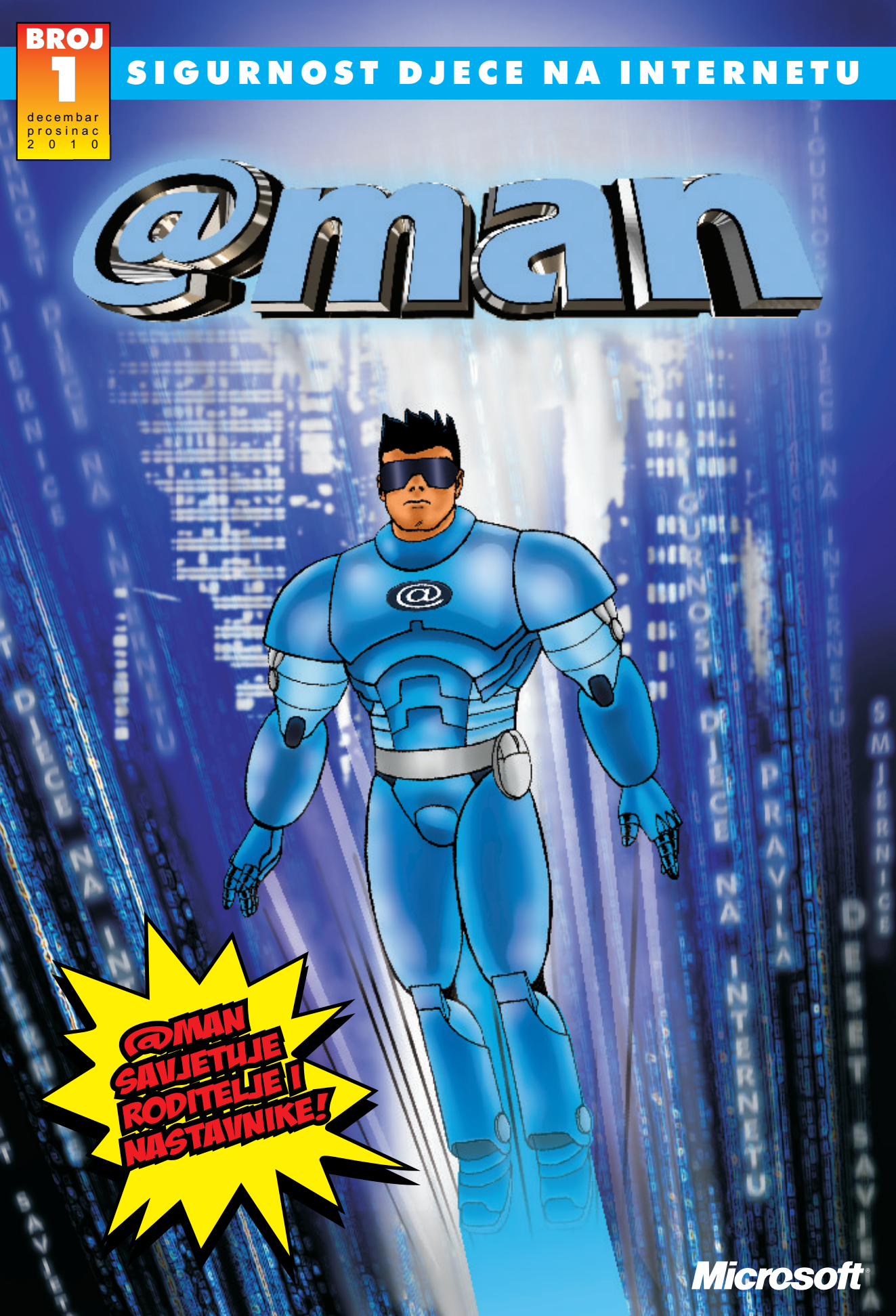
BROJ 1
decembar
prosinac
2010

SIGURNOST DJECE NA INTERNETU

@man



Microsoft

DESET SAVJETA

ZA VEĆU SIGURNOST VAŠE DJECE NA INTERNETU

PRIJE NEGO ŠTO SVOM DJETETU DOZVOLITE DA IDE NA INTERNET (ONLINE) BEZ VAŠEG NADZORA, POBRINITE SE DA STE UTVRDILI GRUPU PRAVILA OKO KOJIH SE SVI MOŽETE SLOŽITI.

AKO NISTE SIGURNI ODAKLE DA POČNETE, EVO NEKIH PRIJEDLOGA O ČEMU DA RAZGOVARATE SA SVOJOM DJECOM KAKO BISTE IH NAUČILI DA NA SIGURNIJI NAČIN KORISTE INTERNET.

1. Podstičite svoju djecu da sa Vama podijele svoja iskustva sa interneta. Uživajte u internetu zajedno sa svojom djecom.

2. Naučite djecu da vjeruju svojim instinktima. Ako su uznemireni ili nervozni zbog bilo čega na internetu, trebaju Vam to reći.

3. Ako Vaša djeca koriste internet usluge za koje je potrebno ime za prijavu kako bi se identifikovali, pomozite im da odaberu to ime i pobrinite se da ono ne otkriva nikakav lični podatak o njima.

4. Insistirajte na tome da Vaša djeca nikada ne otkrivaju Vašu adresu, broj telefona ili druge lične podatke, uključujući i to gdje idu u školu ili gdje se vole igrati.

5. Naučite svoju djecu da je razlika između toga šta je dobro, a šta loše ista na internetu kao i u stvarnom životu.

6. Pokažite svojoj djeci kako da poštuju druge na internetu. Pobrinite se da znaju da se pravila dobrog ponašanja ne mijenjaju samo zbog toga što su za računarom.

7. Insistirajte da Vaša djeca poštuju imovinu drugih na internetu. Objasnite im da je ilegalno kopiranje rada i djela drugih ljudi (muzike, video igara i ostalih programa) jednako kao da su ih ukrali iz prodavnice.

8. Recite svojoj djeci da se nikada ne trebaju sastajati uživo sa osobama koje su upoznali na internetu. Objasnite im da njihov prijatelj kojeg su upoznali na internetu možda nije ona osoba za koju se izdaje.

9. Naučite djecu da nije istina sve što pročitaju ili vide na internetu. Podstičite ih da Vas pitaju ako nisu sigurna.

10. Kontrolišite aktivnost svoje djece na internetu pomoću naprednog internet softvera. Roditeljska kontrola može Vam pomoći da uklonite štetne sadržaje, da pratite sajtove (sites) koje posjećuju Vaša djeca i da saznate šta tamo rade.

Tekst brošure predstavlja adaptaciju i lokalizaciju originalnog teksta na engleskom jeziku objavljenog na: http://www.microsoft.com/protect/.
Ilustraciju teksta razvila LUNA\TBWA\SARAJEVO.

DESET SAVJETA O ZAŠTITI OD IGRAČA VIDEO IGARA KOJI ZLOSTAVLJAJU I MALTRETIRAJU DRUGE IGRAČE

INTERNETSKI NASILNICI (CYBERBULLIES) SU POZNATI POD RAZLIČITIM IMENIMA (TWINKS, SNERTS, CHEESE PLAYERS) I POSTOJE VELIKE ŠANSE DA JE BAREM JEDNOM NEKO OD OVIH NIŠTARIJA MALTRETIRAO I VAŠE DIJETE DOK JE NA INTERNETU IGRALO NEKU OD VIDEO IGARA ZA VIŠE IGRAČA KAO ŠTO SU HALO 2, EVERQUEST, THE SIMS ONLINE, SOCOM, STAR WARS GALAXIES I DR.
IGRAČI KOJI MALTRETIRAJU DRUGE SU VIRTUALNI EKVIVALENT NASILNIKA U ŠKOLSKOM DVORIŠTU KOJI UŽIVAJU U PONIŽAVANJU I UGNJETAVANJU DRUGIH.

Tipični postupci ovog tipa igrača:
Tipični vidovi ponašanja koje pokazuju ovi igrači su: provociranje drugih igrača - posebno početnika, ometanje igrača iz istog tima, korištenje neprimjerenog rječnika, udruživanje s ostalim igračima sličnog profila, blokiranje prolaza, namamljivanje protivnika do drugih igrača ili neki drugi način korištenja igre isključivo radi izazivanja neprijatnosti za pojedine igrače ili uznemiravanja onih koji se usprotive njihovom neprijateljskom ponašanju.
Iako čine tek mali procenat igračke zajednice, igrači koji maltretiraju druge predstavljaju problem za kompanije koje se bave video igrama, jer postoji strah od gubitka korisnika. Kao posljedica toga, mnoge web stranice posvećene igrama, kao i ponuđači usluga iz ove sfere sve manje tolerišu ovakve igrače i koriste nove metode da ih uklone ili ograniče njihovo štetno djelovanje.
Najbolji način za zaštitu od igrača koji maltretiraju druge igrače je da se informišete o njima i objasnite djeci kako da se sami nose s njima. Otvoreni razgovor s Vašom djecom ima važnu ulogu u svakoj aktivnosti koju oni obavljaju na internetu.

1. Ignorišite ih. Ako ih Vaše dijete ignoriše, većina igrača ovog profila će osjetiti dosadu i povući se.
2. Promijenite opcije unutar igre. Dajte djeci da igraju igre koje nude pravila i opcije koje onemogućavaju neke nepoželjne taktike poput eliminisanja saigrača iz istog tima.
3. Kreirajte privatne sesije igranja. Većina novijih video igara za više igrača i sličnih web stranica dopušta igračima da kreiraju privatne sesije igranja u kojima učestvuju samo njihovi prijatelji.
4. Igrajte na web stranicama na kojima važe striktna pravila. Igrajte na web stranicama za igranje na kojim važe pravila ponašanja ili korištenja i na kojima administratori imaju pravo da isključe igrače koji kontinuirano maltretiraju druge.
5. Igrajte nešto drugo. Ako neki igrači ne prestaju maltretirati Vaše dijete, dajte mu da proba neku drugu igru ili da joj se vrati nakon izvjesne pauze.
6. Prijavite greške unutar igre. Zajedno s djetetom pokušajte prepoznati greške koje neki igrači iskorištavaju, kao i metode varanja u igrama. Prijavite ih administratoru web stranice za igranje.
7. Igrajte naslove koji onemogućavaju da jedni igrači maltretiraju druge. Predložite djetetu da proba novije naslove koji nude posebne mehanizme zaštite od ovih igrača, poput mogućnosti njihovog prijavljivanja administratorima, blokiranja poruka ili prekida audio komunikacije, kao i isključivanja nepoželjnih igrača putem glasanja.
8. Ne vodite se poslovicom «klin se klinom izbija». Ne dopustite djetetu da protiv igrača koji maltretiraju svoje saigrače koristi istu taktiku, jer će tako uglavnom samo pogoršati njihovo ponašanje ili, još gore, Vaše dijete će biti svrstano u isti koš s njima.
9. Izbjegavajte korištenje provokativnih imena. Spriječite potencijalne probleme tako što nećete dopustiti Vašem djetetu da koristi korisnička imena ili nadimke («gamertag») koji mogu navesti na maltretiranje.
10. Ne otkrivajte lične podatke. Zlonamjerni igrači (ili bilo ko drugi) mogu koristiti prava imena, brojeve telefona, kućne ili e-mail adrese kako bi dodatno uznemiravali vaše dijete i uzrokovali druge probleme.

DESET SAVJETA ZA

SIGURNIJE KORIŠTENJE INSTANT MESSAGING SERVISA (SERVISA SLANJA ISTOVREMENIH PORUKA)

Komuniciranje uz pomoć programa za instant messaging servis (IM servis - servis slanja istovremenih poruka, npr. MSN messenger) sa sobom povlači iste rizike kao i korištenje elektronske pošte (e-mail), ali u tom slučaju postoji i nekoliko specifičnih vidova opasnosti koje morate imati na umu.

1. Budite oprezni kada kreirate svoje korisničko ime (screen name, user name, user ID). Svaki program za IM od Vas traži da kreirate korisničko ime koje je slično e-mail adresi. Vaše korisničko ime ne bi trebalo odavati ili aludirati na Vaše lične podatke. Na primjer, koristite nadimak "LjubiteljNogometa" umjesto "BayernDamir".

2. Osigurajte se od neželjenih IM poruka. Nemojte ostavljati svoje korisničko ime ili e-mail adresu u javnim zonama (poput velikih web direktorija ili u profilima virtualnih zajednica) ili ih davati nepoznatim osobama. Neki IM servisi prilikom registracije povezuju Vaše korisničko ime sa e-mail adresom. Omogućavanje jednostavnog pristupa Vašoj e-mail adresi može dovesti do toga da primate veću količinu neželjene pošte (spama) i da budete izloženiji phishing napadima (slanje lažnih poruka u kojim se korisnik navodi na otkrivanje ličnih podataka).

3. Nikada ne otkrivajte povjerljive informacije lične prirode poput broja kreditne kartice ili lozinke (password) tokom razgovora preko IM servisa.

4. Komunicirajte samo s ljudima koji su na Vašoj listi kontakata ili prijatelja.

5. Ako poželite upoznati osobu s kojom ste komunicirali preko IM servisa, poduzmite neophodne mjere sigurnosti. Naprimjer, izbjegavajte samostalan odlazak na upoznavanje s njom i uvijek se držite javnih mjesta poput kafića.

6. Nikada nemojte otvarati slike, preuzimati datoteke ili posjećivati linkove (adrese za sadržaje na istoj ili drugoj web stranici) koje vam šalju nepoznate osobe. Ako ih šalje Vama poznata osoba, tražite da vam potvrdi da je e-mail poruka (i prateći dodatak/attachment) stigla iz pouzdanog izvora. U suprotnom je zatvorite.

7. Nemojte slati lične ili privatne poruke preko IM servisa dok ste na poslu. Vaš poslodavac može zadržati pravo da ih pročita.

8. Ako koristite javni računar, nemojte koristiti opciju za automatsko prijavljivanje na sistem. U protivnom će osobe koje budu koristile računar nakon Vas moći vidjeti i iskoristiti Vaše korisničko ime za prijavljivanje na sistem.

9. Pratite aktivnosti Vaše djece i ograničite im korištenje IM servisa. To možete učiniti preko usluge Windows Live OneCare Family Safety. Operativni sistem Windows 7 u svom paketu sadrži set alata za roditeljski nadzor nad računarom.

10. Ako trenutno niste u mogućnosti pratiti primljene poruke, obratite pažnju na način na koji ćete tu informaciju obznaniti drugim korisnicima. Moguće je da, naprimjer, ne želite da svako na Vašoj listi kontakata zna da ste "Otišli na ručak" ("Out to lunch").

Smjernice za korištenje interneta za djecu različitog uzrasta

AKO VAŠA DJECA KORISTE INTERNET KOD KUĆE, VI VEĆ ZNATE KOLIKO JE VAŽNA NJIHOVA ZAŠTITA OD NEPRIMJERENIH SADRŽAJA I KONTAKATA.

DJECA MLAĐA OD DESET GODINA

Alati poput **Windows Live Family Safety** (https://fss.live.com/safety/default.aspx) i **Roditeljski nadzor** (http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx) predstavljaju sastavni dio operativnih sistema Windows 7 i Windovs Vista i mogu Vam pomoći u kreiranju sigurnijeg internetskog okruženja za Vašu djecu.

Djecu ovog uzrasta morate držati pod stalnim nadzorom. Možete koristiti alate za sigurnost na internetu kako biste im ograničili pristup pojedinim sadržajima, web stranicama i aktivnostima, kao i aktivno kontrolisati korištenje interneta od strane Vašeg djeteta, ali @man Vam preporučuje da, kada se radi o djeci ovog uzrasta, sjedite uz njih dok se služe internetom. Ovdje su navedeni neki od savjeta za kontrolu korištenja interneta za djecu uzrasta između dvije i deset godina:

1. Nikada nije prerano za uspostavljanje otvorene i pozitivne komunikacije s djecom. Preporučljivo je s djecom razgovarati o računarima i biti susretljiv prema njihovim pitanjima i radoznalosti.
2. Budite uz djecu ovog uzrasta sve dok ona provode vrijeme na internetu.
3. Postavite jasna pravila za korištenje interneta.
4. Zabranite djeci da osobama koje upoznaju na internetu ostavljaju lične podatke na internetu, poput pravog imena, adrese, broja telefona ili lozinki (password).
5. Ako se na nekoj web stranici traži unošenje imena radi prilagođavanja web sadržaja pojedincu, pomozite djeci da kreiraju nadimke u kojima neće biti sadržani njihovi lični podaci.
6. Koristite alate za porodičnu sigurnost kako biste kreirali odgovarajuće profile za svakog člana i tako olakšali filtriranje internet sadržaja.

SVI ČLANOVI PORODICE TREBAJU POSLUŽITI KAO UZOR DJECI MLAĐEG UZRASTA KOJA TEK POČINJU KORISTITI INTERNET.

Više informacija o ovim alatima potražite na:
https://fss.live.com/safety/default.aspx (Porodična sigurnost na servisu Windows Live),
http://www.microsoft.com/windows/windows-7/features/parental-controls.aspx
(Roditeljski nadzor u okviru operativnog sistema Windows 7)
http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx
(Roditeljski nadzor u okviru operativnog sistema Windows Vista).
Zaštitite djecu od agresivnih pop-up (skočnih) prozora uz pomoć alata za njihovo blokiranje koji je sastavni dio pretraživača Internet Explorera: http://www.microsoft.com/windows/internet-explorer/default.aspx

DJECA UZRASTA OD 11 DO 14 GODINA

DJECA OVOG UZRASTA POSJEDUJU VIŠE ZNANJA O KORIŠTENJU INTERNETA, ALI JE I DALJE PREPORUČLJIVO PRATITI I KONTROLISATI NJIHOVE INTERNETSKE AKTIVNOSTI KAKO BI SE OSIGURALO DA NE DOĐU U KONTAKT S NEPRIMJERENIM SADRŽAJIMA. MOŽETE SE POSLUŽITI ALATIMA ZA SIGURNOST NA INTERNETU KAKO BISTE IM OGRANIČILI PRISTUP SADRŽAJIMA I WEB STRANICAMA I PRATILI NJIHOVE AKTIVNOSTI NA INTERNETU. OBJASNITE DJECI KOJE LIČNE PODATKE NE SMIJU OTKRIVATI NA INTERNETU.

Kad se radi o djeci ovog uzrasta, stalna fizička kontrola njihovih aktivnosti na internetu nije najpraktičnije rješenje. Možete koristiti alate poput **Windows Live Family Safety** (https://fss.live.com/safety/default.aspx), **Windows 7 Parental Controls** (http://www.microsoft.com/windows/windows-7/features/parental-controls.aspx), **Windows Vista Parental Controls** (http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx). Ovdje su navedeni neki od savjeta za kontrolu korištenja interneta za djecu uzrasta od 11 do 14 godina:

Smjernice za korištenje interneta za djecu različitog uzrasta

1. Preporučljivo je uspostaviti otvorenu i pozitivnu komunikaciju s djecom. Razgovarajte s djecom o računarima i budite susretljivi prema njihovim pitanjima i radoznalosti.
2. Postavite jasna pravila za korištenje interneta.
3. Zabranite djeci da osobama koje upoznaju na internetu ostavljaju lične podatke, poput pravog imena, adrese, broja telefona ili lozinki.
4. Ako se na nekoj web stranici traži unošenje imena radi prilagođavanja web sadržaja pojedincu, pomozite djeci da kreiraju nadimke u kojima neće biti sadržani njihovi lični podaci.
5. Koristite alate za porodičnu sigurnost kako biste kreirali odgovarajuće profile za svakog člana i tako olakšali filtriranje internet sadržaja. Više informacija o ovim alatima potražite na:
    a. Windows Live Family Safety (https://fss.live.com/safety/default.aspx),
    b. Windows 7 Parental Controls (http://www.microsoft.com/windows/windows-7/features/parental-controls.aspx),
    c. Windows Vista Parental Controls (http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx).
6. Podesite postavke alata za porodičnu sigurnost na srednji nivo zaštite koji djelimično ograničava pristup nekim sadržajima, web stranicama i aktivnostima.
7. Računare koji su spojeni na internet postavite na vidljiva mjesta s kojih možete lako pratiti aktivnosti Vaše djece.
8. Zaštitite djecu od agresivnih pop-up (skočnih) prozora uz pomoć alata za njihovo blokiranje koji je sastavni dio Internet Explorera: http://www.microsoft.com/windows/internet-explorer/default.aspx.

Podstičite djecu da Vam kažu ako ih nešto ili neko uznemirava ili im prijeti. Sačuvajte prisebnost i objasnite djeci da neće imati problema zato što su vas obavijestili o tome. Pohvalite ih i posavjetujte ih da urade isto ako dožive nešto slično.

TINEJDŽERI UZRASTA OD 15 DO 18 GODINA

OVDJE SU NAVEDENI NEKI OD SAVJETA ZA KONTROLU KORIŠTENJA INTERNETA OD STRANE TINEJDŽERA:

Tinejdžeri bi trebali imati gotovo neograničen pristup sadržajima, web stranicama i aktivnostima koje se nude na internetu. Oni već znaju dosta toga o internetu , ali ih roditelji i dalje moraju podsjećati o smjernicama za njegovo sigurno korištenje. Roditelji moraju biti u mogućnosti da pomognu svojoj djeci ovog uzrasta da shvate šta su neprimjerene poruke i da izbjegavaju rizične situacije. Preporučljivo je da roditelji podsjećaju tinejdžere na to koje lične podatke ne bi smjeli ostavljati na internetu.

1. Nastavite održavati otvorenu i pozitivnu komunikaciju koja se tiče upotrebe računara i interneta. Razgovarajte o njihovim virtuelnim životima, prijateljima i aktivnostima, na isti način kao i o drugim vrstama prijatelja i aktivnosti. Podstičite ih da Vam kažu ako ih nešto ili neko uznemirava ili im prijeti. Također im recite da, ako im se čini da na internetu nešto nije u redu s nečim ili nekom osobom, obavijeste druge o tome.

2. Kreirajte listu kućnih pravila za korištenje interneta. Navedite koje web stranice su zabranjene, vrijeme kada se internet smije koristiti, informacije koje se ne smiju ostavljati na internetu, kao i uputstva o komunikaciji s drugim korisnicima interneta, uključujući i društvene mreže.

3. Računare koji su spojeni na internet postavite na vidljivo mjesto, a ne u dječju sobu.

4. Probajte i alate za kontrolu pristupa internetu (kao što su Windows Live Family Safety (https://fss.live.com/safety/default.aspx), Windows 7 Parental Controls (http://www.microsoft.com/windows/windows-7/features/parental-controls.aspx), Windows Vista Parental Controls (http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx) kao potencijalnu pomoć u roditeljskom nadzoru.

5. Zaštitite djecu od agresivnih pop-up (skočnih) prozora uz pomoć alata za njihovo blokiranje koji je sastavni dio Internet Explorera: http://www.microsoft.com/windows/internet-explorer/default.aspx.

6. Saznajte koje web stranice posjećuju Vaša djeca, kao i s kim razgovaraju. Savjetujte ih da koriste chat sobe koje se nadziru, kao i da ne napuštaju javne chat sobe.

7. Odgovarajte ih od susreta s osobama koje upoznaju preko interneta.

8. Zabranite im da s interneta skidaju programe, muziku ili datoteke bez vaše dozvole. Razmjena datoteka i preuzimanje teksta, slika ili umjetničkih radova s interneta može predstavljati zakonom kažnjivo kršenje zakona o autorskim pravima.

9. Razgovarajte s djecom o seksualnim i pornografskim sadržajima i uputite ih na korisne web stranice koje se bave zdravljem i seksualnošću.

10. Pomozite im da se zaštite od spama (neželjene elektronske pošte, više na: http://www.microsoft.com/protect/fraud/spam/email.aspx). Objasnite im da ne ostavljaju svoje e-mail adrese na internetu, kao i da ne odgovaraju na spam poruke i da koriste filtere za e-mail.

11. Saznajte koje web stranice posjećuju Vaša djeca. Ne dopuštajte im da posjećuju web stranice s neprimjerenim sadržajima i da na internetu ostavljaju lične podatke. Pripazite i na fotografije Vaše djece i njihovih prijatelja koje oni postavljaju na internet.

12. Naučite ih šta je odgovorno i etično ponašanje na internetu. Internet im ne bi trebao koristiti za ogovaranje, nasilje i prijetnje drugima.

13. Objasnite im da se moraju konsultovati s vama prije nego obave neku finansijsku transakciju putem interneta, uključujući i naručivanje, kupovinu ili prodaju različitih artikala.

14. Porazgovarajte s njima o kockanju preko interneta i potencijalnim opasnostima koje ono nosi sa sobom. Podsjetite ih na činjenicu da je kockanje preko interneta zabranjeno osobama njihovog uzrasta.

Vodič o sigurnosti na internetu za nastavnike

Glavne napomene

Internet je izvanredan alat koji djeca mogu koristiti za istraživanje i učenje o svijetu koji ih okružuje. Nastavnici također moraju imati na umu da je "tehnološka pismenost" učenika jedan od preduslova za njihovo buduće uspješno nošenje sa zahtjevima današnje umrežene ekonomije. Program No Child Left Behind predviđa da škola pomogne svakom učeniku u "prevazilaženju digitalnog jaza" i osigura "tehnološko opismenjavanje svakog učenika do završetka osmog razreda".

Iako internet našoj djeci nudi nevjerovatne mogućnosti za učenje, on ih istovremeno izlaže izvjesnim opasnostima i problemima, poput krađe identiteta, neprimjerenih sadržaja i seksualnih ponuda, zlostavljanja i uznemiravanja. Jasno je da obrazovanje koje vodi tehnološkom opismenjavanju mora uključiti i poduku o takvim opasnostima i zaštiti od njih, kao i razvijanje dobrih navika jednog građanina interneta (pojam kojim se označava član internetske zajednice), poput poštovanja privatnog vlasništva i prihvatanja osnovnih normi prihvatljivog oblika ponašanja u ophođenju s drugima.

Sigurnost na internetu - Seksualne ponude i ostale opasnosti

Prema studiji koju su proveli Nacionalni centar za nestalu i izrabljivanu djecu i Univerzitet u New Hampshireu, svako sedmo dijete je tokom korištenja interneta dobilo neku vrstu seksualnih ponuda. Iako su roditelji i nastavnici uglavnom svjesni ovog problema, djeca često ne shvataju ozbiljnost spomenute opasnosti. U istoj studiji se navodi da djeca vjeruju da 43% ovih ponuda dolazi od drugih tinejdžera, dok 66% djece ovakve ponude nisu uplašile niti uznemirile.

Jasno je da edukacija o sigurnosti na internetu mora uključiti savjete o "sigurnom ponašanju" koje može pomoći u zaštiti djece od neželjenih vidova komunikacije i ponuda i podučiti ih o primjerenim "strategijama reagiranja" u ovim slučajevima, od čega je najvažnija ona koja se tiče obavještavanja odraslih o situacijama neugodnim po djecu. Osim toga, djeca moraju biti svjesna važnosti zaštite ličnih podataka, poput imena, koliko imaju godina i koja im je adresa, te im se mora pomoći u razvijanju navika koje će umanjiti rizik koji sa sobom nose različite aktivnosti na internetu, poput pisanja blogova, uključivanja u društvene mreže itd.

Vodič o sigurnosti na internetu za nastavnike

Sigurnost na internetu - Zaštita od krađe identiteta i drugih finansijskih prevara

Učenici mogu biti i žrtve krađe identiteta i internetskih prevara. Prema podacima Savezne trgovinske komisije SAD-a, 5% žrtava krađe identiteta u 2006. godini bili su korisnici mlađi od 18 godina, dok su u najbrojnijoj skupini žrtava krađe identiteta u istoj godini bili korisnici starosne dobi od 18 do 29 godina.

Djecu je potrebno podučiti o važnosti opreznog korištenja ličnih podataka na internetu, posebno onih najvažnijih, poput matičnog broja građana i broja kreditnih kartica. Ona moraju shvatiti značaj posjedovanja kvalitetne lozinke (password), opasnosti koju predstavljaju virusi i načina prepoznavanja phishing prevara (lažnih poruka u kojim se korisnik navodi na otkrivanje ličnih podataka) i pharming napada (preusmjeravanje konekcije s legitimne web stranice na neku lažnu web stranicu). Djecu treba obučiti da u virtualnom svijetu postanu snalažljivi, skeptični i osviješteni korisnici, a ne naivne žrtve osoba s kojima dolaze u kontakt putem interneta.

Internetska zajednica (internet citizenship) - Podsticanje odgovornog ponašanja tokom korištenja interneta

Prema studiji koju su proveli Nacionalni centar za nestalu i izrabljivanu djecu i Univerzitet u New Hampshireu, broj slučajeva uznemiravanja preko interneta porastao je za 50% između 2000. i 2006., a u 44 % njih, žrtve su uznemiravane od strane svojih vršnjaka. Studija organizacije PEW pokazala je da je trećina svih tinejdžera koji koriste internet bila žrtva nasilja preko interneta (cyber-bullying). Još neki od problema su: virtuelne zajednice u kojima se podstiče antisocijalno ponašanje poput korištenja narkotika, kockanja i klađenja preko interneta, kao i rašireno nepoštovanje privatnog vlasništva.

Učenicima je potrebno objasniti da se pravila koja postoje u nevirtuelnom tj. "realnom" svijetu jednako tako uvažavaju i na internetu. Tu spada i poštovanje osjećaja i ličnog integriteta drugih korisnika interneta. Nasilje i uznemiravanje na internetu jednako su neprihvatljivi kao i isti vidovi ponašanja u školskom dvorištu i mogli bi biti i kažnjivi zakonom. Učenici koji su žrtve takvog ponašanja moraju znati kako da prijave takve slučajeve odraslima. Istovjetno, krađa je uvijek krađa, bilo da se radi o nezakonitom skidanju materijala s interneta ili krađi CD-a ili DVD-a iz dućana. Djeci i naročito tinejdžerima mora se skrenuti pažnja na važnost njihovog ličnog integriteta, kao i na činjenicu da se informacije koje iznose u sobama za chat i na društvenim mrežama nalaze u javnoj domeni i da mogu imati potencijalno negativan učinak na njih u kasnijim fazama života.

Korisni izvori informacija

Dodatne materijale o sigurnosti na internetu možete dobiti besplatno ili po simboličnim cijenama putem organizacija specijalizovanim za tu oblast:

i-SAFE www.isafe.org/channels/?ch=ed
WiredSafety www.wiredsafety.org/educators.html
NetSmartz www.netsmartz.org/overview/statepartnerships.htm

Dodatne informacije o edukaciji o sigurnosti na internetu možete pronaći na web stranici američke organizacije National Cyber Security Alliance http://www.staysafeonline.info/