

Ghid pentru părinți

Protejarea copiilor pe Internet



ins@fe

Cu sprijinul:  upc

CUPRINS

A. Cum să folosim acest ghid

p. 4



B. Sfaturi pentru părinți și supraveghetori

p. 6



1. Paza bună trece primejdia rea

p. 6

2. Să comunicăm

p. 10

3. Hărțuirea pe Internet

p. 15

4. Divertisment & descărcare

p. 17

C. Soluții propuse pentru activități

p. 21



1. Paza bună trece primejdia rea

p. 21

2. Să comunicăm

p. 24

3. Hărțuirea pe Internet

p. 26

4. Divertisment & descărcare

p. 27

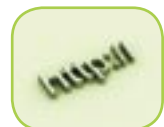
D. Glosar

p. 29



E. Legături utile

p. 38





A. Cum să folosim acest ghid

Dacă faceți planuri pentru un an, plantați orez.
Dacă faceți planuri pentru zece ani, plantați un copac.
Dacă faceți planuri pentru o viață, educați-vă copilul

Proverb chinezesc

Dragi părinți/supraveghetori,

Sunteți în posesia ghidului pentru întreaga familie privind securitatea pe Internet. Acesta se adresează familiilor cu copii în vârstă de 6 până la 12 ani și reprezintă o resursă educațională realizată cu convingerea că noile tehnologii nu ar trebui să separe generațiile, ci să le unească. Acest ghid a fost creat de către Insafe, rețeaua pan-europeană a centrelor naționale de contact care desfășoară activități de conștientizare a securității pe Internet. Dezvoltarea și crearea acestui ghid despre securitatea în mediul virtual a fost sprijinită de UPC.

Așa cum joaca pe teren sau traversarea străzii pot fi periculoase, așa și folosirea Internetului și a tehnologiilor mobile poate avea consecințe nefaste dacă nu sunteți precauți. Din fericire, există mijloace disponibile care le permit utilizatorilor de Internet să se informeze cu privire la avantajele și riscurile navigării pe Internet.

Folosiți acest ghid pentru a vă ajuta copiii să învețe cum să utilizeze Internetul în mod sigur și eficient. Acesta oferă peste cincizeci de sfaturi și exerciții utile care vă ajută să-i învățați pe copii despre securi-



tatea pe Internet într-un mod amuzant, antrenant și plăcut. Ghidul cuprinde:

- Două cărți despre securitatea pe Internet: una amuzantă adresată întregii familii și un ghid pentru părinți;
- Reguli de aur;
- O diplomă pentru întreaga familie;
- Un set de abțibilduri;
- 12 carduri de decupat cu diverse situații.

Atât în cartea pentru întreaga familie, cât și în cea pentru părinți, cele patru teme cheie referitoare la securitatea pe Internet: „**Paza bună trece primejdia rea**“, „**Să comunicăm**“, „**Divertisment și descărcare**“ și „**Hărțuirea pe Internet**“ sunt evidențiate prin diferite culori. Cartea pentru părinți servește drept referință pentru cea amuzantă adresată întregii familii. Ea conține informații utile, scurte explicații legate de activitățile propuse, soluțiile exercițiilor și situațiilor prezentate pe carduri.

Cartea pentru întreaga familie se adresează atât părinților, cât și copiilor. Cele patru teme sunt abordate prin intermediul unei povești despre doi copii, Alex și Teodora, părinții lor și experta în IT, Maria. Fiecare capitol conține activități cu caracter educațional, inclusiv exerciții online, întrebări de verificare a cunoștințelor acumulate, reguli de aur și legături utile.

Citiți povestea cu voce tare în prezența copiilor și împreună cu ei lucrați activitățile propuse. La sfârșitul fiecărui capitol puteți utiliza cardurile care prezintă situațiile aferente pentru a iniția o discuție cu copiii dumneavoastră în scopul înțelegerii în profunzime a conținutului.

După ce copiii au parcurs cu succes toate activitățile și exercițiile propuse, recompensați-i prin stabilirea unui set cu reguli de aur și solicitați-le să semneze diploma pentru întreaga familie. La sfârșit, copiii pot decora cărțile folosind abțibildurile cu emoticonițe.

Păreră dumneavoastră este foarte importantă pentru noi. Nu ezitați să luați legătura cu centrul local de contact Insafe pentru întrebări sau comentarii. Vă dorim dumneavoastră și familiei succes în „îmblânzirea“ Internetului!

Navigați în siguranță!

ins@fe



B. Sfaturi pentru părinți și supraveghetori

1. Paza bună trece primejdia rea



COMPUTERUL DE ACASĂ

Computerul de acasă poate fi o resursă educațională și de divertisment pentru întreaga familie. Așezarea computerului în camera de zi și stabilirea unor reguli clare privitoare la condițiile și timpul de utilizare a acestuia vă vor ajuta copiii să fie în siguranță.

Nu uitați că ei pot accesa **Internetul** acasă la prieteni, la Internet Café etc. De aceea, este important ca împreună să stabiliți un cod de conduită pe care să-l aplicați oricând și oriunde.

PROTEJAREA COMPUTERULUI

Protejarea computerului poate fi realizată prin înțelegerea posibilelor amenințări și prin cunoașterea unor remedii simple. Acestea includ instrumente utile de tehnologie, precum și inteligența utilizatorilor care se dezvoltă pe măsura înaintării în vârstă și a acumulării de experiență.

Diversele operații pe care dumneavoastră împreună cu copiii le puteți face utilizând computerul de acasă, precum folosirea unui **stick de memorie** sau a unui **CD-ROM**, deschiderea **atașamentelor** și **descărcarea de fișiere**, implică riscuri. Acestea au în principal legătură cu programele **malware** (programele de calculator periculoase) create pentru a produce daune computerului, pentru a vă fura datele personale sau pentru a vă furniza reclame nesolicitate.

Copiii li se prezintă diferite tipuri de malware: **virusi**, **viermi**, **cai troieni** și **spyware** și sunt învățați să recunoască simptomele unui computer virusat. Ei învață cum să prevină virusarea accesând întotdeauna Internetul de la un computer care este protejat de programe **anti-virus** sau **anti-spyware** actualizate. De asemenea, ei sunt sfătuiți să fie atenți când deschid atașamente e-mail provenite de la expeditori necunoscuți, când descarcă programe de pe Internet sau când folosesc stick-uri USB sau CD-ROM-uri.

LUPTA ÎMPOTRIVA SPAM-ULUI

80% din e-mail-urile care circulă pe Internet sunt **spam** (mesaje e-mail nesolicitate). Acestea pot avea efecte negative asupra copiilor dumneavoastră. Fără să vă dați seama, publicarea unei adrese de e-mail pe **web** când folosiți un **newsgroup** (grup de știri), un site pentru sesiuni de **chat**, un **forum** public, un site de **social networking** sau un **formular online** poate genera spam. Anumite programe software pot aduna adresele de e-mail de pe web și crea liste de distribuție care sunt apoi folosite pentru a trimite nenumărate mesaje nesolicitate. Companiile implicate în acest gen de activități sunt adesea plasate în locuri unde nu există legislația necesară pentru a preveni astfel de e-mail-uri nesolicitate!

Cel mai adesea, spam-ul are legătură cu pornografia, produse farmaceutice, tranzacții financiare dubioase etc. În plus, spam-ul poate constitui și sursa programelor care produc daune. În majoritatea cazurilor, e-mail-urile nesolicitate sunt trimise cu intenții necinstite. Iată câteva sfaturi utile pentru a vă proteja familia:

- Folosiți „**filtre spam**“. De obicei, furnizorul dumneavoastră de servicii e-mail vă pune la dispoziție opțiuni anti-spam pe care le puteți activa în cadrul programului de e-mail. Pentru mai multe informații, contactați-vă furnizorul de servicii e-mail. Verificați-vă regulat **dosarul junk** sau **spam** pentru a vedea dacă nu cumva e-mailurile pe care le așteptați au ajuns acolo. Tehnologia nu este perfectă.
- Învățați-vă copiii să nu deschidă e-mail-urile trimise de persoane necunoscute. Aproape întotdeauna spam-ul conține propuneri tentante și atașamente. Arătați-le cum să blocheze expeditorul unui e-mail sau rugați-i să ștergă mesajele cu subiecte suspecte.

NAVIGAREA PE INTERNET

Chiar și copiii mai mici pot folosi Internetul pentru a se juca și a vizita **site-uri web** cu conținut educațional. Cu toate acestea, pe Internet putem găsi și informații care nu sunt întotdeauna potrivite vârstei copiilor. Motoarele de căutare sunt utile pentru localizarea conținutului pe Internet. Totuși, deoarece căutarea se

face în funcție de alegerea cuvintelor cheie, se poate cu ușurință localiza și conținut nedorit. Căutarea unui simplu cuvânt cheie ar putea genera un site web cu conținut îndoielnic care conține cuvântul cheie în întrebare. Iată câteva sfaturi utile pentru a-i ajuta pe copii să navigheze pe Internet în siguranță:

- Creați un cont de utilizator destinat copilului folosind un **sistem de operare** (de exemplu, Windows, Linux, Mac OS) în care activați opțiunea **control parental**;
- Verificați caracteristicile opțiunii control parental în **browser-ul** de Internet și în motorul de căutare. Asigurați-vă că ați citit cu atenție opțiunile oferite de **setările de familie** ale acestor instrumente;
- Sugerați-le micilor utilizatori de Internet pe care îi aveți în grijă să utilizeze motoare de căutare destinate copiilor. De exemplu, <http://kids.yahoo.com>, <http://www.askforkids.com>, cu conținut în limba engleză, sau <http://edu.genium.ro>, cu conținut în limba română.
- Salvați adresele site-urilor web pe care copiii dumneavoastră le utilizează cel mai des în dosarul **Favorite** (una dintre opțiunile browser-ului). Astfel, le oferiți posibilitatea de a accesa site-urile de pe **net** și altă dată fără să mai utilizeze un motor de căutare.

În afară de activarea opțiunii de control parental a browser-ului și a motorului de căutare, puteți folosi un **filtru** suplimentar, program care îi protejează pe minori de site-urile web cu conținut îndoielnic. Cereți sfatul vânzătorilor de programe de calculator sau căutați pe Internet **versiuni de testare**. Nu uitați că sfaturile părinților și ale supraveghetorilor sunt extrem de importante. Tehnologia nu este perfectă, iar uneori poate crea senzația falsă de siguranță pentru copii.

Programele de filtrare pot fi atât de restrictive încât pot bloca accesul nu numai la site-urile cu conținut îndoielnic. Acestea i-ar putea împiedica pe copii să caute, de exemplu, informații despre cel de-al II-lea Război Mondial, necesare scrierii unui eseu la istorie, deoarece căutarea conduce către site-uri web în care este descrisă violența. Mai mult decât atât, orice filtru poate fi pornit sau oprit de tinerii utilizatori isteți care adesea sunt experți în ascunderea site-urilor web pe care le-au accesat. Veți afla că așa se întâmplă dacă învățați cum să utilizați computerul și programele de calculator singuri.

Vizitați site-ul web al **SIP-Bench**, un studiu sprijinit de Comisia Europeană în cadrul căruia au fost testate 30 de instrumente de control parental și anti-spam pentru a le măsura eficacitatea în protejarea copiilor cu vârste cuprinse între 6 și 16 ani împotriva conținutului dăunător din diferite aplicații de Internet: **browsing**, trimiterea sau primirea de e-mail-uri, **transferul de fișiere**, sesiunile de chat și **mesagerie instantanee** (instant messaging).

Pe lângă evitarea **conținutului dăunător**, trebuie să vă asigurați că tinerii nu cred tot ceea ce văd sau citesc pe Internet. În broșura amuzantă destinată întregii familii, sugerăm ca, întotdeauna când copiii caută informații pe Internet, să viziteze cel puțin 3 site-uri web pentru a compara conținutul găsit online. Copiii sunt de asemenea sfătuiți să menționeze în mod sistematic sursa pentru informațiile găsite, ori de câte ori le folosesc pentru efectuarea temelor.

REGULI DE AUR PENTRU PĂRINȚII MICILOR UTILIZATORI DE INTERNET

- Asigurați-vă că aveți computerul protejat de un **firewall**, precum și de programe anti-virus și anti-spyware. Actualizați aceste programe și fiți atenți la **alerțele** pe care le generează.

Verificați dacă furnizorul dumneavoastră de servicii de Internet vă oferă instrumente anti-virus și anti-spyware pe care le puteți utiliza;

- Folosiți un filtru spam în cadrul programului dumneavoastră de e-mail și păstrați-vă adresa de e-mail secretă, nepublicând-o pe Internet. Evitați e-mail-urile de la persoane necunoscute și **scațați** atașamentele înainte de a le deschide;
- Măriți la maximum nivelul controlului parental al computerului dumneavoastră: a sistemului de operare, a browser-ului de Internet, a motorului de căutare și a programului de e-mail. Creați conturi de utilizator separate pentru copiii dumneavoastră. Asigurați-vă că setările de confidențialitate sunt configurate la nivel maxim (vizitați meniul „opțiuni“ din browser-ul dumneavoastră);
- Aveți în vedere folosirea unor programe filtru suplimentare;
- Contactați furnizorul dumneavoastră de servicii de Internet sau un expert de îndată ce computerul începe să funcționeze ciudat, deoarece e posibil să fie virusat. Și furnizorul dumneavoastră de servicii de Internet ar putea să ofere sfaturi pentru părinți;
- Reclamați la **centrul de asistență** național al utilizatorilor de Internet (consultați Legături utile) în cazul în care ați dat peste conținut online nedorit;
- Ori de câte ori puteți, stați lângă copii în timp ce utilizează Internetul. Aceasta este o ocazie excelentă de a încuraja comunicarea și de a spori încrederea. Profitați de ocazie și învățați împreună;
- Nu uitați că aceste reguli de securitate sunt valabile atât pentru dumneavoastră, cât și pentru copiii dumneavoastră. Încurajați-i să vă informeze despre orice cred că nu este în regulă.

LEGĂTURI UTILE

Copiii dumneavoastră pot urma un curs despre securitatea pe Internet în limba engleză și urmări aventurile online ale lui Niamh și Fionn:

<http://test.scoilnet.ie/webwise/lessons/index.html>

Pentru a vă bucura de navigarea pe Internet în siguranță, fără a vă teme, cunoașterea riscurilor și a mijloacelor de protecție este cheia. Pentru mai multe informații, accesați site-ul web <http://www.sigur.info/> sau <http://www.makeitsecure.ie> cu conținut în limba engleză.

Dacă în timp ce navigați pe Internet întâlniți conținuturi pe care le considerați ilegale, puteți raporta acest lucru la: <http://www.sigur.info/>.

2. Să comunicăm



PIESELE PUZZLE-ULUI

Vă mai amintiți cât de important a fost pentru dumneavoastră să mențineți contactul cu prietenii pe măsură ce v-ați maturizat? Internetul oferă o mulțime de ocazii de a întâlni prieteni, precum și mijloace de auto-exprimare și socializare prin intermediul serviciului de e-mail, **schimb de fișiere**, **blogging** și social networking (de exemplu: MySpace, Facebook, Hi5, Habbohotel). Adolescenții din zilele noastre utilizează tehnologia pentru a încerca lucruri noi și pentru a socializa într-un loc pe care îl consideră intim și lipsit de supravegherea părinților.

Capitolul despre comunicare le prezintă părinților și copiilor conceptele de **date personale**, **confidențialitate**, interacțiuni online pozitive și gestionarea riscului, de exemplu, contactul cu persoane necunoscute. Confidențialitatea online este strâns legată de conceptul de **conturi** și **profiluri**. Prin intermediul contului se poate accesa un serviciu online.

În mediul nevirtual, abonamentul de transport, abonamentul la sala de gimnastică sau cel de membru al unui club conțin datele dumneavoastră cu caracter personal. Conturile și serviciile online sunt asemănătoare. Nu puteți deschide niciunul dacă nu furnizați niște date personale care sunt utilizate pentru crearea profilului dumneavoastră de utilizator. Important este că puteți alege ce informații cu caracter personal doriți să faceți publice și cui anume.

Protejarea intimității nu înseamnă a spune minciuni, ci a deține controlul asupra informațiilor cu caracter personal pe care doriți să le faceți publice. Tinerii sunt entuziasmați de comunicarea online cu prietenii și de crearea imaginii lor pe Internet. Totuși, ei nu realizează întotdeauna impactul pe care îl poate avea asupra lor furnizarea de date personale pe Internet.

CREAREA PROFILULUI

Primul pas în protejarea datelor personale este crearea unui profil mai sigur. Trebuie să selectați cu foarte multă atenție informațiile pe care le veți include în crearea profilului, precum și setările de confidențialitate pe care le utilizați.

Creați câteva conturi de e-mail pentru diferite activități online. De exemplu, când folosiți servicii online, precum chat-ul, instant messaging, blogging etc. încurajați-vă copilul să utilizeze o adresă de e-mail și un **nume de utilizator** neutre, care să nu le dezvăluie adevăratul nume.

Păstrați întotdeauna **parolele** conturilor dumneavoastră secrete. Asigurați-vă că tinerii conștientizează că nu trebuie să dezvăluie datele conturilor lor prietenilor care ar putea abuza de încrederea acordată. Pe de altă parte, ar fi bine să știți parolele copiilor dumneavoastră, astfel încât să le puteți supraveghea conturile.

Nu uitați să vă particularizați **setările de confidențialitate** ale profilului/contului, prin alegerea opțiunii privat, și nu public. Astfel, aveți posibilitatea de a controla cui anume îi apare vizibil profilul și cu cine puteți interacționa. În cazul alegerii opțiunii profil privat, puteți să vă gestionați lista de contacte. Învățați-i pe copii să accepte numai contactele persoanelor pe care le cunosc deja din viața de zi cu zi.

În cazul în care copiii folosesc camerele de chat, verificați dacă:

- există moderatori prezenți. Lipsa unui moderator înseamnă o sesiune de chat nesigură;
- există mijloace prin care participanții nedorți pot fi ignorați sau blocați;
- există o secțiune pe site unde, în cazul unor probleme, se poate cere ajutor și **raporta** un abuz;
- regulile serviciului de chat sunt clar stabilite și vizibil plasate.

IMAGINI ȘI CAMERE WEB

Copiii trebuie să înțeleagă că fotografia lor reprezintă un lucru personal și că imaginile digitale sunt extrem de importante. Acestea pot fi cu ușurință transmise și **manipulate** digital, dar sunt foarte greu de șters odată ce au fost trimise prin intermediul unui computer sau al telefonului mobil. Ele pot rămâne online pentru totdeauna! **Camerele web** trebuie utilizate cu atenție și nu fără supravegherea părinților. Instrumentele de chat prin intermediul camerei web, precum și **directoarele** pot fi riscante. Atât dumneavoastră, cât și copiii nu trebuie să puneți la dispoziția oricui fotografii personale, ci doar persoanelor pe care le cunoașteți și în care aveți încredere. Întotdeauna cereți permisiunea înainte de a publica o poză a altei persoane. Nu vă lăsați copiii să utilizeze computerul și camera web singuri în camera lor.

CONTACTUL CU PERSOANE NECUNOSCUTE

Persoanele cunoscute online nu sunt întotdeauna ceea ce pretind a fi. Învățați-i pe copii să-și protejeze intimitatea online așa cum ar proceda și în mediul nevirtual. De ce nu ar urma copiii aceleași reguli pe Internet pe care le-ați stabilit în viața de zi cu zi în ceea ce privește comportamentul lor față de persoanele necunoscute?

Copiii dumneavoastră pot construi o relație strânsă cu prietenii de pe Internet și tind să aibă re- pede încredere în persoanele care manifestă interes și înțelegere în ceea ce-i privește, chiar dacă nu îi cunosc cu adevărat. Prin urmare, ei pot fi foarte tentați să se întâlnească cu aceștia, fără a vă informa. Copiii nu sunt adesea conștienți de pericolele unor întâlniri de acest gen și le pot considera inofensive. Astfel, ei devin victime ale **pedofiliei online**. Studiile arată că o mulțime de copii merg neînsoțiți să-și întâlnească „prietenii“ de pe Internet sau fără să le spună părinților. Discutați cu copiii dumneavoastră despre acest lucru pentru a vă asigura că nu vor proceda astfel. Comunicarea este cheia.

NETICHETA

Neticheta se referă la regulile de conduită pe Internet și la tratarea celorlalți în același mod în care v-ar plăcea să fiți tratați. Copiii s-ar putea să nu realizeze că în mod accidental pot ofensa anumite persoane în mediul virtual. Din păcate, unii folosesc Internetul și/sau telefoanele mobile pentru a-i hărțui pe ceilalți online. Acest lucru se numește hărțuire pe Internet și poate afecta unul până la patru copii (pentru mai multe informații, consultați capitolul corespunzător).

LIMBAJUL CHAT-ULUI

Când utilizează chat-ul, tinerii folosesc un limbaj specific, plin de **emoticonițe și acronime!** Consultați tabelul de mai jos pentru a vă familiariza cu acestea. 😊

Iată lista acronimelor folosite în sesiunile de chat. Pentru mai multe informații, consultați secțiunea „Legături utile“.

121: one to one	JJ: just joking
AFK: away from keyboard	K: all right /ok
A/S/L: age, sex, location (or just “ASL”)	KFY/K4Y: kiss for you
BBB: bye bye baby	KISS: keep it simple, stupid
B4N: bye for now	KPC: keeping parents clueless
BBL: be back later	L8R: later
BF: boyfriend or best friend	IRL: in real life
BFF: best friends forever	LMIRL: let’s meet in real life
C: see?	LOL: laughing out loud, lots of love
Comp: computer	LY4E: love you forever
CU: see you	NE1: anyone
CUL: see you later	NP: no problem/ noisy parents
CYO: see you online	OIC: oh, I see
EGBOK: everything going to be ok	OLL: online love
F2F: face to face	PAL: parents are listening

G2G or GTG: got to go

<G>: grin

GFN: gone for now

GL: good luck

GM: good morning /good match

HAND: have a nice day

^5: High 5

H2G: have to go

HDOP: help delete online predators WDYT: what do you think

IDK: I don't know

ILU/ILY: I love you / I like you

PAW: parents are watching

PIR: parent in room / people in room

POS: parent over shoulder

RL: real life

S^, S'UP: what's up?

TTYL: talk to you later

TY: thank you

WB: welcome back/ write back

WTGP: want to go private?

WYCM: will you call me?

Puteți crea emoticonițe combinând semne de punctuație și litere ca în exemplele de mai jos:

Față zâmbitoare (cu sau fără nas)

: -) or :)

două puncte, (liniuță), paranteză

Față tristă (cu sau fără nas)

:(or :(

două puncte, (liniuță), paranteză

Față care face cu ochiul (cu sau fără nas)

;-) or ;)

punct și virgulă, linie, paranteză

Față uimită (cu sau fără nas)

: -o or : o

două puncte, (liniuță), litera o mic de tipar

Zâmbet larg (cu sau fără nas)

:-D or : D

două puncte, (liniuță), litera D mare de tipar

Limba scoasă (cu sau fără nas)

: p or :-p

două puncte, litera p mic de tipar

REGULI DE AUR

- Faceți-vă timp să descoperiți cum își petrec copiii dumneavoastră timpul online și dați-le ocazia să vă arate cum comunică cu prietenii;
- Învățați-i să-și protejeze intimitatea online astfel:
 - Prin crearea de profiluri sigure cu activarea setărilor de confidențialitate
 - Prin protejarea parolilor conturilor personale
 - Prin contactarea pe Internet și trimiterea de răspunsuri numai persoanelor pe care le cunosc din viața de zi cu zi
 - Cerând întotdeauna acordul dumneavoastră înainte de a încărca pe Internet propriile fotografii sau cele cu familia, casa, școala lor etc.
 - Să nu furnizeze date personale, precum numărul lor de telefon, adresa, școala, echipa în care joacă, decât persoanelor pe care le cunosc în viața de zi cu zi;
- Așezați computerul de acasă în camera de zi, astfel încât să puteți supraveghea activitățile pe Internet ale copiilor;
- Împreună cu ei, asigurați-vă că știți:
 - Cum să refuzați anumite contacte sau să blocați anumite persoane din lista de contacte
 - Opțiunile de securitate și de raportare a problemelor care sunt disponibile pe site-urile web pe care le accesați
- Construiți o relație bazată pe încredere cu copiii dumneavoastră, convingându-i să discutați chiar și despre greșelile pe care le-au făcut, astfel încât să căutați soluții împreună! Greșelile fac parte din procesul de învățare.

LEGĂTURI UTILE

Site pentru părinți:

<http://www.scoalaparintilor.ro>

Sparge codul chat-ului vizitând wikiHow (cu conținut în limba engleză):

<http://www.wikihow.com/Understand-Chat-Acronyms>

Consultați raportul Eurobarometru 2007 despre „Internet mai sigur pentru copii”:

http://ec.europa.eu/information_society/activities/sip/eurobarometer

3. Hărțuirea pe Internet



UN INCIDENT DE HĂRȚUIRE PE INTERNET

Comunicarea prin intermediul Internetului și a telefoanelor mobile are o mulțime de avantaje. Din păcate, există și dezavantaje. Copiii dumneavoastră pot primi sau trimite mesaje cu conținut negativ care îi lezează pe ei sau pe ceilalți. Este important să-i învățați pe copii să aibă un comportament acceptat social – chiar și propriii noștri copii nu sunt întotdeauna îngerași;-)

Hărțuirea pe Internet înseamnă folosirea noilor tehnologii de informare și comunicare cu scopul de a hărțui, de a leza și intimida un individ sau un grup. Serviciile de e-mail, chat, instant messaging, telefoane mobile sau alte mijloace digitale pot fi utilizate în acest sens. În cadrul jocurilor din mediul virtual, agresorii online le pot ataca copiilor dumneavoastră **avatarurile**, astfel încercând să le modifice sau să fure **proprietățile virtuale** sau să aducă transformări negative avatarului astfel încât acesta să nu funcționeze normal.

De obicei, copiii se plâng de problemele legate de publicarea datelor personale în spații publice, de exemplu, postarea unei fotografii personale sau a unor informații cu caracter personal pe un forum public sau pe un site web. Așa cum **hărțuirea** la școală sau pe terenul de joacă nu este tolerată, la fel și în cazul celei de pe Internet, părinții, profesorii și copiii trebuie să ia atitudine pentru a acționa împotriva acesteia. Spre deosebire de hărțuirea tradițională, cea de pe Internet poate afecta copilul chiar și atunci când acesta nu se mai află în prezența agresorilor. Aceștia pot trimite mesaje de amenințare în conturile e-mail de acasă și pe telefoanele mobile, la orice oră din zi și noapte.

Părinții pot sprijini promovarea unui mediu în care hărțuirea să nu fie tolerată. Învățați-i pe copii că a fi anonim online nu înseamnă a te comporta iresponsabil. Copiii trebuie să-și cunoască drepturile și responsabilitățile, dar să și respecte drepturile celorlalți.

Mențineți întotdeauna un dialog deschis cu copiii dumneavoastră, astfel încât să puteți discuta cu ei orice problemă care îi neliniștește. Noile tehnologii, precum Internetul și telefoanele mobile, vă oferă ocazia excelentă de a purta discuții și de a vă informa.

REGULI DE AUR:

- Preveniți experiențele negative ale copiilor dumneavoastră asigurându-vă că aceștia știu cum să-și protejeze propria intimitate și cum să respecte intimitatea altor persoane;
- Învățați copiii să nu răspundă mesajelor celor care îi hărțuiesc;

- Ajutați copiii să înțeleagă ce fel de mesaje și ce tip de atitudine i-ar putea deranja pe ceilalți și cum pot evita acest lucru;
- Asigurați-vă că ei știu cum să blocheze expeditorii din lista de contacte;
- Păstrați mesajele de hărțuire drept dovezi;
- Aflați metodele împotriva hărțuirii promovate de școala în care învață copiii dumneavoastră. Implicați-vă împreună cu alți părinți și profesori pentru a preveni hărțuirea din mediul virtual și cel nevirtual;
- Țineți legătura cu anturajul copiilor dumneavoastră: cu prietenii și părinții lor, precum și cu profesorii și colegii lor;
- Încurajați-vă copiii să discute cu dumneavoastră despre orice experiență neplăcută din mediul virtual sau din cel nevirtual. Asigurați-i că indiferent dacă ar greși, i-ați ajuta și ați găsi împreună soluții!
- Asigurați-vă că înțeleg că nu e vina lor dacă cineva îi hărțuiește.

LEGĂTURI UTILE

Pe următorul site web veți găsi informații utile pentru a înțelege mai bine problema hărțuirii la școală și cum poate fi aceasta oprită (conținut în limba engleză):

<http://www.nehb.ie/coolsschoolbullyfree/kids1.htm>

Pe acest site web sunt prezentate desene și activități propuse pentru uz școlar despre cum pot copiii să facă față hărțuirii și cum să o oprească (conținut în limba engleză):

<http://www.stopbullying.org>

Linia verde pentru protecția copilului a fost deschisă în 2001 de Guvernul României prin intermediul Autorității Naționale pentru Protecția Drepturilor Copilului (ANPDC).

Numărul de telefon gratuit al liniei verzi este:

08008200200

4. Divertisment & descărcare



PE INTERNET NU TOT CE ZBOARĂ SE MĂNÂNCĂ

Internetul este un spațiu virtual pentru multe activități, inclusiv comerciale. Dacă nu le permiteți copiilor să ceară tot ceea ce văd în reclamele TV sau ceea ce îi tentează din magazine, atunci trebuie să-i învățați să nu dorească sau să nu aibă încredere nici în reclamele de pe Internet, de exemplu: muzică și jocuri, **tonuri de apel**, alte accesorii și cumpărarea de servicii online.

Petrecerea timpului împreună cu copiii în timp ce aceștia utilizează Internetul vă oferă posibilitatea de a le explica că produsele, ca de exemplu, tonurile de apel, **imaginile de fundal**, **mp3**-urile, avatarurile și altele sunt rar gratuite. Ori de câte ori găesc reclame de acest gen, arătați-le cuvintele scrise cu litere de dimensiuni mici pentru a le demonstra că nu trebuie să ia drept bun tot ceea ce este pe net.

Pentru a vă înscrie la orice serviciu (gratuit sau nu), trebuie să completați un **formular online** cu date personale. Completați aceste formulare numai în cazul în care știți cum vor fi folosite datele dumneavoastră și convingeți-vă copiii să nu completeze astfel de formulare decât împreună cu dumneavoastră.

Ferestrele pop-up sunt adesea utilizate pentru a vinde diverse lucruri pe Internet. Acestea nu sunt întotdeauna dăunătoare. Depinde dacă provin de la un site web sigur sau nu. În general, dacă aveți încredere în site-ul web, puteți avea încredere și în fereastra pop-up. Totuși, unele ferestre pop-up sunt utilizate pentru a vinde produse care nu sunt de calitate sau pentru a vă direcționa către chestionare online de colectare a datelor dumneavoastră personale. Învățați-vă copiii să închidă ferestrele pop-up nesigure, făcând clic pe cruciulița roșie din colțul din dreapta sus.

SĂ JUCĂM JOCURI ONLINE

Jocurile online diferă de cele digitale vechi deoarece necesită o **conexiune la Internet**. Copiii pot juca pe CD-uri/DVD-uri, pe site-uri web, pe console de jocuri sau pe telefoanele mobile și alte dispozitive de mici dimensiuni (handheld devices).

Există **jocuri online** simple, cum ar fi binecunoscutele Pacman și Tetris, sau complexe, în care

se joacă online mai mulți utilizatori care au diverse sarcini, ca de exemplu, să creeze diverse conținuturi și povești. Altele, precum **multiplayer games** (jocurile cu mulți jucători), acceptă adevărate comunități virtuale de jucători. Acestea îi pot expune la riscuri, cum ar fi întâlnirea unor persoane necunoscute (pentru mai multe informații consultați capitolul „Să comunicăm“).

Jocurile sunt importante pentru dezvoltarea copiilor, deoarece prin intermediul unui mediu guvernat de reguli de joc, aceștia își dezvoltă abilitățile sociale și gândirea. Dat fiind faptul că o mulțime de jocuri digitale sunt atractive și interactive, acestea sunt utilizate în scop educațional.

Cu toate acestea, nu toate jocurile digitale sunt de calitate. Dumneavoastră sunteți cei care trebuie să decideți care jocuri sunt potrivite pentru copii și, prin stabilirea unor reguli, puteți să vă asigurați că perioada de timp pe care copiii o petrec jucându-se online nu este în detrimentul altor activități.



Există un sistem pan-european de clasificare în funcție de vârstă, PEGI online, pentru jocurile interactive, în care acestea sunt clasificate după vârstă și conținut. Acesta este susținut de câțiva producători, inclusiv PlayStation, Xbox și Nintendo, precum și de editori și dezvoltatori de jocuri interactive din întreaga Europă.

Căutați aceste informații pe spatele oricărei cutii de joc, dar nu uitați că nu toți copiii în vârstă de 12 ani sunt la fel.



PUNEREA DE FIȘIERE LA DISPOZIȚIA ALTOR UTILIZATORI DE INTERNET ȘI DREPTURILE DE AUTOR ©

Tinerii privesc Internetul ca pe o comoară cu filme, muzică și jocuri care pot fi descărcate, vizionate, ascultate și jucate. Adesea, aceștia descarcă și încarcă materiale folosind **rețelele de calculatoare** fără să țină cont că lucrările originale ale artiștilor sau ale altor **autori** sunt protejate de **drepturile de autor**. Sunt incluse aici filmele, cântecele, cărțile, programele de calculator și fotografiile.

Este ilegal?

Punerea de fișiere la dispoziția altora și schimbul nu sunt ilegale în cazul în care conținutul acestora a fost creat de voi înșivă. În general, încărcarea sau descărcarea de muzică și filme fără permisiunea deținătorului de drepturi este ilegală peste tot în lume (deși fiecare țară are propria lege în ce privește drepturile de autor). Ca regulă practică, considerați ilegală punerea de fișiere cu muzică și filme la dispoziția altora și fiți atenți cu aplicațiile **de la egal la egal (peer to peer)**.

Este riscant?

Schimbul de fișiere vă pune computerul în pericol datorită deschiderii porturilor. Prin intermediul acestora pot pătrunde în computer programe dăunătoare, care vor conduce la disfuncționalități ale acestuia. De asemenea, este posibil ca alte persoane să poată să vă acceseze informațiile cu caracter personal sau să vă folosească computerul pentru a trimite spam sau **conținut ilegal**.

Unde pot găsi muzică legală?

Sute de site-uri web din toată lumea vând muzică legală (vezi legături utile) și uneori chiar o oferă gratuit! De exemplu, site-urile web prin care muzicienii doresc să le ofere fanilor mostre din muzica lor sau să-și promoveze concertele și albumele.

REGULI DE AUR

- Asigurați-vă că folosiți un site legal pentru a descărca muzică și filme de pe Internet;
- Încurajați-vă copiii să acceseze site-uri web cu conținut legal și explicați-le că nu trebuie să ia drept bun tot ceea ce este pe net;
- Explicați-le riscurile descărcării de materiale de pe net fără a fi precauți;
- Asigurați-vă că aveți computerul protejat și utilizați întotdeauna un program anti-virus actualizat;
- Învățați-vă copiii să salveze pe hard-disk fișiere descărcate legal și să le scaneze de viruși înainte de a le deschide;
- Întotdeauna citiți acordul de confidențialitate, precum și termenii și condițiile de utilizare înainte de a instala ceva. Verificați pe Internet dacă programul pe care doriți să-l descărcați este sigur;
- Închideți ferestrele pop-up nesigure făcând clic pe crucea roșie din colțul din dreapta sus. Nu faceți clic în interiorul acestora.

COPIII ȘI JOCURILE:

- Stabiliți reguli în ce privește perioada de timp pe care copilul o poate petrece pentru a se juca;
- Lasați-vă copiii să se joace în camera în care îi puteți supraveghea;
- Urmăriți-vă copiii cum se joacă. Așa cum îi supravegheați când se joacă afară, de ce n-ați proceda la fel când se joacă în mediul virtual?
- Discutați cu ei conținutul jocului: ce corespunde realității și ce nu, ce le place;
- Înainte de a cumpăra un joc pentru copiii dumneavoastră asigurați-vă dacă are un conținut potrivit vârstei lor (sistemul pan-european PEGI sau orice sistem național de clasificare).

Când copiii dumneavoastră se joacă online cu mulți utilizatori:

- Alegeți site-uri cu reguli stricte și moderatori în direct;
- Avertizați-vă copiii să nu dezvăluie date cu caracter personal altor jucători;
- Avertizați-vă copiii să nu se întâlnească cu alți jucători în mediul nevirtual dacă nu sunt însoțiți de dumneavoastră;
- Încurajați-vă copiii să vă informeze despre cazurile de hărțuire, amenințare sau limbaj nepotrivit, afișarea de conținut dăunător sau invitații de întâlnire în mediul nevirtual;
- Retrageți copilul din joc sau schimbați-i ID-ul dacă constatați că jocul se desfășoară într-un mod care vă deranjează.

LEGĂTURI UTILE

Aflați mai multe despre jocurile online și sistemul de clasificare în funcție de vârstă PEGI: <http://www.pegioline.eu/ro/>

O listă a site-urilor web din toată lumea de unde puteți cumpăra muzică legală:

<http://www.pro-music.org>

Webwise oferă instrumente utile pentru a deveni un internaut precaut în ce privește chat-ul, jocurile și punerea de fișiere la dispoziția altor utilizatori de Internet. Studiați lecțiile interactive împreună cu copiii dumneavoastră (cu conținut în limba engleză):

<http://www.webwise.ie>

Descoperiți și înțelegeți jargonul TXT de pe site-ul web transl8it (cu conținut în limba engleză):

<http://www.transl8it.com>

Deveniți mai informați în ce privește jargonul de pe net vizitând:

<http://www.netlingo.com> (conținut în limba engleză)



C. Soluții propuse pentru activități

1. Paza bună trece primejdia rea



EXPLICAȚII PE MARGINEA ACTIVITĂȚILOR

Potrivește cuvintele cu imaginile corespunzătoare: unitate centrală, mouse-pad, ecran, difuzoare, cameră web, imprimantă, stick USB (sau stick de memorie), mouse, CD-Rom.

Un exercițiu de încălzire pentru a-i familiariza pe copii cu părțile componente ale computerului, precum și cu alte componente hardware. Puteți dezvolta acest subiect dacă îl considerați potrivit.

Roagă-ți părinții să îți trimită un e-mail cu **atașament** sau trimite-ți tu însuși unul. Exersează următoarele: fă clic dreapta pe atașament și salvează-l pe desktopul computerului. Du-te la desktop, fă clic dreapta pe document, iar apoi clic pe scanare. Dacă știi că documentul provine dintr-o sursă sigură, atunci poți să-l deschizi. Nu uita: clic dreapta, iar apoi SALVEAZĂ-SCANEAZĂ-DESCHEDE (SAVE-SCAN-OPEN).

Trimiteți un e-mail la adresa copilului sau la propria dumneavoastră adresă și atașați un fișier. Copilul trebuie să urmeze instrucțiunile din cadrul exercițiului pentru a salva documentul prin clic-dreapta pe el, fără a-l deschide. După salvarea documentului pe Desktop sau într-un dosar al computerului, ca de exemplu My Documents, arătați-i copilului cum să facă clic-dreapta pe docu-

ment încă o dată pentru a-l scana înainte de deschidere. Astfel, încurajați copilul să fie precaut.

Urmează sfaturile Mariei și învață cum să îți descrii **adresa de e-mail** ori de câte ori trebuie să o publici online. Așa vei evita preluarea ei în mod automat și folosirea de către persoanele care trimit spam. De exemplu: cybercat.smith@mymail.com = cybercat punct smith la mymail punct com

Pentru a exersa, descrie adresele de e-mail ale membrilor familiei tale: e-mail-ul tău, al familiei tale, al mamei și al tatălui tău

Pentru a evita colectarea în mod automat a adresei dumneavoastră de către un program care are drept scop distribuirea de spam, descrieți-vă adresa în loc să o scrieți în întregime, așa cum este. Puneți-vă copilul să exerseze această tehnică descrisă mai sus. Totuși, tineți minte că micii utilizatori de Internet trebuie să evite publicarea adresei lor de e-mail pe Internet, iar dacă o fac, atunci trebuie să folosească o adresă care să nu le dezvăluie numele (consultați capitolul „Să comunicăm“).

Pentru a o ajuta pe Teodora să înțeleagă, înainte ca Maria să continue cu explicațiile, uită-te la activitățile din chenar și încercuiește-le pe acelea pe care le poți face doar dacă ești conectat la Internet.

S-ar putea ca unor copii foarte mici să nu le fie clar care activități necesită o conexiune la rețea și care nu. Scrierea unui text nu necesită un computer conectat la Internet, dar desfășurarea unei sesiuni de chat da. Puteți asculta muzică la computer folosind un CD sau un fișier cu muzică stocat pe computerul dumneavoastră, dar puteți să ascultați muzică și direct online. Copiii dumneavoastră trebuie să marcheze numai acele activități pentru care conectarea la rețea este necesară.

Împreună cu părinții tăi tastează adresa <http://edu.genium.ro/> în browser. Căutați informații despre Tyrannosaurus Rex și încercați să aflați când a trăit acest dinozaur. De asemenea, încercați să găsiți o poză potrivită cu acest dinozaur. Nu uitați să verificați informațiile pe trei site-uri diferite.

Învățați copiii cum să caute informații pe Internet, amintindu-le să nu aibă încredere în orice găsesc online. Sfătuiți-vă copiii ca atunci când caută ceva să compare informațiile de pe cel puțin trei site-uri și întotdeauna să menționeze sursele când realizează referate pentru școală.

Împreună cu părinții tăi tastează adresa <http://edu.genium.ro/> în browser. Apoi căutați un subiect anume, de exemplu Tyrannosaurus Rex, și salvați cele trei site-uri pe care le considerați cele mai interesante, făcând clic pe meniul Favorite din partea de sus a paginii browser-ului și adăugați-le la site-urile voastre favorite. Puteți să vă creați și un dosar personal.

Salvarea și organizarea site-urilor interesante în dosarul Favorite este o metodă bună pentru a diminua nevoia copiilor de a căuta informații pe Internet.

VERIFICĂ DACĂ AI ÎNȚELES!

1: (protejat) 2: (virusi), (necunoscuți), (descarci), (stick USB), (infectat), (neprotejat) 3: (ciudat) 4: (necunoscute), (atașamente), (subiecte), (spam) 5: (singur), (spam) 6: (prima), (trei), (compară), (oricine), (publica) 7: (anti-virus), (anti-spyware) 8: (vorbește), (părinții) 9: (spune-le)

SOLUȚII PROPUSE PENTRU SITUAȚIILE DE PE CARDURI

SITUAȚIA 1. Nu naviga niciodată pe Internet în condițiile în care computerul tău nu este protejat de un program anti-virus și anti-spyware actualizat. E ca și cum nu ar exista grăniceri la graniță. Computerul tău ar putea fi infectat de programe dăunătoare, precum: virusi, cai troieni, viermi sau spyware.

SITUAȚIA 2. Fii cu ochii-n patru la e-mail-urile care vin de la persoane necunoscute și conțin atașamente, sau e-mail-uri care îți promit „luna de pe cer”. Cu siguranță că acestea sunt spam. Spam-ul îți poate infecta computerul cu programe dăunătoare, precum: virusi, cai troieni, viermi sau spyware. Nu deschide aceste e-mail-uri, ci blochează expeditorul făcând clic dreapta pe e-mail, apoi selectează ‘Blochează expeditorul’ sau șterge-le pur și simplu.

SITUAȚIA 3. Când cauți informații pe Internet, să nu ai încredere imediat în prima pagină pe care ai găsit-o și care ți se pare bună. Verifică cel puțin trei site-uri diferite și compară informațiile din ele. Nu uita: orice persoană cu acces la Internet poate scrie și publica informații pe net. Când scrii un referat sau o temă, trebuie să menționezi întotdeauna sursa de unde ai preluat informațiile și pozele Așa ar proceda un adevărat om de știință.

2. Să comunicăm



EXPLICAȚII PE MARGINEA ACTIVITĂȚILOR

Marchează cât de **personale** sunt aceste informații: Numărul tău de telefon, Culoarea părului tău, Numele tău, Țara unde locuiești, Școala pe care o frecventezi, Adresa ta, Numele animalului tău de casă, Ocupația părinților, Adresa ta de e-mail, Pozele tale, Vârsta ta.

Au copiii dumneavoastră aceeași percepție cu privire la confidențialitatea datelor personale ca și dumneavoastră? Cele trei culori reprezintă informații foarte confidențiale (roșu), destul de confidențiale (portocaliu) și nu atât de confidențiale (verde).

Ajut-o pe Teodora să creeze singură o parolă, urmând sfaturile Mariei:

Parolele bune trebuie să conțină un set de caractere diferite alese aleatoriu (cifre, litere și semne de punctuație) și trebuie ținute secret.

După modelul Teodorei, crează-ți un profil sigur. După aceea, dă un exemplu de profil nesigur:

Lăsați copiii să-și creeze un profil sigur, iar apoi unul mai puțin sigur care să dezvăluie informații cu caracter personal. Amintiți-le copiilor că un profil sigur nu îi apără dacă nu continuă să-și protejeze datele cu caracter personal când comunică online.

Examinează această poză și scrie lucrurile pe care le poți spune despre această persoană.

Ce informații cu caracter personal pot rezulta dintr-o poză? Copiii nu-și dau seama de puterea imaginilor.

Verificați dacă micii utilizatori de Internet și-au dat seama că se expun riscurilor în cazul contactului cu persoane necunoscute.

Urmează ideea Teodorei și gândește-te la 3 sfaturi pe care le-ar primi „Alex, varianta masculină a Scufiței Roșii” de la Maria, pentru a se proteja împotriva „lupilor” de pe Internet.

Verificați dacă copiii dumneavoastră au înțeles că este periculos să contactezi persoane necunoscute online.

Cum ai dori să fii tratat online? (1..... 2..... 3.....)

Asigurați-vă că micii utilizatori de Internet înțeleg că trebuie să-i trateze pe ceilalți așa cum își doresc să fie ei tratați...

SPARGE CODUL: Află ce înseamnă unele dintre cele mai populare acronime folosite în chat,

încercând să faci legătura cu înțelesul lor:

Aflați mai multe despre acronime consultând capitolul „Să comunicăm”, secțiunea Neticheta, limbajul chat-ului.

Folosește tastatura pentru a ilustra următoarele emoticonițe. O față zâmbitoare – O față tristă – O față care face cu ochiul - Față uimită – Zâmbet larg - Limba scoasă

Pentru mai multe informații consultați capitolul Să comunicăm, secțiunea Neticheta, limbajul chat-ului.

VERIFICĂ DACĂ AI ÎNȚELES!

1: (profilul) 2: (personal), (responsabil) 3: (necunoscuți), (spui) 4: (Neticheta), (respectat) 5: (emoticoniță) 6: (parolă), (punctuație) 7: (secretă) 8: (refuz) 9: (cunoscute)

SOLUȚII PROPUSE PENTRU SITUAȚIILE DE PE CARDURI

SITUAȚIA 4. Când utilizezi Internetul, profilul tău sau informațiile despre tine pot ajunge la zeci, sute, mii sau chiar milioane de oameni. De aceea, este important să alegi cu mare atenție informațiile pe care le furnizezi despre tine. Nu da date personale decât persoanelor în care ai încredere și pe care le cunoști bine în viața de zi cu zi.

SITUAȚIA 5. Probabil că Mihai i-a spus parola de la contul lui de e-mail prietenului, care a profitat de acest lucru și a început să trimită e-mail-uri nepotrivite de pe contul lui Mihai. Nu dezvăluie parolele tale altora, cu excepția cazului în care nu ai nimic împotriva citirii e-mailurilor tale de către alte persoane care ar putea pretinde că ești tu și ar spune lucruri pe care tu niciodată nu le-ai spune!

SITUAȚIA 6. Întâlnirea cu o persoană necunoscută nu este deloc o idee bună. Dacă într-adevăr consideri că poți avea încredere într-un prieten online care dorește să se întâlnească cu tine, spune-le părinților astfel încât să te poată însoți. Cu siguranță că pe niciun prieten adevărat cu intenții oneste nu l-ar deranja acest lucru, ci doar pe cei care au ceva de ascuns.

3. Hărțuirea pe Internet



EXPLICAȚII PE MARGINEA ACTIVITĂȚILOR

Desenează o imagine a invitației pe care a primit-o Alex de la profesori. Indică emblema și sloganul „împotriva hărțuirii” pe care îl folosește școala pentru „Săptămâna împotriva hărțuirii”.

Lăsați-vă copiii să fie creativi și să deseneze în chenarul de pe pagină.

Urmează exemplul lui Alex și menționează cinci motive care te-ar determina să dai cuiva „cartonaș roșu”.

Discutați cu copiii pentru a identifica tipul de comportament pe care îl consideră inacceptabil.

VERIFICĂ DACĂ AI ÎNȚELES!

1: (cinstit), (compromit) 2: (discuți) 3: (justifice) 4: (hărțuirea pe Internet) 5: (blochez) 6: (cunosc) 7: (răspunde)

SOLUȚII PROPUSE PENTRU SITUAȚIILE DE PE CARDURI

SITUAȚIA 7. Acesta este într-adevăr un mod inacceptabil de utilizare a telefonului mobil. Nu trimite mesaje, imagini sau alte materiale care i-ar putea leza pe ceilalți. Întotdeauna tratează-i pe ceilalți așa cum dorești să fii tratat. În astfel de situații dificile, vorbește cu părinții sau cu un alt adult în care ai încredere.

SITUAȚIA 8. Alex ar trebui să-i spună prietenului să nu se învinovățească pentru comportamentul total nepotrivit al celui care-l hărțuiește. Acesta nu ar trebui să răspundă la mesajele celui care îl hărțuiește, ci să le păstreze drept dovezi și să le arate părinților și profesorilor. De asemenea, Alex ar trebui să vorbească cu părinții lui despre această problemă, deoarece aceștia l-ar putea sprijini să-și ajute prietenul.

SITUAȚIA 9. Neticheta reprezintă regulile de conduită pe Internet. Cu alte cuvinte, dacă-i respecti pe ceilalți vei fi la rândul tău respectat. Suntem siguri că ai învățat suficient până acum pentru a o ajuta pe Teodora cu idei legate de tema pentru școală.

4. Divertisment & descărcare



EXPLICAȚII PE MARGINEA ACTIVITĂȚILOR

Deschide motorul de căutare preferat. Tastează în chenarul de căutare „tonuri de apel gratuite“ sau „jocuri gratuite“ și vezi ce site-uri web îți apar pe ecran. **Verifică câteva dintre ele. Poți găsi niște capcane?**

Exersați realizând o căutare folosind cuvintele cheie menționate și verificați site-urile web pe care le găsiți și care conțin capcane de marketing pentru consumatorii neatenți. Observați cum informațiile scrise cu litere de dimensiuni mici sunt omise din reclame.

Care este jocul tău pe computer preferat? Verifică dacă părinții îl cunosc și îl pot descrie. Dacă nu știi nimic despre el, explică-le mai întâi și apoi lasă-i să-l descrie pe scurt. L-au înțeles bine? Câte puncte din zece le acorzi? .../10

Părintele completează rezumând jocul preferat al copilului, iar acesta îl ilustrează printr-o imagine.

Știi ce joacă micii dumneavoastră utilizatori de Internet și care este jocul lor preferat? Lăsați-vă copiii să vă testeze în această privință!

VERIFICĂ DACĂ AI ÎNȚELES!

1: (gratuite) 2: (formularele) 3: (capcană) 4: (ilegale) 5: (cruciulița) 6: (ignori) 7: (personal) 8: (pui la dispoziția altor utilizatori), (tu însuși) 9: (descărca)

SOLUȚII PROPUSE PENTRU SITUAȚIILE DE PE CARDURI

SITUAȚIA 10. O mare parte din muzica și filmele pe care le găsești pe Internet sunt de fapt copii ilegale. În plus, site-urile web unde utilizatorii de Internet pot pune la dispoziția altora muzică și filme sunt de obicei pline de programe dăunătoare, precum: viruși, cai troieni, viermi sau spyware. Cea mai bună soluție pentru Teodora ar fi să aleagă varianta b sau c. Bineînțeles că descărcarea cântecului ei preferat de pe un site respectabil cu muzică

legală o va costa mult mai puțin decât cumpărarea întregului CD. Înainte de a lua o decizie ar trebui să ceară părerea și permisiunea părinților.

SITUAȚIA 11. Există servicii gratuite pe Internet, dar tonurile de apel, imaginile de fundal, fișierele mp3, avatarurile și altele sunt rar gratuite. Dacă Alex se va uita cu atenție pe acel site web, va descoperi probabil niște propoziții scrise cu litere de dimensiuni foarte mici în care se precizează costul real al acestor servicii. Tonurile de apel, concursurile, jocurile etc. sunt modalități de a-i tenta pe utilizatorii de Internet să subscrie la aceste servicii așa-zise „gratuite“, dar care de fapt costă.

SITUAȚIA 12. Alex nu trebuie să furnizeze date personale când se joacă online cu persoane pe care nu le cunoaște dincolo de realitatea virtuală. El n-ar trebui să dezvăluie informații referitoare la orașul în care locuiește, școala pe care o frecventează, numele lui de familie etc. De asemenea, ar trebui să-și informeze părinții despre jocurile pe care le joacă. În plus, n-ar trebui să descarce niciun joc de pe Internet înainte de a-și întreba părinții, deoarece acest lucru ar putea dăuna computerului.



D. Glosar

Acronim: o abreviere formată din primele litere ale cuvintelor care compun o sintagmă sau expresie. Acronimele sunt folosite frecvent de cei care utilizează serviciul de chat pentru a comunica mai rapid. De exemplu: LoL, CU, Btw (consultați capitolul „Să comunicăm“).

Adresă de e-mail: o locație virtuală către care sunt trimise mesajele e-mail. Adresele de e-mail se compun din două părți separate prin simbolul @.

Alertă: o casetă de dimensiuni mici care apare pe ecran cu scopul furnizării de informații sau avertizării cu privire la o potențială avarie care ar afecta computerul. De exemplu: mail-uri noi sau starea actualizării programului de protecție anti-virus.

Anti-spyware: un program care combate spyware. Acesta scanează toate datele primite de programul spyware și apoi blochează atacurile spyware sau pune la dispoziție o listă din care pot fi șterse elementele spyware.

Anti-virus: un program de calculator care încearcă să identifice, să izoleze, să împiedice și să elimine virușii informatici, precum și alte programe dăunătoare. Mai întâi, programul anti-virus scanează fișierele, iar apoi identifică disfuncționalitățile care indică virusarea computerului.

Atașament: un fișier digital care este trimis împreună cu un mesaj e-mail. Adesea, virușii și viermii circulă ca atașamente e-mail. Acestea trebuie considerate suspecte când provin de la expeditori necunoscuți.

Autor: creatorul unei lucrări literare sau audio-vizuale, a unui software etc. Drepturile de autor protejează creațiile autorilor împotriva reproducerii ilegale.

Avatar: profilul unui utilizator reprezentat de un nume de utilizator și o imagine, o pictogramă sau de un personaj 3D din jocurile online sau din mediul virtual.

Bară de unelte: un set de pictograme sau butoane care fac parte din interfața unui program. Bara de unelte este întotdeauna disponibilă și ușor de utilizat pentru executarea unor comenzi.

Blog: prescurtarea de la blog web. Un site web al cărui conținut este generat de un individ sau un grup, de obicei zilnic, și care conține texte, fotografii, fișiere audio-video și legături (link-uri).

Blogging: acțiunea de generare de conținut și actualizare a blog-ului.

Browser: un program utilizat pentru vizualizarea site-urilor web. Internet Explorer, Netscape Navigator și Firefox sunt unele dintre cele mai utilizate browsere pentru Windows, în timp ce Safari este folosit pe Mac. Majoritatea versiunilor recente ale acestor browsere conțin opțiuni tip control parental ingenioase.

Browsing: acțiunea de utilizare a unui browser pentru a vizualiza site-uri web sau doar pentru a naviga pe net.

Cal Troian: malware, program dăunător care poate pătrunde în computer prin intermediul unor operațiuni aparent nerisicante, precum jocuri sau chiar programe de localizare de viruși. Troienii nu se multiplică singuri, dar sunt creați pentru a accesa sau a distruge date. Aceștia pot șterge hard disk-ul sau fura informații cu caracter confidențial.

Cameră de chat: spațiu virtual public pentru comunicare în timp real. Oameni din toate colțurile lumii se pot întâlni în camerele de chat și discuta prin intermediul mesajelor scrise cu ajutorul tastaturii. Dacă micii utilizatori de Internet folosesc camerele de chat, asigurați-vă că acestea se adresează vârstei lor și au moderatori.

Cameră web: camera care se atașează computerului și transmite imagini în timp real, imagini ce pot fi accesate folosind World Wide Web-ul, mesageria instantanee (instant messaging), o aplicație de video conferință pe computer, platforme de chat etc. Camerele web includ o cameră digitală care încarcă imaginile pe un server web continuu sau la intervale regulate.

CD-Rom: un acronim pentru Compact Disc read-only memory. Acesta este un Compact Disc neînregistrabil cu date digitale. CD-ROM-urile sunt îndeosebi folosite pentru distribuirea de software.

Centru de asistență (Hotline): serviciu prin intermediul unei linii telefonice dedicate sau pe Internet unde oamenii se pot plânge de conținutul ilegal întâlnit online și/sau de utilizarea Internetului. Hotline-urile trebuie să dispună de mijloace transparente și eficiente pentru a rezolva aceste reclamații și să aibă sprijinul guvernului, industriei, justiției și a utilizatorilor de Internet din țările respective.

Chat: comunicare sincronă pe Internet prin mesaje scrise, prin utilizarea aplicațiilor chat și mesagerie instantanee (instant messaging) (de exemplu, MSN).

Conexiune la Internet: mijlocul prin care utilizatorii se conectează la Internet. Acest lucru se poate realiza prin: dial-up, T-lines, Wi-Fi, satelit și telefoane mobile.

Confidențialitate: capacitatea unui individ sau a unui grup de a controla fluxul de informații despre ei înșiși selectând datele pe care doresc să le facă publice. Confidențialitatea este uneori legată de anonim – dorința de a nu fi recunoscut în public.

Cont: contul vă permite să vă autentificați prin intermediul unui nume de utilizator și a unei parole, pentru a putea folosi servicii online. Sistemul dumneavoastră de operare vă permite să creați conturi separate de utilizator pentru fiecare membru al familiei.

Cookie: un fișier plasat pe browser-ul dvs. de Internet prin intermediul unui site web. De fiecare dată când accesați site-ul web, cookie-ul este trimis înapoi la server-ul pe care este stocat site-ul de Internet. Cookie-urile informează cu privire la preferințele dvs. în ce privește site-ul și sunt folosite pentru a vă oferi facilități de cumpărare online.

Control parental: vezi definiția pentru setări de familie.

Conținut dăunător: poze, texte, documente, etc. Al căror conținut nu este indicat pentru copii. De exemplu, imaginile care redau scene violente sunt nepotrivite și dăunătoare pentru copii.

Conținut ilegal: conținut online care este considerat ilegal în legislația națională. De exemplu, imagini care redau abuzul sexual asupra copiilor, activitate ilegală în camerele de chat, site-urile web care promovează incitarea la ură și ideile xenofobe.

Cracker: o persoană care în mod ilegal atacă sistemele computerelor.

Crack: a copia în mod ilegal programe comerciale „spărgând” protecția acestora în ce privește drepturile de autor.

Date personale: orice informații cu caracter personal. Colectarea, procesarea și stocarea datelor personale trebuie adusă la cunoștința utilizatorilor în mod explicit.

Descărcare: se referă la procesul de copiere a unui fișier pe computer de la un serviciu online.

Director: o unitate cu rol de organizare pe care computerul o utilizează în scopul administrării și organizării dosarelor și fișierelor într-o structură ierarhică, de exemplu: My Documents, My Pictures etc.

Dosar: o entitate în sistemul de operare care conține un grup de fișiere și/sau de alte directoare. Fișierele pot conține mai multe documente și sunt create pentru organizarea informațiilor.

Dosar Junk/Spam: locul (din cutia de e-mail) unde e-mail-urile considerate a fi spam/junk sunt stocate.

Drept de autor: un set de drepturi cu caracter exclusiv care reglementează folosirea unei idei, a unei lucrări sau a unor informații. Dreptul de autor este reprezentat prin simbolul “©”.

E-mail: mijloc de comunicare electronică în scris care vă permite să trimiteți mesaje cu fișiere atașate care pot conține text, fotografii, material audio etc.

Emoticoniță: o imagine sau o pictogramă folosită pentru a reda stări și sentimente. De exemplu: imagini faciale expresive. Emoticonița poate fi reprezentată prin utilizarea caracterelor standard

ale tastaturii, precum și a semnelor de punctuație sau prin folosirea caracterelor deja create și puse la dispoziție în cadrul camerelor de chat, a jocurilor, a serviciilor de mesagerie instantanee, a telefoanelor mobile etc.

Favorite: dosar în cadrul browser-ului unde pot fi salvate legături (link-uri) interesante. Acestea din urmă pot fi organizate în sub-dosare și/sau salvate folosind anumite cuvinte cheie cu scopul căutării rapide.

Fereastră pop-up: o fereastră care apare pe neașteptate în momentul vizitării unui site web sau al executării unei anumite comenzi cu ajutorul tastaturii. De obicei, ferestrele pop-up conțin un meniu cu comenzi și rămân pe ecran până în momentul în care selectați una dintre comenzi sau o închideți executând clic pe cruciulița din dreapta sus.

Filtru: aplicație care reglează accesul la informații sau servicii de Internet specifice, avertizează împotriva site-urilor web dăunătoare, înregistrează navigarea pe Internet a utilizatorului, blochează site-urile cu conținut dăunător și chiar oprește complet funcționarea computerului. Sistemele de filtrare pot fi instalate pe computere de sine stătătoare, servere, telefoane cu acces la Internet etc.

Filtru spam: o aplicație care blochează mesajele spam pentru a nu fi stocate în cutia dumneavoastră de e-mail.

Firewall: un dispozitiv hardware (integrat în router) sau software (instalat pe computer) configurat pentru a împiedica utilizatorii neautorizați (precum hackeri sau crackeri) să aibă acces la un computer sau la o rețea de computere conectate la Internet.

Fișier: o arhivă/colecție de informații înrudite (documente, programe etc.) stocate în computer sub o denumire. Fișierele reprezintă varianta modernă a documentelor din hârtie care se păstrau în birouri sau arhive.

Flaming: schimbul de mesaje ostile și jignitoare între utilizatorii de Internet. De obicei, apare în cadrul grupurilor de discuții, a Internet Relay Chat (IRC) – program client-server care permite conversații cu persoane de pe Internet, având canale dedicate diferitelor subiecte de interes, sau chiar în mesajele e-mail.

Formular (formular online): un document formatat care conține câmpuri libere pe care le puteți completa cu date. Formularul electronic poate fi completat cu texte libere sau prin alegerea unor anumite date din cele listate sub forma unui meniu drop-down. După completare, datele sunt trimise direct către o aplicație de procesare care le introduce într-o bază de date.

Forum: grup de discuții online în care utilizatorii cu interese comune pot face în mod public schimb de mesaje pe diferite teme.

Freeware și shareware: în general, software-ul este protejat de dreptul de autor și, ca urmare, nu poate fi descărcat. Freeware înseamnă că deținătorul dreptului de autor al software-ului este de acord ca acesta să fie utilizat de oricine în mod gratuit. Shareware înseamnă că deținătorul dreptului de autor al software-ului este de acord ca acesta să fie utilizat de oricine pentru o perioadă de probă. După această perioadă, utilizatorul trebuie să plătească o taxă pentru a putea folosi în continuare serviciul respectiv.

Furt de identitate: furtul datelor personale (de exemplu, nume, data nașterii, numărul cardului de

credit) și folosirea acestora în mod fraudulos.

Hacker: în general este folosit pentru a face referire la o persoană care se ocupă cu „spargerea” computerelor (vezi ‘cracker’). În cercurile utilizatorilor de calculatoare se mai folosește și pentru a face referire la o persoană entuziasă în ceea ce privește computerele.

Hardware: componenta fizică a computerului, diferită de software (programele care indică computerului ce să facă). Aceasta poate fi internă: placa de bază, hard drive-ul și memoria RAM (considerate componente) sau externă: monitor, tastatură, imprimantă etc. (numite și perifericele computerului).

Hărțuire: deranjarea cu insistență prin crearea de neplăceri în mod repetat, prin insulte și amenințări fizice, remarci cu caracter sexual și denigrări comise de unul sau mai mulți agresori.

Hărțuire pe Internet: se referă la hărțuirea online, de obicei prin intermediul mesageriei instantanee și e-mail. Aceasta constă în deranjarea cu insistență prin crearea de neplăceri în mod repetat, prin insulte și amenințări fizice, remarci cu caracter sexual și denigrări comise de unul sau mai mulți agresori. Aceștia pot publica datele personale ale victimelor și chiar își pot asuma identitatea acestora, pentru ca apoi să publice materiale în numele victimelor lor cu scopul de a le calomnia și ridiculiza.

Imagine de fundal: un model, o fotografie sau altă imagine grafică care se utilizează ca fundal pentru ecranul computerului.

Internet: este o rețea internațională publică de rețele de calculatoare interconectate prin care se realizează transmiterea și schimbul de date. Se compune din rețele casnice, de proveniență academică, de business, guvernamentale care oferă diferite servicii: surse de informare, e-mail, chat online, transfer de fișiere etc.

Înregistrare (Sign-up): înscrierea sau înregistrarea la un serviciu online: buletin informativ, forum de discuții, e-mail, platformă chat etc. În mod normal, ar trebui să existe și opțiunea de anulare a înscrierii, pentru ca utilizatorii care doresc anularea înscrierii să o poată face.

Joc online: joc creat de dezvoltatorii de jocuri și care se joacă pe un computer. Jocul online este definit ca un joc digital care necesită o conexiune la rețea în direct pentru a putea fi jucat. Jocurile online permit interacțiunea între mai mulți jucători.

Junk: mesaje e-mail aproape identice, nesolicitate și care sunt trimise oamenilor la adresele lor de e-mail. Întrucât Internetul este public, prea puțin se poate face în sensul prevenirii e-mailurilor junk, așa cum este imposibil de prevenit spam-ul.

Legătură: o trimitere la un document disponibil online (pagină web, document text, fotografie etc.). Când execuți clic pe legătură se face saltul la o pagină nouă sau la un site web complet diferit. Legăturile text sunt de obicei albastre și apar subliniate, dar nu neapărat (pot avea orice culoare și pot fi nesubliniate). Imaginile pot funcționa și ele ca legături pentru alte pagini web.

Linie de asistență (Helpline): un e-mail sau serviciu telefonic pus la dispoziție în câteva țări de către organizațiile care sprijină copiii și de către membrii rețelei Insafe. Copiii își pot exprima îngrijorarea în ce privește conținutul ilegal și dăunător întâlnit pe Internet și pot relata experiențele neplăcute legate de utilizarea tehnologiilor online.

Listă de contacte: o colecție de contacte în cadrul aplicațiilor de mesagerie instantanee, e-mail, jocuri online, telefoane mobile etc. Într-o listă se pot adăuga, respinge și șterge contacte.

Malware: prescurtarea pentru software dăunător. Acesta poate prelua controlul asupra computerului (fără acordul proprietarului) și produce daune și disfuncționalități computerului. Principalele categorii de malware sunt reprezentate de viruși, viermi, troieni, spyware, precum și alte programe dăunătoare.

Manipula: procedura de modificare a unei imagini, a unui fișier, a unei fotografii sau ilustrații în mod evident sau mai puțin evident. În zilele noastre, există numeroase instrumente care pot fi utilizate pentru a influența conținutul sau forma datelor, conducând la un rezultat diferit de realitate.

Mesagerie Instantanee (Instant Messaging sau IM): formă a comunicării electronice simultane și rapide între doi sau mai mulți utilizatori. IM vă permite să comunicați cu cei din lista de contacte aleasă. Când cei din lista dumneavoastră de contacte nu sunt online, sunteți imediat anunțat.

Mobil: dispozitiv electronic de telecomunicație, cunoscut și sub denumirea de telefon mobil, telefon celular, gsm, smartphone sau handphone. Acesta are aceeași utilitate ca și telefonul fix tradițional. În zilele noastre majoritatea telefoanelor mobile au o cameră digitală integrată și multe dintre ele oferă acces la Internet (contra cost).

Motor de căutare: un instrument utilizat pentru a căuta informații cuprinse în site-uri web. Cele mai cunoscute sunt Google și MSN Search. Motoarele de căutare pun la dispoziție opțiuni avansate pentru utilizator care pot include și setări de siguranță extrem de utile.

Mp3: este un format digital de compresie audio. Un mp3 este de aproape zece ori mai mic decât fișierul audio original, dar sunetul este de aproape aceeași calitate ca și pe CD. Datorită dimensiunii mici a fișierelor, precum și a capacității de reținere a majorității detaliilor audio perceptibile, fișierele mp3 au devenit cel mai popular mijloc de stocare a fișierelor cu muzică atât pe computere, cât și pe dispozitivele portabile.

Multiplayer Games (jocurile cu mulți jucători): jocuri care prezintă o lume 3D populată de mii de jucători care își imaginează că sunt personaje de ficțiune și se întrec între ei. Jocurile de rol sunt caracteristice acestei categorii în care participanții creează în colaborare sau joacă anumite roluri.

Net: prescurtarea pentru Internet.

Neticheta: regulile de conduită pe Internet pentru comunicarea online.

Newsgrup: vezi definiția pentru forum.

Nume de utilizator: vezi definiția pentru pseudonim.

Pagină de start: este pagina web care se încarcă automat când se deschide browser-ul web. Termenul se mai folosește și pentru a indica prima pagină sau pagina web principală a unui site (vezi definiția).

Parolă: o serie de caractere secrete care permit utilizatorului să acceseze un fișier, un computer, un cont sau un program. Parola vă protejează contul de utilizatorii neautorizați (vezi capitolul „Să comunicăm“)

Pedofilie online (Grooming): utilizarea camerelor de chat de către pedofili pentru a găsi posibile victime printre copii, pretinzând că sunt de aceeași vârstă cu ei. Aceștia inițiază conversații cu posibilele victime pentru a afla informații privitoare la locul în care se află, interesele, activitățile preferate, precum și experiențele lor sexuale.

Personal: informații (despre un individ sau un grup) care nu trebuie dezvăluite publicului larg. Când ceva aparține unei persoane, de obicei acest lucru este în mod firesc considerat special.

Pornografie infantilă: pornografia infantilă este definită diferit din punct de vedere juridic, în funcție de țară. Pe scurt, aceasta se poate defini ca o imagine înfățișând un copil care este angajat sau prezentat ca fiind angajat într-o activitate sexuală explicită.

Port: interfața utilizată pentru a conecta computerul la alt dispozitiv. Porturile pot fi atât interne, cât și externe. Porturile interne fac legătura cu un disk-drive sau o rețea, în timp ce porturile externe se conectează cu un dispozitiv periferic, ca de exemplu imprimanta sau o tastatura.

Procesor: sau Unitatea Centrală de Procesare este o componentă a computerului care procesează datele, comandă funcțiile principale ale computerului și stochează rezultatele. Împreună cu memoria formează unitatea centrală a computerului.

Profil: informațiile personale ale utilizatorului în spațiul de social networking, în sistemele de mesagerie instantanee (instant messaging), în aplicațiile de chat online, în jocuri online etc. Profilurile pot fi publice sau confidențiale. Acestea sunt personalizate de către utilizatori pentru a-i reprezenta în mediul virtual.

Profil de utilizator: un set de informații care descriu un anume utilizator al programului, al site-ului web sau al altui instrument tehnic. Profilul utilizatorului conține informații, precum: numele de utilizator, parola și alte detalii (de exemplu, data nașterii, pasiuni etc.).

Program de calculator: vezi definiția pentru software.

Proprietate virtuală: un set de obiecte care sunt acordate fiecărui jucător. Aceste obiecte sunt în proprietatea virtuală a fiecărui jucător prin intermediul unui terminal care le afișează.

Pseudonim: sinonim pentru nume de utilizator și poreclă. Acesta îl reprezintă pe utilizatorul unui serviciu online și este ales de acesta. Pseudonimul sau numele de utilizator apare în listele de contact, camerele de chat etc. Dacă este ales bine, acesta vă poate proteja anonimatul online.

Raporta: opțiunea care le permite utilizatorilor din spațiile virtuale publice să reclame o problemă (tehnică, comportament inacceptabil al utilizatorilor, conținut ilegal etc.) unui moderator sau administratorului site-ului.

Recycle Bin (Coș de gunoi): un director al computerului unde fișierele șterse sunt păstrate temporar înainte ca utilizatorii să le șteargă definitiv. Trebuie să vă goliți în mod regulat coșul de gunoi de datele de care nu mai aveți nevoie pentru a obține spațiu liber pe hard-disk – unitatea internă de stocare.

Rețea de la egal la egal (peer-to-peer network sau P2P): rețeaua de la egal la egal (P2P) le permite celor care sunt conectați la ea să facă schimb de fișiere prin procesul de încărcare și descărcare (vezi definiția). Aceasta este doar una din modalitățile prin care se poate face schimb

de fișiere pe Internet. Unele dintre serviciile care permit acest lucru sunt ilegale.

Scana: acțiunea sau procesul de transformare a materialului tipărit în fișiere digitale, prin utilizarea unui scanner. Această transformare vă permite să le vizualizați pe computer ca fișiere electronice și să le trimiteți online.

Schimb de fișiere (File sharing): schimb online de fișiere realizat între utilizatorii de computere. Termenul se referă atât la punerea de fișiere la dispoziția altor utilizatori (încărcare), cât și la copierea pe un computer a fișierelor disponibile pe Internet (descărcare). Schimbul de fișiere se face prin rețelele P2P (de la egal la egal).

Second Life: o comunitate web 3D bine-cunoscută pusă la dispoziție de o companie cu sediul în SUA, numită Laboratoarele Linden. Utilizatorii pot interacționa virtual printr-un avatar, își pot crea diferite medii, pot face comerț și pot câștiga bani virtuali etc. Vezi www.secondlife.com

Setări de confidențialitate: un set de informații cu caracter personal ale contului pe care le puteți edita pentru a îmbunătăți protecția în ce privește dezvăluirea datelor personale, a cookie-urilor etc.

Setări de familie (Family settings): sunt cunoscute și sub denumirea de control parental. Acestea sunt utilizate pentru a configura un browser sau un alt instrument web conform tipului de utilizator – în cazul nostru copiii, prin activarea unor opțiuni, precum: filtru de conținut, limită de timp, supraveghere a jocurilor etc.

Setări de siguranță (profil): un set de opțiuni de siguranță care pot fi particularizate în funcție de profilul dumneavoastră online (vezi definiția). Acestea sunt în special legate de deschiderea fișierelor, identificarea furnizorilor de informații sigure și de gradul de permisivitate în ce privește site-urile pentru adulți.

SIP-Bench: un studiu sprijinit de Comisia Europeană în cadrul căruia au fost testate 30 de instrumente de control parental și anti-spam pentru a le măsura eficacitatea în protejarea copiilor împotriva conținutului dăunător din diferite aplicații de Internet.

Sistem de operare: ansamblu de programe care asigură utilizarea optimă a resurselor fizice și logice ale unui sistem de calcul. Cele mai utilizate sunt: Windows, Linux și Mac OS.

Site-uri de social networking: platforme virtuale care „găzduiesc” comunități ai căror membri au preocupări comune. Aceștia trebuie să-și creeze profiluri de utilizator pentru a putea să utilizeze site-ul: să încarce texte, fotografii sau alte fișiere, să posteze mesaje sau să participe la activitatea de pe forum. Multe site-uri de social networking sunt interzise copiilor sub 13 ani și de aceea pun la dispoziție setări de siguranță în ce privește profilul.

Site web: o locație pe World Wide Web. Fiecare site web conține o pagină de start. Acesta reprezintă primul document vizualizat când intrați pe site. De obicei, site-urile conțin legături către fișiere și site-uri adiționale. Site-urile web sunt create și administrate de persoane fizice, companii sau organizații

Social networking: comunități online ai căror membri au preocupări comune și care comunică și socializează online prin intermediul unor programe și servicii specifice (vezi site-uri de social networking).

Software (Program de calculator): se compune dintr-o secvență structurată de informații scrisă

de programatori care permite computerelor să execute sarcini. Când cumpărați un program software, acesta este cel mai adesea stocat pe un CD-Rom (vezi definiția) - mijloc fizic de stocare a programelor.

Spam: e-mail nesolicitat, de obicei de natură comercială trimis în dosarul Bulk. Trimiterea de mesaje spam este în mod cert unul dintre cele mai cunoscute abuzuri de pe Internet.

Spyware: malware atașat în mod ilegal la fișierele descărcate de pe Internet, care se instalează singur în computer și controlează activitatea. Acesta trimite informații unei terțe părți, adesea companiilor interesate în identificarea profilurilor personale în scopul trimiterii de reclame sau alte informații, sau cracker-ilor care doresc acces la date cu caracter personal.

Stick USB/de memorie: dispozitiv de stocare a datelor integrat într-un conector USB (universal serial bus). Stick-ul de memorie este mic, ușor, amovibil și reinscriptibil.

Transfer de fișiere: transmiterea fișierelor prin intermediul unei rețele. Din perspectiva utilizatorului acesta reprezintă o descărcare sau încărcare de fișiere.

Ton de apel: sunetul telefonului mobil când sunteți apelat. Există o mare varietate de tonuri și muzică disponibile pentru proprietarii de telefoane celulare. Acestea pot fi descărcate (adesea contra cost) și utilizate.

URL (Uniform Resource Locator): adresa de Internet a unui site sau fișier. Aceasta nu conține caractere sau spații speciale. În cadrul adresei, pentru a indica diferite directoare sunt folosite două linii „/” înainte. Prima parte a adresei indică ce protocol se utilizează, iar a doua parte specifică adresa IP sau numele domeniului unde se află resursa.

Versiune de testare (Trial software): software pe care îl puteți încerca înainte de cumpărare. De obicei, versiunile de probă ale programelor includ toate funcționalitățile, dar pot fi utilizate doar pentru o perioadă de timp limitată.

Virus: un program dăunător, de tip malware, creat pentru a se răspândi cu intervenția utilizatorului. De obicei se transmite prin atașamentele de e-mail, dar și prin instrumente de memorie externă (stick USB, CD-Rom).

Vierme: un tip special de virus care are abilitatea de a se replica rapid și răspândi fără intervenția utilizatorului pe multe calculatoare conectate între ele. Acesta produce daune rețelei, consumă foarte multă lungime de bandă, oprește computerul etc.

Voice over Internet Protocol (VoIP): o tehnologie alternativă la rețelele tradiționale de voce care le permite utilizatorilor să vorbească pe Internet, după descărcarea aplicației. Convorbirile pot fi gratuite pentru utilizatorii care se sună prin același client VoIP (de exemplu Skype, Voicebuster). De obicei, aplicațiile de acest gen oferă și servicii de chat, precum și facilități în ce privește schimbul de fișiere.

Web: prescurtarea de la World Wide Web. O colecție de documente online formate în HTML (HyperText Markup Language) care conțin legături către alte documente, precum și imagini, fișiere audio și video. Web-ul face parte din Internet.



E. Legături utile

SISTEMUL EDUCAȚIONAL INFORMATIZAT

Sistemul Educațional Informatizat (SEI) este un program complex inițiat de Ministerul Educației și Cercetării în anul 2001 pentru susținerea procesului de predare-învățare în învățământul preuniversitar cu tehnologii de ultimă oră: <http://portal.edu.ro/>

HOTLINE

Pentru raporta o problemă legată de un conținut de pe Internet pe care îl suspectați a fi ilegal, contactați: <http://www.sigur.info>

LINIA VERDE

Linia verde pentru protecția copilului a fost deschisă în 2001 de Guvernul României prin intermediul Autorității Naționale pentru Protecția Drepturilor Copilului (ANPDC).

**NUMĂRUL DE TELEFON GRATUIT AL LINIEI VERZI ESTE:
08008200200**

ORANGE

Ghid pentru părinți referitor la utilizarea telefoanelor mobile:

<http://www.orange.ro/files/romanian-family-guide-online-appvd.pdf>

WATCH YOUR SPACE

Acest site web furnizează informații și sfaturi adresate adolescenților în ce privește utilizarea în siguranță și în mod responsabil a site-urilor web de social networking, precum: Bebo, MySpace, YouTube etc. <http://www.watchyourspace.ie> (conținut în limba engleză)

WEBWISE

Centrul irlandez pentru noutăți și sfaturi privitoare la securitatea pe Internet. Webwise oferă sfaturi și instrumente pentru părinți și profesori necesare promovării utilizării Internetului în siguranță și în mod responsabil: <http://www.webwise.ie> (conținut în limba engleză)

MAKEITSECURE

makeITsecure este un site de sensibilizare și informare în ce privește problema securității IT, mai exact phishing (fraudare a informațiilor bancare), spyware și furtul identității: <http://www.makeitsecure.ie> (conținut în limba engleză).

INSAFE

Rețeaua europeană care coordonează activitățile de conștientizare a securității pe Internet și care încurajează utilizatorii să folosească Internetul într-un mod pozitiv, sigur și eficient. <http://www.saferinternet.org>



ins@fe



Cu sprijinul:

upc

Titlu: Ghidul securității pe Internet pentru întreaga familie • Creat de Insafe, cu sprijinul Liberty Global/UPC în 2008

Copyright: această lucrare este produsă sub licența Creative Commons Paternitate-Utilizare Non-Comercială – Fără Modificare 3.0 Unported. Pentru a vedea o copie a licenței, vizitați: <http://creativecommons.org/licenses/by-nc-nd/3.0>