldatzea filmen aurrerakinak bailiran, edo pederastek hamaika trikimailu bide haurrekin harremanetan jartzea. Beraz, sarean, dirudiena maiz ez da benetan dena. Haurrei irakatsi behar zaie mesfidantzaz jokatzeko eta euren segurtasun eta barrukotasuna babesean mantentzen.
- 6 Segurtasun bitarteko eraginkorrak instala itzazu:** Eguneratutako segurtasun erremintek berebiziko garrantzia dute kode maltzurretatik babesteko. Pandaren etxerako segurtasun baliabideek malwarea ezabatzeaz gain, zeure ordenagailua birus ezagun zein ezezagunez babestu, ordenagailua egindako baimen gabeko sarbideak ekidindo dituzu, sistema kutsa dezaketen orrialdeak eta zabor posta (spama) errefusatuak izango dira eta Panda Internet Securityren edukien iragazketari esker zeure seme-alabek zein orrialde ikuskatuko dituzten aukeratu ahal izango duzu.



Adin txikikoentzat informazioa:

- 1 Estekei muzin egiezu:** Berehalako mezularitza sistema baten bitartez hizketan ari zarenean edota postaz mezu bat jasotzen duzunean ez itzazu sekula estekak sakatu. Ezagutzen duzun erabiltzaile batean badago horren jatorria, estekan azaltzen den helbidea sar ezazu nabigatzailearen barran. Iturri ezezagun batetik badator, hobe da muzin egitea, orrialde maltzur batera bideratzeko arriskua baitago zure ordenagailua kutsatuz.
- 2 Jatorri ezezaguneko fitxategiak ez dira jaitsi ezta exekutatu behar:** Sarritan jasoko zenituen berehalako mezularitza bidez argazki, abesti edo bideoak jaisteko gonbidapenak. Zenbaitetan fitxategi horiek ez dira pertsona ezagunek bidalitakoak, nahiz eta zeure ezagunen zerrendako kide batek bidalia izan. Programa maltzurrek bidalitako mezuak izan ohi dira, konfiantzazko pertsona hori kutsatu duena eta ahalik eta erabiltzaile gehienen artean barreiatzeko saiakeran ari dena. Ezezkoan badago, azal iezaiozu kutsatua dagoela, fitxategia ezabatu behar duela eta bere "nick" edo ezizena alda dezala ezagun guztiei horren berri emateko, hauek ere infekta ez daitezen.
- 3 Ez da ezezagunekin hitz egin behar:** Ez dugu ziurtasun betea izaterik, txatetan edo berehalako mezularitza zerbitzuetan ariaren beste aldean nor dagoen. Are gutxiago sareko elkarteetan, non bertako kideek ez duten alde aurreko inolako harremanik. Horregatik bazter itzazu ezezagunak, are gehiago hauekin aurrez aurre topatzea.
- 4 Beti gorde behar da isilpeko informazioa sarean:** Jakingai pertsonalak, helbideak etab. Ez dira sekula postaz, berehalako mezularitza bidez ezta blog edo foruen bidez argitaratu behar. Gainera, arreta handia ipini behar da FaceBook edo Myspace moduko zerbitzuetan zeure profilaren berri ematen duzunean. Bertan ez da azalduko ez helbiderik ezta adinik ere. Beti ere ezizen edo "nick" bat erabili ezazu.
- 5 Zalantza txikienaren aurrean ere ez zaitetz fida:** Baliteke aurrez instalatu duzula oroitzen ez duzun programaren batek gezurrezko infekzioen berri ematea eta pop-up erako mezu edo leihoetan antibirusa erosteko eskaintzak egitea. Ziurrenik zure ordenagailuan nolabaiteko malwarea instalatua egongo da.
- 6 Ez itzazu fitxategi susmagarriak exekutatu:** Segurtasunerako erabiltzen duzun baliabideak fitxategi baten zalantzaragarratasuna jakinarazten badizu, ez ezazu zabaldu. Ezaba ezazu.
- 7 Nagusiekin hitz egin ezazu:** Gai jakin baten inguruan zalantzak badituzu, zerbait susmagarria jaso baduzu, mezu mehatxagarri, mingarri edo arriskutsuk jaso badituzu, emaitza horren barri nagusiren bati. Hark lagunduko zaitu.



Irakasle eta hezitzaileentzat aholkuak

Irakasleek ere berebiziko garrantzia dute haurrek Teknologia Berrien ganorazko erabileraren ikaste prozesuan, are gehiago ordenagailuek ikasgeletan esparrua finkatuz doazen testuinguruan. Hori dela eta honako jarraibideak kontuan izan behar dira:

- 1 Informa zaitetz:** Sarearekin lotutako arriskuak aztertu. Horiek identifikatu eta ekar ditzaketen ondorioak gazteei zein eratan helarazi.
- 2 Informatika segurtasunaren inguruko heziketa plana ezarri:** Informatika ezagutu eta erabiltzen hasten diren une beretik kontuan izan behar dituzte horrek sor ditzakeen arazoak. Era horretan, txikiak izanik ganorazko jokabiderako oinarriak ezartzen zaizkie. Lan horretan plan bat ezartzea komeni da, aldeztatik bertan zein kontzeptu agertuko diren zehaztuz eta behar adineko informazioa pilatuz.
- 3 Arina eta praktikoa izan zaitetz zeure azalpenetan:** Adibide praktikoa erabiltzea irtenbide egokia izan daiteke, haur eta gazteek arriskuak gogoan izateko biderik onena, hauek sortzen dituzten ondorioak azaltzea da. Erakutsi iezaizkiezu benazko kasuen ereduak, non malwarea dela eta datuak galtzea eman den, edota sarearen bidez norbait ezagutuz eskarmentu tamalgarria izan dutenenak.
- 4 Euren burua zaintzen irakatsi iezaiezu:** Ikasgai praktikoen artean azal iezaiozu antibirusa nola konfiguratu, pasahitz seguruak sortu, sare bidezko erosketak zuhurtasunez egiten etab.

