SIGURNA I ODGOVORNA UPOTREBA IKT-A U ŠKOLI

- Prijedlog sadržaja dokumenta

Uvod

Koncept digitalne zrelosti škola postaje sve više značajan zbog vrlo brzog razvoja i sve veće važnosti informacijsko-komunikacijskih tehnologija (IKT) u obrazovanju. Europska komisija je također uvidjela tu važnost, te podržava razvoj digitalne zrelosti škola. Digitalno zrele škole se definiraju kao škole s visokom razinom integracije IKT-a, sistematiziranim pristupom korištenja IKT-a u upravljanju školom i u obrazovnim procesima.

S obzirom na sve veću sustavnu uporabu IKT-a u školama, potrebno je voditi računa o prijetnjama informacijskom sadržaju i IKT infrastrukturi koje mogu rezultirati različitim oblicima štete informacijskom sustavu škole (npr. gubitak informacija, nemogućnost pristupa resursima i informacijskom sadržaju, uništenje opreme i sl.). Zbog toga je potrebno veliku pozornost potrebno posvetiti vidu sigurnog i odgovornog korištenja IKT-a, što je moguće postići definiranjem sigurnosne politike škole.Takav dokument pomaže školi ne samo da zaštiti informacijski sadržaj i opremu već i da zaštiti korisnike od različitih vrsta internetskog zlostavljanja, da promovira sustave i usluge koji su najprikladniji za djecu, te da potiče aktivno sudjelovanje djece u radu s IKT-om promovirajući sigurno, odgovorno i učinkovito korištenje digitalnih tehnologija u mrežnoj zajednici.

Koje ciljeve treba postići sigurnosna politika?

Svrha sigurnosne politike je definirati prihvatljive i neprihvatljive načine ponašanja, jasno raspodijeliti zadatke i odgovornosti te propisati sankcije u slučaju nepridržavanja. Drugim riječima, sigurnosna politika je organizacijska mjera za očuvanje integriteta informacijskog sustava škole te osiguranja nesmetanog djelovanja tog sustava pod pretpostavljenim oblicima prijetnji.

Zbog toga sigurnosna politika mora biti pisana jednostavnim i razumljivim jezikom te prilagođena lokalnoj kulturi, a istovremeno usklađena sa zakonima i propisima koji vrijede u državi. Za njezino provođenje potrebna je podrška uprave, a s njezinim načelima treba upoznati sve administratore i korisnike informacijsko-komunikacijskih sustava. Zato nakon prihvaćanja politike treba uložiti napor u obrazovanje korisnika.

Nove djelatnike treba pri zapošljavanju upoznati s pravilima propisanim politikom, a učenike pri otvaranju korisničkih računa.

Čemu služi ovaj dokument?

Ovaj dokument daje smjernice i preporuke za izradu Pravilnika o sigurnoj i odgovornoj upotrebi IKT-a u školi kao dijela sigurnosne politike škole. Oblikovan je uzimajući u obzir postojeću praksu u školama koje su oblikovale neku vrstu dokumenta koji govori o sigurnoj i odgovornoj upotrebi IKT-a, te uzevši u obzir preporuke EACEA/Eurydice mreže (http://eurydice.hr) koja analizira i pruža informacije o europskim obrazovnim sustavima, a usmjerena je na strukturu i organizaciju obrazovanja u Europi na svim razinama.

Kako koristiti ovaj dokument?

Kako ovaj dokument propisuje izgled Pravilnika o sigurnoj i odgovornoj upotrebi IKT-a u školi, u nastavku je prikazana i predložena struktura Pravilnika, a svaki dio je detaljno opisan. Škole bi trebale kroz te upute oblikovati vlastiti Pravilnik.

Svaki dio Pravilnika započinje kratkim uvodom, odnosno opisom područja (pisano ukoso, eng. italic), a nakon toga slijedi detaljna razrada područja u obliku pitanja, natuknica i izjava. Odgovori na ta pitanja/natuknice/izjave trebaju se formulirati u obliku članaka Pravilnika.

Pri izradi Pravilnika, preporučamo korištenje materijala dostupnih na mrežnoj str. http://www.petzanet.hr koji su nastali kao rezultat projekta usmjerenog ka sigurnosti djece na internetu, te dokumente Nacionalnog CERT-a koji se bave sigurnošću i privatnošću na internetu, dostupni na http://www.cert.hr.

Škole mogu dorađivati i prilagođavati se ovim smjernicama da bi njihova vlastita sigurnosna politika bila primjenjiva u specifičnim uvjetima. Mogu dodavati i nova pravila, u skladu s uslugama koje pružaju korisnicima.

Prijedlog strukture Pravilnika o sigurnoj i odgovornoj upotrebi IKT-a u školi

Uvod

U uvodnim napomenama potrebno je jasno navesti koja je svrha odluke; poput jasnog i nedvosmislenog određivanja načina prihvatljivog i dopuštenog korištenja IKT resursa škole.

Potrebno je također navesti za koga vrijedi odluka: za sve korisnike IKT infrastrukture škole, ili možda samo za učenike, nastavnike i sl. Ukoliko postoji i infrastruktura CARNetove mreže, potrebno je to spomenuti.

Potrebno je navesti i da se učenici moraju pridržavati uputa koje im mogu dati nastavnici, a kojima je cilj unapređenje sigurnosti školske informatičke opreme i mreže.

Isto tako je potrebno navesti da se i svi školski djelatnici moraju pridržavati uputa koje im može dati školski administrator sustava ili neka druga ovlaštena osoba radi unapređenja sigurnosti školske informatičke opreme i mreže.

Osnovne sigurnosne odredbe

Ovaj odjeljak ima zadaću istaknuti potrebu za sigurnošću informacija, infrastrukture te utjecaj ljudskih i drugih resursa na funkcionalnost pojedinih dijelova IKT infrastrukture.

Potrebno je definirati sve materijalne i nematerijalne resurse izravno povezane s IKT infrastrukturom (korisnike IKT infrastrukture te opremu koja se smatra IKT infrastrukturom škole):

- Tko su korisnici IKT infrastrukture?
- Koja oprema se smatra IKT infrastrukturom?
- Koja vrsta informacija postoji u školi (interne, javne, povjerljive i sl.)?
- Koja vrsta aplikacija se koristi u školi (npr. e-Dnevnik, računovodstveni sustav i sl.)?

Potrebno je jasno navesti da se školska oprema treba čuvati i koristiti pažljivo.

Jasno navedite da se tuđi osobni podaci mogu koristiti isključivo uz prethodno odobrenje.

U Pravilniku je potrebno odgovoriti i na sljedeća pitanja: Koje sigurnosne mjere zaštite podataka škola primjenjuje? Postoje li antivirusni programi, vatrozid, sigurnosna kopija podataka, neka domenska politika sigurnosti u računalnim mrežama ili nešto drugo? Na koji način se implementiraju te mjere zaštite? Postoje li neka određena pravila vezana uz te mjere zaštite?

Potrebno je navesti jesu li zaposlenici dužni koristiti službenu e-mail adresu (ime.prezime@skole.hr) za komunikaciju. Preporuka škole bi svakako trebala biti da se koristi isključivo službena adresa elektroničke pošte, posebice u službenoj komunikaciji s nadležnim tijelima i drugim institucijama iz sustava znanosti i obrazovanja.

Potrebno je navesti da je nastavnicima i drugim djelatnicima škole strogo zabranjeno davati učenicima i drugim korisnicima vlastite zaporke i digitalne identitete. To se odnosi na pristup školskim računalima, e-Matici, e-Dnevniku, računovodstvenim programima, knjižničarskim programima i ostalim informacijskim sustavima ili mrežnim aplikacijama koje sadrže osobne podatke djelatnika i/ili učenika.

Poželjno je definirati da svi djelatnici škole moraju potpisati izjavu o tajnosti podataka te da se moraju pridržavati etičkih načela pri korištenju IKT-a.

Isto je tako potrebno definirati što se događa u slučaju nepridržavanja pravila, kako škola sankcionira kršenje / nepridržavanje pravila te kome se prijavljuje svako ponašanje koje nije u skladu s odlukom (kome se javljaju učenici i drugi djelatnici ako primijete bilo kakvo kršenje pravila opisanih ovim dokumentom)?

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na mrežnoj stranici www.cert.hr“

Školska IKT oprema i održavanje

U ovom odjeljku potrebno je definirati školsku IKT opremu i način njezinog održavanja.

Definira se računalna mreža, njen sastav i nadležnosti osoblja za pojedine segmente mreže ukoliko takvi postoje. Npr. škola može dio računalne mrežne infrastrukture održavati sama, a dio mreže može biti u nadležnosti CARNeta ili nekog drugog održavatelja opreme.

Definiraju se računala i ostala računalna oprema škole i nadležnost za održavanje te opreme. Može se definirati posebno za sklopovlje, a posebno za računalne programe ukoliko je to potrebno. Definirajte i uvjete zbrinjavanja računalnog otpada.

Potrebno je definirati i konfiguraciju računalne mreže i lokalnih računala u smislu rasporeda i mrežnog priključenja postojećih računala, mogućnosti priključenja na mrežu (bežično/žično) ostalih računala te dostupnosti pojedine vrste mreža u pojedinim dijelovima školskih prostorija. Nadalje, potrebno je definirati korišteni osnovni sustavski i aplikativni softver na školskim računalima, postavke koje je postavio administrator, redoviti način ažuriranja računalnih programa, priključenje na lokalnu mrežu, internet, instalirane alate za zaštitu infrastrukture / opreme (npr. zaporke, antivirusni programi, vatrozid, filtriranje sadržaja i sl.).

U Pravilniku odgovorite i na sljedeća pitanja: Postoji li nadzor licenciranja? Tko je odgovoran za instalaciju i održavanje računalnih programa? Smiju li učenici instalirati računalne programe te pod kojim uvjetima? Kome se treba javiti ukoliko se želi instalirati računalni program? Koje su sankcije predviđene za nepridržavanje ovih pravila?

Reguliranje pristupa IKT opremi

Kako bi se zaštitila materijalna (IKT oprema) i nematerijalna imovina (informacije i podaci), potrebno je regulirati pristup svim IKT resursima identificiranih u odjeljku Osnovne sigurnosne odredbe.

Definirajte tko može pristupiti žičnoj i bežičnoj mrežnoj infrastrukturi, tko su sve korisnici te mreže, na koje načine se štiti računalna mreža (npr. WPA/WPA2 enkripcija i sl.) te pod kojim uvjetima korisnici imaju pravo pristupa mreži?

Definirajte mehanizme zaštite lokalnih računala (npr. domenska politika, zaporke, vatrozid, redovito ažuriranje, omogućavanje / onemogućavanje da krajnji korisnik i sl. instalira softver i sl.) Definirajte uvjete pod kojima korisnici mogu pristupiti lokalnim računalima; kojim računalima smiju pristupiti učenici, kojima nastavnici, a kojima ostalo osoblje.

Potrebno je definirati postojanje posebnog prostora na nekom poslužitelju ili mrežnom mjestu za zajedničko dijeljenje podataka, korisnike s pravima pristupa te uvjete pristupanja tom prostoru.

Definirajte vremenske termine korištenja računala i ostale opreme, npr. učenici za vrijeme nastave ili samo za vrijeme odmora, koju opremu i sl. Kada i pod kojim uvjetima učenici smiju pristupiti internetskim sadržajima, npr. pretraživanju interneta, društvenim mrežama i sl.?

Postoje li posebni propisi za korištenje opreme u informatičkim učionicama? Postoji li posebna odgovornost nastavnika za tu opremu (ili voditelja informatičke učionice)? Ovdje ju je potrebno definirati.

Potrebno je postaviti preporuke za korisničke zaporke, npr. da zaporka ne bude kraća od šest (6) znakova ili deset (10), da ima kombinaciju malih/velikih slova, brojki i sl. Treba preporučiti redovitu promjenu zaporki (odrediti vremenski rok).

Definirajte načine filtriranja internetskih sadržaja, odnosno postoje li internetski sadržaji koji nisu primjereni za učenike pa im učenici niti ne mogu pristupiti? Pozovite se na Odluku Ministarstva znanosti i obrazovanja prema kojoj su sve osnovne i srednje škole spojene na CARNetovu mrežu.

automatski uključene i u sustav filtriranja nepoćudnih sadržaja. Odlukom MZO-a onemogućava se prikazivanje četrnaest (14) kategorija stranica na računalima u osnovnim i srednjim školama (vidite: http://www.carnet.hr/filtriranje_sadrzaja).

Potrebno je jasno naglasiti da se od učenika očekuje da prihvate filtriranje određenih sadržaja kao sigurnosnu mjeru te ga ne smiju pokušati zaobići jer je ono postavljeno radi njihove sigurnosti, ali i sigurnosti svih drugih učenika. Potrebno je zabraniti zaobilaženje bilo kojih sigurnosnih postavki računalne opreme.

Postoji li nadzor mrežnog prometa? Tko ga obavlja?

Sigurnost korisnika

U ovom odjeljku nužno je definirati sve mjere sigurnosti vezane uz korisnika i utvrditi neka poželjna pravila ponašanja.

Na početku je potrebno istaknuti potrebu za stalnom edukacijom učenika i cijelog školskog kolektiva da bi se držao korak s trendovima u korištenju IKT-a, kao i s nadolazećim prijetnjama računalnoj sigurnosti.

Definirajte načine prijave i odjave korisnika u radu sa sustavom (računalima i drugim servisima koji zahtijevaju prijavu).

Definirajte postupak ophođenja s privatnim (i tajnim) podacima koje su korisnici dobili od škole (poput elektroničkog identiteta u sustavu AAI@Edu.hri sl.), uvjete preuzimanja datoteka na lokalno računalo i moguće pokretanje izvršnih datoteka (poželjno je zabraniti sve vrste takve interakcije).

Uredite odnos škole prema Elektroničkom identitetu u sustavu AAI@Edu.hr: postoji li potreba revidirati ih na godišnjoj razini, kako se oni izdaju i daju učenicima i sl.

Definirajte kada prestaju prava učenika (ili prava nad elektroničkim identitetom u sustavu AAI@Edu.hr), odnosno kad je prava potrebno ukinuti.

Definirajte prava pristupa djelatnika škole te načine ukidanja i postavljanja njihovih prava (korisnički računi i sl.).

Prihvatljivo i odgovorno korištenje informacijsko-komunikacijskih tehnologija

Ovaj odjeljak je strukturiran uzevši u obzir preporuke EACEA/Eurydice mreže koja analizira i pruža informacije o europskim obrazovnim sustavima (uključivši i integraciju IKT-a), a usmjerena je na strukturu i organizaciju obrazovanja u trideset i osam (38) zemalja Europe.

Ponašanje na internetu

Za svakog korisnika koji se susreće s internetom nužno je prvo upoznati ga s osnovnim pravilima ponašanja u takvoj komunikaciji i takvom okruženju. To se još naziva i 'internetskim bontonom', a vrlo čest naziv je i 'Netiquette'. 'Netiquette' je ustaljen popis pravila lijepog ponašanja u internetskoj komunikaciji i preveden je na mnoštvo jezika. Hrvatske stranice dostupne su na http://hr-netiquette.org. 'Netiquette' propisuju smjernice i pravila ponašanja u tri (3) kategorije: elektronička pošta, popis e-adresa i forumi. Poželjno je da škola ovaj skup pravila učini dostupnim svojim učenicima, o tome ih poduči, te primjeni vlastitu politiku u skladu s tim pravilima.

U sklopu ovog dokumenta škola mora definirati postojanje općeprihvaćenog skupa pravila ponašanja na internetu – *'Netiquette'* te načine upoznavanja svih korisnika s tim pravilima, npr. da će ona biti izvješena u informatičkim učionicama i nekim drugim mjestima. Isto tako, važno je napomenuti da je svaki pojedinac odgovoran za svoje ponašanje u virtualnom svijetu te da se prema drugim korisnicima mora ponašati pristojno, ne vrijeđati ih niti objavljivati neprimjerene sadržaje.

Važan vid ovog odjeljka je i sigurno korištenje interneta; potrebno je definirati načine na koje se učenike poučava da ne otkrivaju osobne podatke, uključujući svoju adresu, ime škole, telefonske brojeve i slično.

Potrebno je definirati da se uz Pravila lijepog ponašanja na internetu postave i Pravila sigurnog ponašanja, koja mogu uključivati naputke poput:

- Osobne informacije na internetu se nikad ne smiju odavati.
- Zaporka je tajna i nikad se ne smije nikome reći.
- Ne odgovarajte na zlonamjerne ili prijeteće poruke!
- Treba pomoći prijateljima koji su zlostavljani preko interneta tako da se to ne prikriva i da se odmah obavijeste odrasli.
- Provjeriti je li Facebook profil skriven za osobe koji nam nisu ‘prijatelji’. Treba biti kritičan prema ljudima koji se primaju za ‘prijatelje’.
- Potrebno je biti oprezan s izborom fotografija koje se objavljuju na Facebooku.
- Treba provjeriti postoji li neka mrežna stranica o nama te koje informacije sadrži (treba upisati svoje ime i prezime u Google).

Autorsko pravo

U ovom odjeljku se definiraju autorska prava koja se tiču digitalnih sadržaja, te se preporuča koristiti sustav licenciranja opisan u sljedećem odjeljku.

Autorska prava na online dokumentima najčešće se definiraju s tzv. Creative Commons (CC) licencama (vidite: https://creativecommons.org/licenses/?lang=hr). Creative Commons licence jesu skup autorsko-pravnih licenci pravovaljanih u čitavom svijetu. Svaka od licenci pomaže autorima da zadrže svoja autorska prava, a drugima dopuste da umnožavaju, distribuiraju i na neke druge načine koriste njihova djela, barem u nekomercijalne svrhe. Svaka Creative Commons licenca osigurava davateljima licence i da ih se prizna i označi kao autore djela.

Ovdje je potrebno istaknuti da se korisnike potiče da potpisuju materijale koje su sami izradili koristeći neku licencu poput one navedene u prethodnom odjeljku, ali i da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti nedopušteno preuzimati tuđe radove s interneta. Korištenje tuđih materijala s interneta mora biti citirano, obavezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja).

Pri korištenju IKT opreme važno je napomenuti i da su računalni programi također zaštićeni zakonom kao jezična djela. Najčešće su zaštićeni samo izvorni programi, no ne i ideje na kojima se oni zasnivaju. U to su uključeni naravno i mrežni programi, odnosno aplikacije.

Kod mrežnog mjesta je moguće posebno zaštititi samo objavljeni sadržaj, a moguće je zaštititi i elemente koji se odnose na samo mrežno mjesto i djelo su dizajnera i/ili tvrtke/osobe koja je izradila samo mrežno mjesto.

Dijeljenje datoteka

Prednost digitalnog sadržaja je da se ne uništava ili mu se ne umanjuje kvaliteta s brojem kopiranja. Ipak, baš zbog tog vida potrebno je biti vrlo oprezan s korištenjem digitalnih materijala, a još više s njihovim dijeljenjem. Naime, dijeljenje datoteka, samo po sebi, nije nelegalno. U slučaju da je datoteka proizvod pojedinca, pojedinac je može bez problema podijeliti s drugima na različite načine. Pritom je, dakako, uputno zaštititi djelo nekom vrstom prikladne licence.

Primjer nelegalnog dijeljenja datoteke jeste kopiranje ili preuzimanje autorski zaštićenog materijala poput e-knjige, glazbe ili pak videosadržaja. Mnogi online servisi danas omogućuju preuzimanje glazbenih albuma, pjesama, video-sadržaja ili pak e-knjiga na nelegalan način. Primjer su klijenti (npr. Torrent) koji omogućuju dijeljenje sadržaja između računala pa se tako dijele najčešće nelegalno nabavljeni videosadržaji te glazbeni sadržaji, ključevi za korištenje različitih aplikacija i drugi digitalni sadržaji koji su zaštićeni autorskim pravima, gdje je izričito zabranjeno daljnje distribuiranje i umnožavanje bez dozvole autora ili bez plaćanja naknade. Postoje i različiti oblici mrežnog servisa koji omogućuju

registraciju korisnika za vrlo nisku mjesečnu pretplatu te nude preuzimanje gotovo neograničene količine digitalnog sadržaja koji je zaštićen autorskim pravom, no to je također nelegalno.

U ovom odjeljku se dakle preporuča definirati nelegalno dijeljenje datoteka te to izričito zabraniti.

Dodatne preporuke:

1. Učenike i nastavnike treba podučiti o autorskom pravu i intelektualnom vlasništvu.
2. Učenike i nastavnike potrebno je podučiti i usmjeriti na korištenje licenci za zaštitu autorskog prava i intelektualnog vlasništva. Mogu se koristiti materijali s https://creativecommons.org/licenses/?lang=hr
3. Učenike i nastavnike treba podučiti o načinima nelegalnog dijeljenja datoteka i servisima koji to omogućuju poput *Torrent* servisa, mrežnog mjesta koja zahtijevaju registraciju i plaćanje vrlo niske članarine za neograničeno preuzimanje digitalnog sadržaja i sl.
4. Učenike i nastavnike treba informirati o mogućim posljedicama nelegalnog korištenja, dijeljenja i umnažanja autorski zaštićenih materijala.

Internetsko nasilje

Internetsko nasilje se općenito može definirati kao namjerno i opetovano nanošenje štete korištenjem računala, mobitela i drugih elektroničkih uređaja.

Postoje različiti oblici internetskog zlostavljanja:

- *nastavljanja slanja e-pošte usprkos tome što netko više ne želi komunicirati s pošiljateljem*

otkrivanje osobnih podataka žrtve na mrežnim stranicama ili forumima

- *lažno predstavljanje žrtve na internetu*
- *slanje prijetećih poruka žrtvi koristeći različite internetske servise (poput Facebooka, Skypea, e-maila i drugih servisa za komunikaciju)*
- *postavljanje internetske ankete o žrtvi*
- *slanje virusa na e-mail ili mobitel*
- *slanje uznemirujućih fotografija putem e-maila, mms-a ili drugih komunikacijskih alata.*

Nasilje u školama je postao sve veći problem tijekom nekoliko posljednjih godina, a budući da sve više djece koristi internet i mobilne telefone za komuniciranje, internetsko nasilje 'cyberbullying' je postalo velik problem. U nekim zemljama ovom se problemu pristupa u suradnji s udrugama ili drugim javnim tijelima koja djeluju u školama.

Iako se velika većina incidenata može riješiti neformalnim putem (zvanjem roditelja, slanja djece savjetniku i sl.), postoje i situacije kad se zahtijeva službena reakcija škole. To se događa u slučajevima koji uključuju ozbiljne prijetnje prema drugim učenicima, a rezultiraju time da žrtva više ne želi ići u školu ili pak ako se nasilje nastavi iako su već korištena druga neformalna sredstva. U takvim težim oblicima zlostavljanja potrebno je izreći neku od

disciplinskih mjera škole.

U ovom je odjeljku potrebno definirati nasilničko ponašanje koristeći spomenute primjere. Potrebno je istaknuti da su svi oblici nasilničkog ponašanja nedopušteni i da će disciplinski odgovarati svi oni za koje se utvrdi da provode takve aktivnosti.

Uputno je preporučiti da se jasne poruke o takvom ponašanju šalju kroz predmete koji koriste tehnologiju ili Sat razrednika te da pravila o prihvatljivom ponašanju i korištenju tehnologije budu vidljiva i u prostorijama škole.

Potrebno je definirati i mjere (ili strategije) odgovora na relativno male oblike uznemiravanja koja nisu prouzročila veliku štetu.

Dodatne preporuke:

1. Potrebno je podučiti učenike i nastavnike o mogućim oblicima internetskog nasilja.
2. Učenike i nastavnike treba podučiti o tome kako prepoznati internetsko nasilje.
3. Jasno je potrebno istaknuti prihvatljiva pravila ponašanja te učenike i nastavnike podučiti kroz predmete koji koriste tehnologiju.
4. Treba izraditi strategiju odgovora na internetsko nasilje, i to na blaži i teži oblik.
5. Potrebno je razviti nultu stopu tolerancije na internetsko nasilje.
6. Poželjno je objaviti natječaj za najbolji videouradak, likovni ili literarni uradak na temu internetskog nasilja da bi se potaknula svijest o temi među učenicima.

Korištenje mobilnih telefona

Ovdje je potrebno vrlo kratko definirati uvjete pod kojima je moguće koristiti mobilne telefone, na nastavi i u školi općenito. Isto tako potrebno je upozoriti da mobilni telefoni sve više imaju potpuni pristup internetu i djeca i mladi koriste fiksne internetske veze kao i mobitele za pretraživanje interneta. Stoga, iste sigurnosne mjere za korištenje interneta postaju važne i za korištenje mobilnih telefona (zaštita osobnih podataka, izbjegavanje štetnih sadržaja, zaštita potrošača, ovisnost o računalnim igrama, i slično).