

MENORS A LA XARXA Un joc de NENS?



PANDA
SECURITY

One step ahead.

MENORS A LA XARXA



Un joc de NENS?



L'any 2007 el malware (virus, spyware i altres codis maliciosos) es va multiplicar per deu respecte l'any anterior. A més, els ciberdelinqüents han descobert en noves eines com la missatgeria instantània (programes tipus MSN Messenger o Yahoo! Messenger, etc.), programes d'intercanvi d'arxius (com eMule o Kazaa) o els blogs una nova forma d'infectar als usuaris o de fer-se amb les seves dades confidencials.

Dit d'una altra manera, els riscos a Internet van en augment i els menors, que són els que no tenen gaire preparació, també són els que estan més desprotegits.

Tot seguit, exposarem quines són les principals amenaces d'Internet per als menors, i com se'n poden defensar. La major part d'aquesta tasca de protecció correspon als pares, que han de ser capaços de controlar el que els seus fills fan a Internet, educant-los per a fer un ús responsable i segur de les noves tecnologies.

Dades significatives: Els menors a Internet



A Espanya, 7 de cada 10 nens i nenes d'entre 10 i 14 anys fan ús d'Internet, essent Catalunya la regió on més menors s'hi connecten, el 88,5%

Segons se'n deriva d'un estudi dut a terme l'any 2004 per Kleiner i Lewis, el 90% dels nens entre 6 i 10 anys d'edat fa ús d'Internet habitualment. L'any 2006 un *estudi* realitzat per l'American Psychological Association (Associació Estadounidenca de Psicologia) va xifrar entre el 75 i el 90% el percentatge de joves estatunidencs que fa ús d'Internet, participa en xats o parla tot sovint per missatgeria instantània.

A la Unió Europea les dades no són molt diferents. Segons l'Eurobaròmetre, un 64% dels joves té *accés a Internet* a Dinamarca, els Països Baixos i el Regne Unit; a Suècia, aquest percentatge és del 63%, a Finlàndia del 62% i a Estònia del 60%. A la resta de països de la Unió es mouen en proporcions similars, a excepció de Grècia (15%), Xipre (20%), Eslovàquia (30%) i Portugal (31%).

De fet, a Espanya, 7 de cada 10 **nens i nenes** d'entre 10 i 14 anys **fan ús d'Internet**, essent **Catalunya** la regió on més menors s'hi connecten, el 88,5%.

És a dir, Internet és un món quotidià en la vida dels menors. S'hi passen moltes hores connectats, a l'escola i a casa. Per això, tant els seus pares com ells mateixos han de conèixer els riscos que els aguaiten a la xarxa i saber com combatre'ls.



Principals riscos

Els nens i els joves que naveguen per Internet s'enfronten a diferents riscos. Des de possibles fonts d'infecció de l'ordinador fins a una suplantació de la personalitat que pot acabar en una mala trobada.

Tot seguit, presentarem una llista de les principals amenaces i la forma en què pares i fills poden enfrontar-s'hi.



En la missatgeria instantània la identitat dels usuaris es produeix a través d'una adreça de correu associada a un password. D'aquesta manera, si algú té accés al compte d'un dels nostres contactes, no hi haurà res que indiqui que amb qui estem parlant no és el nostre interlocutor legítim

La missatgeria instantània i el correu electrònic

La missatgeria instantània (a través de programes com MSN Messenger, Yahoo! Messenger, Google Talk, ...) s'ha convertit en una de les principals eines de comunicació entre els joves. Aquest ús massiu no ha passat desapercebut als ciberdelinqüents, que les han convertit en un dels principals mitjans on actuar.

Un dels riscos a què s'enfronten els nens i els joves que fan ús d'aquestes eines és la suplantació de la identitat (que algú es faci passar per una altra persona per tal d'enganyar al seu interlocutor). En aquests programes la identitat dels usuaris es produeix a través d'una adreça de correu associada a un password. D'aquesta manera, si algú té accés al compte d'un dels nostres contactes, no hi haurà res que indiqui que amb qui estem parlant no és el nostre interlocutor legítim. Si tenim arxius compartits amb aquest contacte, l'atacant hi podrà tenir lliure accés. Per això, és important no compartir informació confidencial (dades personals, adreça física, números d'identificació o bancaris, claus, etc.) a través de mitjans insegurs com la missatgeria instantània.

Un altre perill de la suplantació d'identitat – molt més seriós i que ja ha provocat fortes alarmes socials – és el de la pederàstia. Casos com el de la menor asturiana que va ser coaccionada per un pederasta que contactà amb ella per Messenger, *i d'altres que s'han produït en els darrers mesos* han posat de manifest l'ús que els pedòfils fan d'aquests serveis. Els pedòfils, un cop s'han guanyat la confiança dels menors, miren de fer-se passar per persones joves, fotògrafs de moda interessats a fer un book als adolescents i d'altres argücies similars.

Per tal de protegir als menors d'aquest risc, cal ensenyar-los, igual que a la vida real, a no relacionar-se amb estranys i a donar-los la confiança suficient per a què, en cas que tinguin dubtes o por, parlin obertament amb els seus pares o un altre adult.

Para La infecció de l'ordinador per l'entrada d'algun virus o d'un altre codi maliciós és un altre risc de la missatgeria instantània. Més del 58,6% dels cucs (codis maliciosos capaços de propagar-se per si mateixos) que PandaLabs ha detectat al llarg del primer semestre de l'any estaven dissenyats per a propagar-se a través d'aquestes eines. Alguns estan dissenyats per a capturar contrasenyes bancàries de banca online. D'aquesta manera, el risc en cas d'infecció ja no el pateixen només els joves, sinó que en cas d'emprar el mateix ordinador que els seus pares, l'ús inadequat d'aquests serveis pot suposar el robatori de les claus bancàries, i, a través d'elles, els diners dels pares.

MENORS A LA XARXA



Un joc de NENS?



Per a lluitar contra el codis maliciosos que es distribueixen a través de missatgeria instantània, cal seguir un senzill consell: no executar cap arxiu ni seguir cap vincle que ens arribi per aquest mitjà

Per a lluitar contra el codis maliciosos que es distribueixen a través de missatgeria instantània, cal seguir un senzill consell: no executar cap arxiu ni seguir cap vincle que ens arribi per aquest mitjà. Com a mínim, no fer-ho abans de preguntar-li-ho a la persona que suposadament ens ho envia, per a comprovar que ens ho està enviant de debò.

El correu electrònic és una altra de les fonts de risc per als més petits. En aquest cas hi ha diverses amenaces:

- En primer lloc, hi ha l'spam. Tot sovint arriben emails al correu anunciant tota mena de coses, des de casinos online fins a medicines. Els nens i les nenes, que són molt més innocents que els adults, es poden arribar a creure tot el que s'explica en aquests missatges i crear-se a si mateixos un greu problema. D'aquesta manera, poden tenir accés a casinos online i a perdre diners, acabar desenvolupant una ludopatia o adquirir medicines, fins i tot droga, de procedència més que dubtosa i que, en cas d'estar adulterada, pot provocar-li un greu problema de salut.
- En segon lloc, hi ha les falses ofertes de feina. Aquest risc potser no afecta als més joves, però és un perill per als adolescents. Es tracta de missatges que ofereixen increïbles ofertes de feina. L'usuari podrà guanyar-hi molts diners a canvi de no fer res o gairebé res. Només haurà de facilitar un número de compte bancari on s'ingressarà una quantitat de diners que haurà de desviar a un altre compte a canvi d'una comissió. Sembla tan senzill que qualsevol adult amb sentit comú ho trobaria sospitós. Tot i així, un jove que vulgui guanyar-se un diner fàcil pot caure en la temptació. I això suposaria estar convertint-se en el còmplice d'un delictes, donat que l'objectiu d'aquests moviments bancaris és blanquejar diner procedent d'activitats delictives.
- Un tercer risc és que s'introdueixi algun virus o un altre exemplar de malware a l'ordinador. Els codis maliciosos que es distribueixen a través d'aquest sistema sovint inciten als usuaris a seguir un vincle o a descarregar un arxiu (la qual cosa provocarà la infecció) mitjançant l'ús d'un tema suggerent: accedir al tràiler d'una pel·lícula, imatges eròtiques de personatges famosos, descàrregues de jocs, etc. Això es coneix com enginyeria social. Aquests atractius fan que molts adults mosseguin l'ham, i tot plegat ens dona una idea del fàcil que seria enganyar un menor.

Per tal de protegir als menors d'aquestes amenaces, cal ensenyar-los a desconfiar dels missatges procedents de fonts desconegudes. Se'ls ha de convèncer de què no tot el que s'explica en aquests missatges és veritat i que no han d'executar cap arxiu ni clicar sobre cap vincle que vingui d'aquest tipus de fonts.



Els riscos dels programes d'intercanvi d'arxius (Emule, Kazaa, etc.)

L'intercanvi d'arxius a través d'aquests programes és una altra de les principals fonts d'infecció dels ordinadors. Molts codis maliciosos, generalment els anomenats cucs, es copien a les carpetes d'aquests programes amb noms suggerents (títols de pel·lícules, de programes, etc.) per tal que altres usuaris els descarreguin i els executin al seu ordinador.

El perill és similar al de l'enginyeria social. De fet, aquest comportament se'n podria considerar una variant: el nom suggerent pot servir per a temptar a nens i nenes que, sense voler-ho, estaran introduint a l'ordinador un arxíu maliciós.

Per tot això, els menors han de saber quins arxius poden baixar i quins no d'aquestes xarxes. A més, convé analitzar l'arxíu amb una solució de seguretat abans d'obrir-lo per primer cop. Si quan l'obrim apareix un missatge d'error o un altre on se'ns demana que descarreguem una llicència o códec, hem de començar a sospitar, doncs és gairebé del tot segur que aquest arxíu oculta algun virus o codi maliciós.

Molts codis maliciosos es copien a les carpetes d'aquests programes amb noms suggerents per tal que altres usuaris els descarreguin i els executin

Xarxes socials i blogs

Les anomenades xarxes socials (portals com MySpace o Facebook) que serveixen per a compartir fotografies i vídeos, conèixer gent o xatejar, etc. juntament amb els blogs o bitàcores, són alguns dels llocs web més visitats pels joves. Un element comú d'aquestes pàgines és que cal crear un perfil personal per a tenir-hi accés. En aquests perfils normalment s'hi introdueixen dades com el nom, l'edat, etc.

Convé recordar als menors que, en general, no cal donar aquesta informació, perquè n'hi ha prou amb una adreça de correu i un nom, que pot no ser l'autèntic, sinó un "nick" o pseudònim. A més, convé que no facilitin dades com la seva edat, adreça i, encara menys, fotografies seves.

El blog s'ha convertit per a molts menors en el substitut online del tradicional diari personal. Igual que al diari, a les bitàcores de la xarxa sovint es dona molta més informació de la que és aconsellable. Per això, els joves han de tenir cura de no publicar dades que puguin servir per a identificar l'usuari com un menor, o per a conèixer el lloc on viu, on estudia, etc.

A més, en diverses xarxes socials com MySpace es poden compartir arxius i fitxers amb la resta d'usuaris. Els menors han d'anar amb molt de compte amb qui comparteixen i a qui donen permís per a veure aquesta informació. No hi ha cap problema amb penjar fotografies, per exemple, sempre i quan es protegeixin amb una clau que només es distribueixi entre els amics i els familiars.

Els pares han de conèixer aquests nous serveis, el seu funcionament i els riscos. També han de ser capaços de transmetre als seus fills la forma correcta i segura d'utilitzar-los.



L'ús de telèfons amb tecnologies com bluetooth i una ràpida connexió a Internet estan fent aquests dispositius més vulnerables als atacs

Mòbils amb Internet: una nova font de risc

Segons se'n deriva d'un estudi de la companyia Frost & Sullivan, la creixent sofisticació dels telèfons mòbils farà que els ciberdelinqüents els situïn com un dels seus objectius prioritaris del proper any. L'ús de telèfons amb tecnologies com bluetooth (que permet l'intercanvi d'arxius entre telèfons inalàmbrics) i una ràpida connexió a Internet estan fent aquests dispositius més vulnerables als atacs.

El telèfon mòbil és un altre dels grans complements dels joves d'avui dia. Els riscos a què s'enfronten en aquest camp no són molt diferents dels d'aquells que anteriorment s'han esmentat en l'àmbit de l'ordinador.

En primer lloc, els serveis de missatgeria instantània per a mòbils ja són un fet habitual. Els joves poden xatejar a qualsevol lloc i els riscos són els mateixos que s'han esmentat anteriorment: robatori d'identitat, males trobades, infecció del dispositiu, etc.

L'spam per al mòbil també està a l'ordre del dia. Des de ja fa uns anys s'han anat enregistrant enviaments d'SMS que anuncien tota mena de productes i serveis. Molts d'ells estan relacionats amb pornografia. És a dir, que ja no només s'introdueix a l'ordinador del nen, sinó que el segueix allà on vagi a través del seu telèfon mòbil.

Per tant, els pares també hauran de controlar l'ús que els seus fills fan de la telefonia mòbil. Amb aquest fi, és aconsellable, en el cas dels més petits, que se'ls compri dispositius que no tinguin funcions que puguin ser font de risc i, en el cas dels més grans, aconsellar-los sobre l'ús adequat d'aquests dispositius. Se'ls ha de recordar que no han de contestar missatges de procedència sospitosa, ni trobar-se amb desconeguts.

MENORS A LA XARXA

Un joc de NENS?



El risc d'infectar-se

Hem vist als epígrafs anteriors diverses formes en què els usuaris més joves poden infectar el seu ordinador o el de la família (vincles que arriben a través de la missatgeria instantània o del correu, amb la descàrrega d'arxius infectats, ...) Els perills que suposen tenir un codi maliciós al sistema són molts i diversos.

En primer lloc, i com s'ha comentat anteriorment, si els joves comparteixen l'ordinador amb els seus pares, pot passar que una conducta de risc del jove acabi infectant l'ordinador amb programes dissenyats per a robar les claus bancàries quan els adults inicien la seva sessió.

Però el malware no és només un risc per als adults. També ho és per als propis menors. Per exemple, pot passar que s'introdueixi un adware al seu ordinador. Aquests codis maliciosos estan dissenyats per a mostrar anuncis mitjançant finestres emergents, banners, etc. En el cas dels adults, aquests exemplars de malware poden ser més aviat només una molèstia (encara que també s'hi ha d'anar amb compte, ja que alguns descarreguen trojans a l'equip), però en el cas dels nens i nenes el risc és més important perquè alguns ensenyen anuncis i porten a pàgines amb un contingut clarament pornogràfic. D'aquesta manera, els menors poden ensopegar amb la pornografia al seu propi ordinador, sense que els calgui navegar per a anar a trobar-la.



Si els joves comparteixen l'ordinador amb els seus pares, pot passar que una conducta de risc del jove acabi infectant l'ordinador

MENORS A LA XARXA

Un joc de NENS?



Consells per als pares

- 1 Parla amb els teus fills.** La primera tasca que has d'emprendre per a protegir als teus fills és parlar amb ells. Has de saber quines pàgines visiten, amb qui xerren, què els agrada veure, etc. Igual que no els deixaries sortir de casa sense saber on van i amb qui, tampoc els has de deixar entrar a Internet sense saber abans si el que estan fent està bé.
- 2 Informa't i aconsella als teus fills.** Per molts pares Internet encara és un món desconegut. Altres el fan servir per a cercar informació, llegir la premsa o descarregar música, pel·lícules i altres arxius, però la major part dels serveis que fan anar els seus fills són completament desconeguts. Per això, un pas molt important serà informar-te sobre les eines que ofereix la xarxa als menors, els perills que hi aguiten i la forma d'evitar-los. Un cop acomplert això, podràs aconsellar als teus fills sobre la forma més segura de gaudir d'allò que els agrada.
- 3 Estableix normes fermes en l'ús d'Internet.** Has de posar normes clares i contundents que regulin l'horari, el temps de connexió i la forma d'ús d'Internet. A més, has de vigilar que s'acompleixin, especialment pel que fa a l'horari nocturn. Un altre aspecte és el de la situació dels ordinadors a casa: si hi ha un sol ordinador per a tota la família, és millor que estigui en una sala comuna i no al dormitori del menor.
- 4 Prohibeix als menors donar informació confidencial.** Has d'ensenyar als teus fills a no facilitar dades com el seu nom, la seva adreça o les seves fotografies per la Xarxa. Recomana'ls que facin servir "nicks" o pseudònims al fòrums on es connecten i ensenya'ls a crear contrasenyes segures (que barregin majúscules, minúscules i nombres) que impedeixen que els ciberdelinqüents o usuaris malintencionats tinguin accés als comptes de correu, de missatgeria o similars.
- 5 Ensenya als teus fills a no fiar-se de les aparences.** A Internet les aparences enganyen. Hem vist com els codis maliciosos es disfressen de targetes online o de tràilers de pel·lícules, com molts pederastes es fan passar per qui no són per a fer amistat amb menors o com un missatge que sembla que ens envia un contacte conegut de missatgeria instantània pot estar infectat. Així doncs, moltes vegades a la Xarxa res no és el que sembla. Per aquest motiu has d'ensenyar als menors a ser desconfiats i a no dur a terme accions que posin en risc la seva seguretat i la seva intimitat.
- 6 Instal·la una solució de seguretat eficaç.** Per tal de protegir als teus fills dels codis maliciosos, el millor és una solució eficient i actualitzada. Les solucions per a la llar de Panda no només eliminen el malware, sinó que a més bloquegen les pàgines que puguin infectar el sistema, bloquegen l'spam i, fins i tot, en el cas de Panda Internet Security, tenen un sistema de fitrat (control parental) que et permet decidir quines pàgines poden visitar els teus fills i quines no.



Consells per als menors

- 1 No pinches sobre links.** Quan xerres per un sistema de missatgeria instantània o rebis un missatge, no cliquis mai directament sobre cap vincle. Si el missatge o el correu procedeixen d'un usuari conegut, tecleja l'adreça a la barra del navegador. Si procedeix de fonts desconegudes, val més que l'ignoris. Encara que el teclegis al navegador, podries acabar en una pàgina maliciosa que provi d'introduir algun malware al teu equip.
- 2 No descarreguis ni executis arxius de procedència desconeguda.** Moltes vegades deus haver rebut per missatgeria instantània un missatge d'un contacte que et convidava a descarregar-te una fotografia, una cançó o un vídeo. De vegades, aquest arxiu no l'ha enviat el contacte, sinó un programa maliciós que l'ha infectat i que està provant d'estendre's a més usuaris. Així doncs, el millor que pots fer és preguntar al teu contacte si de debò t'ha enviat alguna cosa. Si et contesta que no, informa'l de què està infectat i que ha de posar un missatge al seu nick que ho faci saber als seus contactes per tal que evitin "contagiar-se" també, mentre ell elimina l'arxiu nociu del seu ordinador. .
- 3 No parlis amb desconeguts.** Als xats o als sistemes de missatgeria instantània, mai no podem estar completament segurs de qui hi ha a l'altre costat. Encara menys quan es tracta de comunitats online en què els membres no tenen cap relació prèvia entre ells. Per això, mira de no fer amistat amb desconeguts i encara menys trobar-te amb ells a la vida real.
- 4 No donis informació confidencial a través de la xarxa.** No enviïs informació sensible (dades privades, la teva adreça, etc.) a través d'email o missatgeria instantània i encara menys la publicuis en un blog o en un fòrum. A més, has d'anar amb cura quan creïs els teus perfils per a serveis com FaceBook o MySpace. Allí no hi han d'aparèixer dades confidencials com la teva adreça o la teva edat. També és aconsellable que no facis servir el teu nom real, sinó un pseudònim o "nick".
- 5 Sospita al menor indici.** Si algun programa que no recordes haver instal·lat comença a mostrar-te falses infeccions o finestres emergents o pop-ups on se't convida a comprar algun tipus d'antivirus, o un altre producte, desconfia. De ben segur és que se t'hagi instal·lat algun tipus de malware a l'equip.
- 6 No executis arxius sospitosos.** Si la teva solució de seguretat t'indica que un arxiu és sospitós de tenir un malware o que, de fet, el té, no l'obris. Senzillament, elimina'l del sistema.
- 7 Parla amb els adults.** Quan tinguis dubtes sobre algun tema, vegis alguna cosa sospitosa o rebis correus o missatges ofensius o perillosos, parla amb un adult. Ells et podran aconsellar.

MENORS A LA XARXA

Un joc de NENS?



Consells per als professors

Els professors també tenen una responsabilitat important a l'hora d'educar al més petits a fer un ús correcte de les Noves Tecnologies, sobretot, avui dia que els ordinadors van guanyant espai a les aules. Per això, hi ha una sèrie de recomanacions que s'han de seguir.

- 1 Informa't.** Estudia prèviament els conceptes relacionats amb els perills a la Xarxa. Descobreix quins són i quines conseqüències tenen i com els pots fer arribar aquesta informació.
- 2 Fixa un pla d'educació en seguretat informàtica.** Mentre aprenen a fer servir i a relacionar-se amb la informàtica, els més petits han de prendre consciència dels perills que hi agaiten. D'aquesta manera se'ls estarà inculcant des de petits una conducta segura. Amb aquest objectiu convé que fixis un pla a seguir, tot preparant prèviament el que els vols explicar i reunint tota la documentació necessària.
- 3 Prepara explicacions pràctiques i amenes.** Un bon mètode és posar exemples pràctics. Una de les millors maneres per a què el petits i els joves prenguin consciència dels perills existents és ensenyar-los els efectes que tenen. Cerqueu notícies de casos reals de males trobades a la Xarxa, dades de pèrdua de dades produïdes pel malware, etc.
- 4 Ensenya'ls a protegir-se.** Entre les classes pràctiques inclou-ne alguna sobre la configuració de l'antivirus, explicacions sobre com comprar online de manera segura, etc.

