SIGURNOST DJECE NA INTERNETU

Internet djeci i mladima nudi fantastične mogućnosti otkrivanja, povezivanja i stvaranja. No, pri korištenju Interneta postoje i rizici.

Kako roditelji mogu djeci pomoći da ublaže te rizike? Nema jednostavnog odgovora – rizici su različiti i ovise o uzrastu djeteta i poznavanju rada na računalu.

Najvažnije je osobne podatke na računalu učiniti sigurnima, tj. zaštiti računalo od virusa i stalno nadograđivati softver. Postavkama filtra i mogućnostima filtriranja sadržaja dostupnim u većini programa možete poboljšati sigurnost podataka koje vaša djeca korist

Naravno, važno je da računalna oprema radi ispravno. Internet je djeci i mladima prije svega društveno okruženje u kojem mogu sresti prijatelje, ali i nepoznate osobe. Na mreži možete biti uznemiravani, doživjeti nasilje ili čak zloupotrebu. Od presudne je važnosti djecu obavijestiti o opasnostima na Internetu tako da se ponašaju na siguran način te biti na raspolaganju za razgovor o svim problemima na koja djeca nailaze tijekom korištenja Interneta.

Postupno izgradite povjerenje

Roditelji se suočavaju s istim izazovima bez obzira na to radi li se o Internetu ili drugim djetetovim hobijima. Iznimno je važno da roditelji znaju čime se njihova djeca bave i da podržavaju djecu u njihovim aktivnostima.

Djeca će možda htjeti sačuvati privatnost vezanu uz korištenje Interneta. Možda neće htjeti da roditelji imaju uvid u njihovo korištenje Interneta – posebno ako misle da će im roditelji ograničiti korištenje Interneta. Važno je zapamtiti da je Internet odličan resurs s mnogo uzbudljivih i obrazovnih informacija. Važno je i izbjegavati neprimjerene reakcije ili prevelika ograničenja vezana uz korištenje Interneta od strane djece. Rizike treba razumjeti tako da djeca ostanu sigurna i dobiju najbolje od tog sjajnog alata. Djeca uče eksperimentiranjem, metodom pokušaja i pogrešaka. Ako ste zainteresirani za korištenje Interneta i upoznati sa sjajnim stvarima koje nudi, bit ćete u mnogo boljem položaju tijekom razgovora s djetetom o korištenju Interneta. Bit će vam i lakše ustanoviti kako dijete koristi Internet, što će, nadamo se, dovesti do stalnog dijaloga tijekom tinejdžerskog razdoblja života djeteta.

Što više znate o načinu na koji dijete koristi Internet, lakše će vam biti prepoznati i objasniti što je prihvatljivo i sigurno. Vaše dijete može biti vrlo sposobno u radu s tehnologijom, ali životno iskustvo odrasle osobe je nezamjenjivo kada dijete treba shvatiti kako se ponašati u virtualnom svijetu

Savjeti:

Postavite računalo u sobu koju koristi čitava obitelj

Na taj način razgovaranje o Internetu i praćenje korištenja postaje dio svakodnevice. Jednostavnije je razgovarati o problemima kada je računalo u zajedničkoj prostoriji. Možete i zajedno koristiti Internet.

Razgovarajte o Internetu

Pokažite interes za ono što vaše dijete radi s prijateljima, na mreži i izvan nje. Razgovarajte o divnim i uzbudljivim stvarima za koje možete koristiti Internet te o problemima na koje je moguće naići. Razgovarajte s djetetom o tome što učiniti ako naiđe na neugodne situacije na mreži.

Naučite više o korištenju računala

Ako koristite Internet, lakše ćete odrediti što je dobro za vaše dijete i pomoći pri traženju korisnog materijala na mreži.

Koristite Internet zajedno

Pronađite web-mjesta namijenjena djeci ili naučite pronalaziti korisne informacije – zajedno isplanirajte putovanje, iskoristite obrazovna web-mjesta za pisanje domaće zadaće ili pronađite informacije o hobijima ili interesima djeteta. Zajedničkim pretraživanjem Interneta možete pomoći djetetu da procijeni informacije koje pronađete. Omiljena web-mjesta možete obilježiti da bi djetetu za ponovni posjet bio potreban samo jedan klik.

Dogovorite se s djecom o tome kako i kada koriste Internet

Preporučuje se dogovor vezan uz određeno vrijeme tijekom kojeg će dijete koristiti Internet te uz web-mjesta koja smije posjećivati. O tome morate razgovarati s djecom i doći do zajedničke odluke.

Korištenje Interneta je sigurno sve dok na umu imate tri osnovne stvari:

1 Zaštita računala

Održavajte operacijski sustav ažurnim.

Koristite protuvirusni program.

Koristite vatrozid.

Stvarajte sigurnosne kopije važnih datoteka.

Budite pažljivi pri preuzimanju sadržaja.

2 Zaštita na mreži

Budite pažljivi pri objavljivanju osobnih podataka.

Imajte na umu s kim razgovarate.

Imajte na umu da na mreži nije sve pouzdano i da nisu svi iskreni.

3 Poštivanje pravila

Morate se pridržavati zakona, čaki na Internetu.

Vodite računa o drugima i o sebi kada ste na mreži.

Kućna pravila korištenja Interneta

Dobar način za smanjivanje opasnosti na Internetu je određivanje pravila u dogovoru s djecom. Zajednička pravila dobar su početak razgovora o sigurnom korištenju Interneta.

- Vrijeme provedeno za računalom trebalo bi ograničiti iz zdravstvenih razloga.
- Računalo, na primjer, postavite u dnevni boravak. Odrasla bi osoba trebala biti uz djecu predškolskog uzrasta tijekom korištenja Interneta.
- Pristup Internetu djeci predškolskog uzrasta trebao bi biti ograničen na unaprijed određena web-mjesta. Naprednija djeca mogu poznata web-mjesta pronaći putem izbornika "Omiljena web-mjesta“ u internetskom pregledniku.
- Najsigurnije rješenje je stvaranje osobnog radnog okruženja za dijete u kojem je pristup Internetu ograničen samo na određena web-mjesta.

Internet sadrži materijale koji su neprikladni za djecu. Veći dio tih materijala možete blokirati korištenjem raznih filtara. Imajte na umu da ta tehnologija nije jedini način zaštite djece od neprikladnog sadržaja na mreži.

Siguran prostor

Najsigurniji način na koji djeca mogu istraživati Internet jest stvaranje sigurnog prostora ili područja u kojem se dopušta korištenje samo web-mjesta koja su odobrile pouzdane odrasle osobe. Postavke preglednika možete koristiti da biste djetetu dopustili pristup sigurnim web-mjestima koja sami odredite. U tom slučaju, ako dijete želi posjetiti novo web-mjesto, najprije morate na popis odobrenih web-mjesta dodati adresu mjesta.

U operacijskom sustavu morate stvoriti osobni korisnički račun za dijete. Na taj ćete način djetetu definirati prava pristupa i postavke internetskog preglednika.

Programi za filtriranje

Programi za filtriranje omogućuju ograničavanje pristupa internetskim mjestima na temelju sadržaja. To znači da program sprječava pristup mjestima koja sadrže materijale definirane kao štetne (pornografija, nasilje itd.).

Ograničavanje dolaznih kontakata

Broj osoba s kojima dijete kontaktira putem Interneta možete ograničiti putem filtra ili tehnologija blokiranja.

Povijest stranica

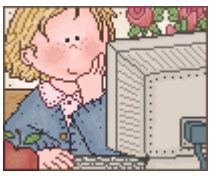
Značajka "Povijest stranica" internetskog preglednika omogućuje pregledavanje mjesta koja su ostali korisnici nedavno posjetili. (No, povijest stranica jednostavno je izbrisati).

Savjet:

Što učiniti ako vaše dijete naiđe na neugodan ili neprikladan materijal na Internetu?

– Izbjegavajte neprimjerene reakcije da bi vam dijete i u budućnosti skrenulo pažnju na slične situacije.
– Naglasite djetetu da to nije njegova krivnja.
– Izbrišite tragove neprikladnog materijala – uključujući reference iz predmemorije preglednika, kolačiće i povijest stranica.
– Razgovarajte s djetetom o načinima izbjegavanja sličnih iskustava u budućnosti uključujući pretraživače prilagođene djeci i brisanje poruka e-pošte od nepoznatih osoba.

RASPRAVE NA MREŽI popularan su način komunikacije između djece. U sobama za razgovor uvijek je netko s kim mogu razgovarati. Razgovor na mreži može biti zabavan i siguran ako znate brinuti se o svojoj sigurnosti. Prije nego počnu razgovarati na mreži, djeca moraju biti svjesna mogućih rizika i znati kako komunicirati s drugima da mogla zaštiti svoj identitet.



Nadimci jamče zaštitu

Ljudi često koriste nadimke na Internetu da bi zaštitili svoj pravi identitet. Razgovor uz korištenje nadimka je siguran: nitko ne može stupiti u kontakt s vama ako ne otkrijete svoje osobne podatke za kontakt. No, takva anonimnost može ljude navesti da se ponašaju nedolično te da koriste nedoličan jezik. Skupine za raspravu često podrazumijevaju skupinu redovitih korisnika.

Lozinke su tajne

Da bi sudjelovali u razgovorima na mreži, korisnici često moraju stvoriti osobni profil ili identitet. To je opis korisnika, na primjer, identifikator ili nadimak koji se koristi u razgovoru. Profili su obično zaštićeni lozinkama radi sprječavanja korištenja identiteta drugih osoba. Lozinke uvijek moraju biti tajne.

Osobna privatnost – što treba, a što ne treba reći o sebi?

Razgovor na mreži omogućuje djeci razgovor s ostalom djecom i stjecanje novih prijatelja, a to podrazumijeva i dijeljenje nekih informacija o sebi. Na mreži ne bi trebalo otkrivati osobne podatke koji omogućuju identifikaciju djeteta niti informacije o kontaktu (puno ime, adresu i broj telefona). Da biste zaštitili svoju privatnost na mreži, morate znati i kako se informacije koje navedete mogu koristiti. Osoba se može identificirati i povezivanjem različitih vrsta podataka koje pružite (na primjer, ime škole, sportski klub, područje u kojem živite i ostalo).

Budite oprezni kada otkrivate podatke za kontakt ili druge osobne podatke. Sve fotografije koje pošaljete ili osobni podaci koje otkrijete nepoznatoj osobi mogu postati dostupni svima na Internetu. Dnevnici na mreži mogu se učiniti dostupnim za javnost u čitljivom obliku dugi niz godina. Kada se tekst ili fotografija objave na Internetu, gubite kontrolu nad njima. Moguće ih je jednostavno kopirati na mnoga različita mjesta, a možda ih se nikada neće moći ukloniti.

Zapamtite:

- Razgovarajte s djecom o opasnosti koju nosi odavanje osobnih podataka.
- Preporučuje se da se osobni podaci u mnogim različitim situacijama ne dijele.
- Nemojte nikome odavati svoju lozinku, čak ni dobrim prijateljima. Potrebno je i redovito mijenjati lozinku.
- Internet je javno mjesto. Prije nego objavite informacije ili fotografije o sebi (i drugima), zapamtite da tim informacijama svatko može pristupiti. Da biste saznali koje su informacije o vama dostupne na Internetu, koristite preglednik i svoje ime kao pojam za pretraživanje.
- Djeca moraju razgovarati sa svojim roditeljima o svim negativnim iskustvima na mreži.

E-POŠTA rasprostranjen je način slanja poruka putem Interneta, ali važno je koristiti je pažljivo.

Pretinci ulazne e-pošte mogu se napuniti neželjenom ili bezvrijednom poštom, često u obliku poruka s reklamama koje nisu uvijek adresirane na vas. Uz rizik od virusa u takvim porukama e-pošte, neželjena pošta može sadržavati i materijal ili veze sa sadržajem neprikladnim za mlade.

Što možete učiniti:

Nabavite filtar za bezvrijednu poštu

Preporučujemo da djetetu stvorite adresu e-pošte davatelja internetskih usluga koji nudi automatiziranu zaštitu od virusa i filtriranje bezvrijedne pošte. Na taj se način sprječava većina bezvrijedne pošte.

Dopustite samo pošiljatelje koje poznajete

Vjerojatno najsigurniji, iako ograničavajući, način korištenja e-pošte jest podešavanje postavki tako da vaše dijete ima pristup samo porukama s određenih adresa. Većina programa za e-poštu dopušta blokiranje poruka poslanih s određenih adresa e-pošte.

Razmislite o korištenju anonimne adrese e-pošte

Adrese e-pošte obično su ime.prezime@domena.hr. Puno ime je osobni podatak i ne biste ga trebali javno objavljivati. Ako dijete želi razmijeniti adresu e-pošte s kontaktima na mreži, najbolje je koristiti adresu e-pošte koja ne otkriva puno ime, npr. nadimak01@domena.hr. Preporučuje se da adrese e-pošte sadrže brojčanu vrijednost jer je njih teže "pogoditi", a na taj se način dobiva manje bezvrijedne pošte. Ne savjetuje se korištenje istog nadimka dva puta u sobama za razgovor. Tu je vrstu adrese e-pošte lakše i zatvoriti ako dobivate previše bezvrijedne pošte ili neželjenih poruka. Veze široke propusnosti obično sadrže nekoliko adresa e-pošte.

Što je razgovor?

Razgovor se odnosi na otvorene skupine za raspravu na Internetu u kojima možete razgovarati s drugim korisnicima u stvarnom vremenu koristeći nadimak. Grupe za razgovor ili sobe za razgovor obično imaju nazive prema temi ili uzrastu skupine. U raspravi može sudjelovati više korisnika, ali često su mogući i privatni razgovori između dva korisnika. Razgovor ima svoj jezik, pravila ponašanja, čak i kulturu. Bilo bi dobro da roditelji saznaju nešto više o tim pravilima razgovora. Preporučuje se da to učine uz pomoć djeteta.

Sigurni razgovori – upute

Djeca koja koriste razgovor moraju znati kako to činiti sigurno. Svako dijete mora proučiti sljedeća pravila razgovora.

1. Osobni podaci moraju biti na sigurnom te moraju biti tajni.
2. Obavijestite administratora razgovora ako vas netko uznemirava.
3. Ako vam nije ugodno, napustite sobu za razgovor.
4. Recite roditeljima ako doživljavate neugodnosti.
5. Budite obzirni prema drugim ljudima tijekom razgovora.

Što je siguran razgovor?

Koliko je razgovor siguran i zabavan, najviše ovisi o osobi s kojom razgovarate. Sigurnost sobe za razgovor koju vaše dijete koristi obično možete odrediti na temelju sljedeća tri pitanja:

1. Je li soba za razgovor namijenjena djeci?
U sobama za razgovor namijenjenima djeci vjerojatnost neprikladnih tema i kontakata je manja.

2. Postoji li administrator sobe za razgovor?
Ponekad postoje dobrovoljni administratori soba za razgovor koji reguliraju neprikladnu komunikaciju i koji osobama koje uznemiravaju ostale mogu blokirati pristup sobi za razgovor. Ako nadzor nije aktivan, soba za razgovor trebala bi barem imati gumb za javljanje administratoru. Sobe za razgovor s administratorom bolje su za djecu, a povećava se i sigurnost tijekom čuvanja razgovora.

3. Je li moguće blokirati pristup osobama?
Da. Blokiranje podrazumijeva zabranu postavljanja poruka u sobu za razgovor određenim osobama. Kada je osoba blokirana, njezine se poruke više ne prikazuju na zaslonu.

Privatni razgovor

Kada upoznate novu osobu u grupi za razgovor na mreži, možda ćete htjeti prijeći s javnog razgovora na privatni razgovor. U sobi za razgovor možete, na primjer, početi u javnoj sobi, a zatim prijeći na razgovor razmjenom neposrednih poruka ili poruka e-pošte. Kada koristite te alate, svoj identitet još uvijek možete zaštititi korištenjem nadimka. Tu je vrstu adrese bolje objaviti i ako zaključite da s novim kontaktom ne želite komunicirati. Preporuka za djecu jest da se ne upuštaju u privatne razgovore na mreži s osobama koje ne poznaju u stvarnom životu.

Sastanak s kontaktima

Kada vaše dijete upozna novu osobu na mreži, možda će htjeti upoznati je uživo. Čak i ako se prijateljstvo na mreži održava neko vrijeme, važno je biti pažljiv prilikom sastanka. Ako je sastanak dogovoren, dijete obavezno mora biti u pratnji roditelja ili druge odrasle osobe od povjerenja. Važno je i dogovoriti sastanak na javnom mjestu. Preporučuje se i da roditelji unaprijed razgovaraju s djecom o sastancima s kontaktima s mreže.

Razmjena neposrednih poruka (MSN Messenger, ICQ itd.)

Kao i sobe za razgovor, program za razmjenu neposrednih poruka omogućuje razgovor u stvarnom vremenu. Jedina je razlika mogućnost odabira osoba s kojima želite razgovarati. Program prikazuje koji vaši prijatelji su trenutno na mreži, a jednog ili više njih možete pozvati na privatni razgovor. Možete i dijeliti datoteke kao što su fotografije, audio ili videozapisi, zajedno igrati igre ili upućivati telefonske ili videopozive.

Tehnologija razmjene neposrednih poruka nosi sa sobom iste rizike kao i e-pošta i razgovor. Korisnik može otvoriti datoteku privitka ili vezu koja sadrži virus, špijunski softver ili materijal sa sadržajem neprikladnim za djecu. Ako drugu osobu poznajete u "stvarnom životu", razgovor na mreži je mnogo sigurniji. Razgovori razmjenom neposrednih poruka uvijek su privatni, a vi ne kontrolirate samo s kim razgovarate, nego i trajanje razgovora.

Rasprave možete učiniti sigurnijim ako postavke programa za razmjenu neposrednih poruka podesite kao što je navedeno u nastavku.

Kada prvi put koristite program, morate odrediti svoj korisnički profil. Nemojte koristiti podatke koji vas identificiraju jer će vaš profil vidjeti svi korisnici. Većina grupa za razgovor i igara na mreži zahtijevat će stvaranje korisničkog profila. Na njih se odnose iste upute.

Odabir osoba za komunikaciju

Razgovaranje je najsigurnije s osobama koje već poznajete. No, vašem djetetu svatko može poslati poruku. Ti programi imaju popis kontakata koji vam omogućuje dodavanje imena korisnika s kojima želite razmjenjivati poruke. Da biste spriječili da vaše dijete dobiva poruke od nepoznatih osoba, postavke programa možete prilagoditi tako da blokiraju kontakt sa svim osobama koje nisu na popisu.

Neka vam dijete pokaže popis kontakata i kaže koga poznaje u "stvarnom životu", a koga je upoznalo na mreži. Na taj ćete način bolje znati s kim vaše dijete razgovara na mreži.

Čuvanje razgovora

Razgovore na mreži možete sačuvati. Ako ostali korisnici vide da to radite, na taj način možete povećati sigurnost svog djeteta. Ako ljudi razgovaraju na mreži i znaju da se razgovori čuvaju, obično su pažljiviji tijekom razgovora. Možete čuvati pojedinačne razgovore ili podesiti program da automatski čuva sve razgovore.

Razmjena neposrednih poruka (IM) – zabava za cijelu obitelj

Razmjena neposrednih poruka nije namijenjena samo djeci i mladima: velik broj tvrtki koristi neposredne poruke za komunikaciju između zaposlenika. Na primjer. Ako se vaše dijete povezuje s mrežom kada dođe iz škole, a vi ste na poslu, možete međusobno razmjenjivati poruke i smanjiti troškove telefonskog računa. Možete pratiti i kako dijete koristi Internet – program za razmjenu neposrednih poruka će vas obavijestiti kada se vaše dijete prijavi.

KAKO EDUCIRATI DIJETE O SIGURNOSTI NA INTERNETU

Najčešći rizici i opasnosti

Od brojnih rizika i opasnosti za djecu, koji su danas svakodnevno prisutni na Internetu, izdvojit ćemo nekoliko najčešćih.

Online komunikacija

Sobe za online razgovor (engl. chat rooms), elektronska pošta te brojni programi za razmjenu poruka u realnom vremenu (MSN, ICQ, Yahoo!Messenger i sl.) pružaju priliku za praktički neograničenu audio-vizualnu komunikaciju. Na Internetu je dostupan gotovo svatko, neovisno o dobi, spolu, nacionalnosti te raznim preferencijama. S jedne strane djetetu se time pruža prilika za nova prijateljstva i poznanstva, ali istovremeno postoji i velika opasnost od zlouporabe djetetove naivnosti, mladosti i neiskustva. Najopasnije zlouporabe su slijedeće:

- online predatori

  Online predatori naziv je za osobe koje koriste anonimnost Interneta te navedene komunikacijske alate kako bi uspostavili online odnos s djetetom te ga potom zloupotrijebili. Predatori postepeno privlače dječju pažnju i naklonost nudeći im ljubaznost, srdačnost, razumijevanje za njihove probleme, pa čak i poklone. Potom postepeno uvode neprimjerene slikovne seksualne materijale u razgovore te navode djecu na razgovor o takvim temama u svrhu vlastitih nemoralnih potreba.

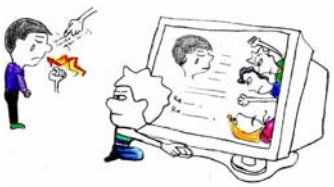
  U težim slučajevima, online predatori uspijevaju dijete nagovoriti i na pravi, oči-u-oči sastanak, što po dijete može završiti kobno. Najrizičnija skupina su mladi adolescenti koji se nalaze u osjetljivom dobu kada istražuju svjou seksualnost, udaljavaju se od nadzora roditelja te traže nove veze i poznanstva izvan obitelji. Skrivajući se pod maskom anonimnosti, traže odgovore na svoja pitanja nesvjesni opasnosti koja ih vreba...

- kršenje privatnosti

  Ovaj način zlouporabe koristi navedene komunikacijske alate kako bi od djeteta izvukao privatne informacije. Najčešće pitanje koje se postavlja djeci u brojnim sobama za online razgovor je njihova dob, spol i mjesto stanovanja. Otkrivajući te podatke neznancima, djeca se dovode u direktnu opasnost od raznih oblika iskorištavanja poput slanja pornografskih sadržaja. Kršenje privatnosti može se manifestirati i na razne druge načine, poput zahtijevanja privatnih informacija prilikom registracije na različite web portale, popunjavanje formulara i anketa i sl.

- cyber bullying

  Bullying je pojam koji označava metode maltretiranja, zastrašivanja i zlostavljanja djece od strane drugog djeteta ili skupine djece. Bullying se manifestira kroz više oblika: fizički, emocionalni, verbalni, seksualni ili cyber bullying. Posljednje navedeni oblik koristi upravo Internet i njegove već spomenute komunikacijske alate za navedenu svrhu. S obzirom na raširenost Interneta, taj način bullyinga raste eksponencijalno i potrebno mu je posvetiti posebnu pozornost.

  U zadnje vrijeme posebno je aktualan blog (internet dnevnik), kao alat pomoću kojega dijete zlostavljač, lažno se predstavljajući upravo kao zlostavljano dijete, piše online dnevnik i služi se brojnim neistinama i lažnim pričama kako bi povrijedio osjećaje i diskreditirao drugo dijete, kojim se ujedno predstavlja.

Pretraživanje web sadržaja

Osim navedenih rizika i opasnosti korištenja raznih alata za online komunikaciju te mogućih zlouporaba, jednako opasnim pokazuje se i tzv. „surfanje“, odnosno pregledavanje raznih web sadržaja putem web preglednika. Svi smo svjesni da je Internet osim nenadmašnog izvora informacija i znanja, ujedno i izvor nevjerojatno velikog broja sadržaja koji su u potpunosti neprimjereni djeci. Slijede tipični primjeri takvih materijala:

- pornografski sadržaji

  Pornografski sadržaji danas su strahovito rašireni na Internetu, a po nekim procjenama zauzimaju i preko 25% ukupnog web prostora. Dostupnost ovih sadržaja je velika pa često slobodan pristup imaju i djeca. Studije pokazuju da mlađi uzrasti djece koji slučajno naiđu na takve sadržaje najčešće to iskustvo doživljavaju uznemirujućim. Na adolescente, koji su često u namjernoj potrazi za takvim sadržajima, utjecaj također često može biti negativan. Naime, pristup raznim devijantnim i nasilnim oblicima seksualnih sadržaja može imati vrlo loš utjecaj u seksualnom razvoju adolescenta.

Pornografska online industrija izuzetno je razvijena, konkurencija je žestoka te se stoga konstantno izrađuju nove strategije kako sadržaj nametnuti korisnicima, makar i na ilegalan način. Promjena početne stranice web pretraživača, razni načini reklamiranja (npr. putem pop-up prozora), socijali inženjering, beskonačne petlje pornografskih sadržaja, samo su neke od čestih strategija.

- nasilni sadržaji i sadržaji poticanja mržnje

Općem porastu prikazivanja eksplicitnog nasilja u medijima poput televizije, video igara i glazbe pridružio se i Internet. Djeca su izložena nebrojenoj količini nasilno orijentiranih web sadržaja koji variraju od web stranica crnog humora pa do web stranica isključivo posvećenih sadizmu, načinima torture i sl. Primjeri takvih web sadržaja poput www.rotten.com ili www.gorezone.com koji sadrže stvarne slike mjesta nesreće, torture, osakaćenja, nažalost su izrazito popularni među adolescentima i studentima.

Uz nasilje, široko dostupni su i sadržaji koji potiču mržnju i netrpeljivost, poput npr. ekstremno rasističkih, homofobnih i sl. Čak i sadržaji koji za cilj imaju ismijavanje (npr. www.uglypeople.com) i naoko se čine bezopasnima, mogu loše pridonjeti razvoju djeteta te njegovim stavovima. Nevjerovatno je da su neki od takvih sadržaja isključivo namjenjeni djeci, kao npr. dječje stranice Ku Klux Klana na kojoj se mogu pronaći djeci prilagođene informacije o cjelokupnoj ideologiji, praktični savjeti o provođenu iste u djelo i sl. Količina i evidentna štetnost ovakvih sadržaja potiču na dodatan oprez.

- dezinformacijski sadržaji

Opće je poznato da je Internet slobodan medij kojeg je izuzetno teško, tj. gotovo nemoguće kontrolirati. Kao poseban problem na površinu izlazi teškoća verifikacije web sadržaja. Kako pouzdano znati da je neka informacija na Internetu točna ili nije? Kojim izvorima vjerovati? Navedeni problem postaje još veći kada su u pitanju djeca s obzirom na njihovu mladost i neiskustvo.

Varijanti dezinformacijskih sadržaja je mnogo, na primjer: web stranice koje potiču mržnju i ekstremne stavove kao normalne, web stranice koje promoviraju i prodaju lažne ili loše i štetne proizvode, web stranice koje osobna mišljenja predstavljaju kao činjenice, web stranice s lažnim informacijama o virusima, prevarama, novčanim piramidama i sl.

Neželjena elektronička pošta (SPAM)

Većinu današnje elektronske pošte u svijetu čini spam – neželjena pošta. Osim brojnih opasnosti koje spam nosi (više pročitajte ovdje), za djecu je dodatno opasan spam koji prenosi grafičke pornografske sadržaje. Količina i eksplicitnost takvih sadržaja nemaju granica te to roditeljima predstavlja sve značajniji problem. Manje problematične su poruke koje razni spam filteri mogu automatski očistiti ili one koje u svom naslovu vrlo jasno daju do znanja o kakvom se sadržaju radi. No uvijek će se naći i one koje će pobjeći najboljim filterima i zavarati krajnjeg korisnika. Osim eksplicitnih sadržaja, često se u porukama mogu pronaći i linkovi na dodatne sadržaje iste vrste ili pak na specijalizirane sobe za online komunikaciju.

Online kockanje i klađenje

Web sadržaji za online kockanje i klađenje izuzetno su opasani i rizični za djecu, a istovremeno sve popularniji i učestaliji. Standardnom klađenju u kladioničarskim poslovnicama djeca često neće imati pristup zbog zakonske regulative koja brani takve radnje maloljetnicima. No online klađenje nema takva ograničenja te na taj način ostavlja otvorena vrata djeci. Jednako vrijedi i za kockanje i slične sadržaje igara za novac. S obzirom da djecu iznimno privuče ideja brze i lake zarade, najčešće se odlučuju na krađu roditeljskih debitnih i/ili kreditnih kartica za uplatu inicijalnih ili dodatnih uloga. Ukoliko se problem na vrijeme ne uoči i identificira, moguće su dugoročne štetne posljedice na budućnost djeteta.

Ovisnost o Internetu

Kao i svaka druga ovisnost, ovisnost o Internetu nije dobra niti zdrava. Makar dijete koristilo Internet isključivo u edukacijske svrhe (što je iznimno rijedak slučaj), nikako nije dobro da provodi prevelike količine vremena pred ekranom. U najvećem broju slučajeva, Internet ovisnost izazivaju alati za online komunikaciju, online igre te čak i pornografija.

Roditeljima je danas sve veći izazov u dnevnoj rutini njihove djece uspostaviti zdravu ravnotežu između vremena provedenog za zabavu te onog iskorištenog za ostale aspekte njihovog života. Pojava Interneta taj je zadatak dodatno otežala kao i činjenica da djeca boraveći na Internetu često u potpunosti gube pojam o vremenu. Problem se najčešće ne uočava dok nije već vrlo kasno i stoga je potrebno pokušati čim prije reagirati.

Najrizičniju skupinu čine djeca koja su sramežljiva, introvertna te usamljena. Dječaci pokazuju posebnu sklonost online igrama u kojima se u potpunosti uživljavaju u online likove te iako se čini da je online interakcija s tisućama druge djece u redu, ona najčešće dovodi do dodatne izolacije djeteta i otuđenje od „stvarnog“ društva.

Kako educirati dijete o sigurnosti na Internetu

Slijedi nekoliko savjeta koji mogu pomoći prilikom edukacije djeteta o sigurnosti na Internetu:

1. Po mogućnosti, koristite Internet zajedno sa djecom te ih potičite da dijele svoja Internet iskustva s Vama.
2. Dajte djeci do znanja da na Internetu postoje određene opasnosti slične onima u stvarnom svijetu (npr. pričanje s nepoznatom osobom) te ih podučite da koriste svoje instinkte i razum u izbjegavanju spomenutih. Naglasite opasnost od lažnih prijatelja te objasnite da obavezno izbjegavaju sastajanje uživo sa takvima.
3. Ukoliko razni online sadržaji traže od djece podatke za registraciju, podučite ih da ne otkrivaju osobne informacije bez nadzora.
4. Inzistirajte da djeca nikad bez nadzora ne odaju Vašu adresu, broj telefona, školu koju pohađaju, svoju sliku, mjesta gdje provode slobodno vrijeme i sl.
5. Upozorite djecu da se pravila pristojnog ponašanja iz pravog života jednako primjenjuju i na ponašanje na Internetu.
6. Poučite djecu poštivati tuđu imovinu na Internetu i objasnite im da je neovlašteno kopiranje glazbe, igrica i ostalih programa identično krađi u dućanu.
7. Objasnite djeci da sve što vide i pročitaju na Internetu nije nužno istina. Potaknite ih da popričaju s Vama o svojim dilemama.
8. Bez obzira na navedene preporuke, ne suspržite se od zaštite Vaše djece putem odgovarajućih programskih alata te postavki operativnog sustava. Microsoft također nudi rješenja za roditeljsku zaštitu, a nešto više o njima čitajte u nastavku ove lekcije.

Praktične preporuke za poboljšanje sigurnosti djece na Internetu

Microsoft intenzivno radi na rješenjima za poboljšavanje sigurnosti djece na Internetu. Iako nema programskog rješenja koje se može mjeriti sa roditeljskom brigom i komunikacijom s djetetom, svejedno se toplo preporuča da iskoristite programska rješenja koja mogu znatno smanjiti opasnosti i rizike koji svakodnevno vrebaju djecu na Internetu.

Slijedi nekoliko preporuka o načinima zaštite djetetove privatnosti te sigurnosti:

1. Odredite koji je sadržaj trenutno primjeren djetetu
   Najefikasniji način zaštite od neprimjerenih i neželjenih sadržaja je njihovo blokiranje, tj. zaustavljanje prije nego dospiju na računala. Microsoft u tom pogledu nudi nekoliko efikasnih programskih rješenja:

> Windows Vista Family safety settings

Ukoliko posjedujete novi Micorsoftov operativni sustav, Windows Vista, kao roditelj imate mogućnost odabira sadržaja koji je pogodan djetetu ovisno o njegovoj dobi, zrelosti i osobnim uvjerenjima. Vista nudi brojne opcije roditeljske zaštite koja omogućava roditeljima da jednostavno kontroliraju, definiraju i uređuju način korištenja računala od strane djeteta.

Neke od mogućnosti Vista Parental Control-a su: kontrola i blokiranje neprimjerenog web sadržaja, razna vremenska ograničenja korištenja računala od strane djeteta, ograničavanje zabavnih igara ovisno o njihovom tipu i primjerenosti uzrastu, blokiranje ostalih programa na računalu neprimjerenih djetetu te konačno - razni izvještaji o aktivnosti djeteta na računalu (pregledavani web sadržaji, količina vremena provedenog na Internetu, količina primljene el. pošte, sugovornici u online komunikaciji i sl.).

> Windows Live OneCare Family Safety

Ukoliko još nemate novu Windows Vistu, dijete od neprimjerenih sadržaja možete zaštititi koristeći i ovo programsko rješenje koje će omogućiti filtriranje informacija ovisno o dobi djeteta. Moguće je limitirati pretrage putem pretraživača, blokirati ili dozvoliti određenu web stranicu te pratiti djetetovu aktivnost na Internetu. Dodatno, roditelj dobija pristup brojnim uputama i savjetima kako pomoći djetetu da sigurno komunicira na Internetu te pregledava samo primjerene sadržaje za njegovu dob. Windows Live OneCare Family Safety dostupan je na sljedećoj adresi - https://fss.live.com/.

2. Povećajte sigurnost i zaštite privatnost

Uz blokiranje neprimjerenih sadržaja, korisno je blokirati i web stranice koje mogu eventualno biti rizične po pitanju sigurnosti i privatnosti.

> Kreirajte različite korisničke račune

Operativni sustavi Windows XP i Windows Vista omogućavaju kreiranje više različitih korisničkih računa (User Accounts) za jedno računalo. Roditelj bi svakako trebao imati Administrator korisnički račun sa punom kontrolom nad računalom, dok bi djeca trebala imati limitirane korisničke račune (Limited User Account). Na taj način, onemogućava se da se za vrijeme djetetova korištenja računala instaliraju nove računalne komponente ili programi, uključujući igre, nove programe za online komunikaciju ili programe za reprodukciju raznih multimedijalnih sadržaja.

>Podesite traženi stupanj sigurnosti i privatnosti u web pregledniku

Internet Explorer ima mogućnost kontrole zaštite sigurnosti i privatnosti putem postavljanja zahtjevane razine sigurnosti i privatnosti za web stranice koje se pregledavaju. Preporučuje se upotreba zadnje generacije preglednika (Internet Explorer 7) zbog brojnih sigurnosnih nadogradnji i mogućnosti podešavanja, poput npr. Phising filtera.

3. Pratite koje web sadržaje djeca posjećuju

Bilo korištenjem opcije History u web pregledniku ili pak putem izvještaja Windows Vista Parental Controls, pratite web sadržaje koje dijete posjećuje i time si omogućite pravoremenu reakciju.

4. Podsjetite djecu da ne komuniciraju s nepoznatim osobama

Iz brojnih spomenutih razloga, online komunikacija djece s nepoznatim osobama može biti vrlo opasna. Podsjećajte djecu na to, a istovremeno podesite Windows Messenger na način da dozvoljava komunikaciju samo sa dozvoljenim (approved) kontaktima. Blokiranje nepoznatih kontakata u Windows Messengeru vrši se u nekoliko koraka:

- iz izbornika odaberete Tools
- zatim Options
- zatim karticu (engl. tab) Privacy
- u Allow listu dodajte sve poznate kontakte, a ostale blokirajte

Nasilje na mreži

Internet otvara nove mogućnosti za uznemiravanje. Na Internetu je moguće objaviti glasine, fotografije ili druge osobne podatke te poslati zlonamjerne poruke – anonimno ili pod tuđim imenom. SMS poruke i mobilni telefoni s fotoaparatom otvaraju nove mogućnosti za zabavu, ali i za zloupotrebu. Nasilje u školi obično je ograničeno na vrijeme provedeno u školi, ali putem Interneta žrtve su dostupne u bilo koje doba. Postoji i veći broj potencijalnih žrtava na mreži. Ako vaše dijete vrijeme provodi razgovarajući na mreži, o tim opasnostima porazgovarajte na samom početku. Dobro je navesti i postupke u slučaju da dijete bude izloženo uznemiravanju.

To je važno zbog sljedećih razloga:

- Nasilje na mreži često se događa kada odrasli nisu prisutni.
- Djeca obično smatraju da će se stvari pogoršati ako kažu roditeljima.
- Anonimnost i smanjeni rizik od identificiranja ljude obično potiču da učine nešto što inače ne bi (da kažu, na primjer, nešto što inače drugoj osobi ne bi rekli u lice).
- Nasilje na mreži tehnički je lako izvesti. Slanje zlonamjerne poruke ili prikazivanje zlonamjernog teksta velikom broju korisnika zahtijeva samo nekoliko klikova mišem.

Savjet:

Čak i ako vaše dijete nije doživjelo uznemiravanje na Internetu, savjetujemo vam da razgovarate s njim:

-Nemojte dijeliti svoje podatke za kontakt ili osobne stvari, npr. fotografije, bez razmišljanja o posljedicama. Prijateljstvo na mreži može završiti, a kada se to dogodi, osobni podaci mogu biti poslani neodgovarajućim osobama.

-Svatko ima pravo da se prema njemu odnose s poštovanjem na Internetu.

-Uvijek možete zatvoriti razgovor i e-poštu ili isključiti računalo.

-Djeca bi trebala s roditeljima razgovarati o lošim iskustvima.

Djeca i oglašavanje na Internetu

Internet tvrtkama pruža učinkovit način da dopru do djece i mladih. Zato se mnoštvo proizvoda za mlade oglašava na Internetu.

Što možete učiniti:

- Koristite Internet zajedno s djetetom i naučite dijete da prepoznaje oglašavanje i njegove ciljeve.
- Obavijestite Udrugu potrošača ili davatelja usluga o neprikladnom oglašavanju.

Usluge podložne naplati i kupnja na mreži od strane djeteta

Svaku kupnju putem Interneta ili mobilnog telefona mora izvršiti ili odobriti odrasla osoba.

Savjeti:

-S djetetom dogovorite pravila o kupnji putem Interneta.

-U dogovoru s davateljem usluga podesite odgovarajuće zabrane za telefon ili SMS poruke ili ograničite iznos na djetetovu računu za mobilni telefon.

-Stvorite obiteljsku adresu e-pošte koju ćete vi i vaše dijete koristiti za kupnju putem mreže.

Osobni podaci i fotografije djeteta na Internetu

Mi smo se u obitelji dogovorili da roditelji uvijek provjeravaju pouzdanost internetskih usluga prije nego djeca pošalju bilo kakve podatke na web-mjesto. Obično nije potrebno unositi sve informacije iz zahtjeva, stoga djeci preporučujemo da ispunjavaju samo obavezna polja.

Od korisnika se na velikom broju web-mjesta traži da se registriraju ili da na neki drugi način ostave svoje osobne podatke da bi osvojili nagrade, npr. pristup usluzi, sudjelovanje u nagradnom izvlačenju, besplatne proizvode ili mogućnost sudjelovanja u grupi za razgovor. Tvrtke mogu prikupljati podatke za kontakt od djece i mladih u marketinške svrhe, ali moraju na zakonit način dobiti odobrenje prije bilo kakvih marketinških aktivnosti.

No, administratori web-mjesta ne štite uvijek povjerljivost osobnih podataka, iako su ti podaci zaštićeni Zakonom o zaštiti podataka. Naučite djecu da budu pažljiva pri davanju osobnih podataka.

Savjeti:

Dogovorite pristup s djetetom

Često je korisno dogovoriti se s djetetom oko načela davanja osobnih podataka na Internetu. Ako djetetu dopustite da ostavlja takve podatke, morate se uvjeriti u pouzdanost mjesta na kojem će ostaviti podatke.

Provjerite smjernice za zaštitu privatnosti

Savjetujemo vam da provjerite ima li usluga odgovarajuće smjernice za zaštitu privatnosti koje objašnjavaju na koji se način informacije koriste, razdoblje i svrhu korištenja.

Ostavite samo obavezne informacije

Obično je dovoljno navesti samo obavezne informacije. Kada se registrirate za novu uslugu, davatelj usluga obično pita dopuštate li izravno oglašavanje. Možete odabrati mogućnost "Ne", ali ako slučajno date odobrenje, obratite se davatelju usluga da biste ga otkazali. Preporučuje se stvaranje obiteljske adrese e-pošte koju ćete vi i vaše dijete koristiti za davanje osobnih podataka na mreži.

Osobne podatke nemojte čuvati u pregledniku

Ne preporučuje se čuvanje osobnih podataka ili lozinki u internetskom pregledniku ili drugim programima povezanima s Internetom.

Programi za filtriranje nepoželjnih web stranica i ostalih sadržaja omogućit će vam da djetetu dopustite korištenje računala kraće vrijeme bez vašeg direktnog nadzora.

Kad odlučite dijete ostaviti samo za računalom i omogućiti mu pristup internetu, nužno je ograničiti pristup programima i sadržajima koji nisu pogodni za malu djecu i maloljetnike.

Osnovna zaštita ugrađena u Windowse poslužit će za prvu ruku, no za pravo rješenje morat ćete posegnuti za nekim od specijaliziranih programa koji omogućuju filtriranje web-stranica, vremensko ograničavanje surfanja i izradu izvještaja o aktivnostima korisnika.

Donosimo pregled najpopularnijih programa te vrste. Više o upotrebi samih programa možete naučiti na tečaju NetAkademije, koja se jedina u Hrvatskoj bavi edukacijom roditelja o sigurnosti djece na internetu.

NetNanny Home Suite

Kada je riječ o zaštiti djece na internetu i roditeljskom nadzoru, NetNanny je jedna od najpoznatijih tvrtki.

Njihovi proizvodi dugi niz godina slove kao najbolji na tržištu i osvajali su mnogobrojne nagrade. Nažalost, nisu besplatni i za osnovnu inačicu programa valja izdvojiti 50 dolara.

K9 Web Protection

Potpuno besplatan i vrlo kvalitetan program omogućit će vam filtriranje web-stranica po mnogim kriterijima i za većinu roditelja će predstavljati dovoljno kvalitetno rješenje. Nažalost, omogućuje samo kontrolu nad web-stranicama, ali ne i nad programima koje dijete pokreće.

Child Control 2008

Nažalost, dobre stvari nisu besplatne, pa ćete za ovaj program, koji je jedan od ponajboljih koje možete kupiti, morati odvojiti 30 eura.

Mogućnosti su mu velike i teško mu je naći ijednu zamjerku. Omogućuje blokiranje web-stranica i programa prema svim mogućim parametrima, kao i definiranje čitavog niza sigurnosnih ograničenja.

CyberPatrol

Još jedan solidan, ali, nažalost, komercijalni program.

Za jednu godinu zaštite i sigurnog surfanja svog djeteta morat ćete izdvojiti 40 dolara. Ima gotovo sve mogućnosti kao i netom spomenuti Child Control, samo što ima nešto kompliciranije sučelje.

SentryPC

Nešto manje poznat program koji je natrpan mogućnostima i nudi ama baš sve što bi vam moglo zatrebati da zaštitite svoje dijete od nepoželjnog sadržaja.
Pregledno sučelje i dobra dokumentacija dodatna su prednost. Cijena, nažalost, nije i iznosi 50 dolara.

preuzeto s http://sigurnost.tvz.hr/
http://netakademija.tvz.hr/ostalo/programi-za-zastitu-djece-na-internetu-/