KAKO SE ZAŠTITITI U SVIJETU INTERNETA I MOBILNIH TELEFONA

HAKOM
HRVATSKA REGULATORNA AGENCIJA
ZA MREŽNE DJELATNOSTI

Digitalno doba donijelo je brojne zanimljive aplikacije, a društvene mreže postale su novi prostori za učenje, zabavu i druženje te pronalaženje, kako dobrih, edukativnih i zanimljivih sadržaja, tako i sadržaja koje moramo provjeravati jer nisu primjereni za djecu. Razvoj modernih tehnologija i pojava interneta kao svakodnevnog medija povećali su rizike koji izravno utječu na razvoj i odrastanje djece i mladih. Novi izazovi u korištenju usluge interneta u proteklom, novonastalom razdoblju, svakako su bili nastava na daljinu i rad od kuće. Iako nismo bili u potpunosti spremni na takve promjene, kada smo u isto vrijeme radili i služili se novom tehnologijom, a s druge strane učili na koji način ju koristiti, brzo smo morali usvojiti nove riječi Zoom for Education, Cisco Webex, Googleov paket aplikacija, Microsoftove aplikacije i Apple FaceTime. Iako smo ranije brinuli kako nam dijete provodi previše vremena on line, u ovom trenutku nije vrijeme da djeci pokušamo oduzeti ono što im pomaže kod usvajanju novih znanja, u čemu uživaju i što, ne zaboravimo, ako se primjereno koristi može imati pozitivne učinke. Na internetu postoje izvrsni sadržaji te stoga dopustite svojoj djeci da ih otkriju i koriste, ali i dalje budite na oprezu, kako bi u konačnici naši najmlađi imali zdravo i uravnoteženo djetinjstvo. Možda ćemo ponekad biti zabrinuti što zbog internetske učionice naše dijete provodi dodatno vrijeme pred zaslonom! Shvaćamo da su neke aktivnosti edukativne; a neke su samo zabava. No zapamtimo – ono što radimo pred ekranima i kako to radimo, važnije je od utrošenog vremena.

APLIKACIJE ZA UČENJE NA DALJINU

ZOOM

Zoom je alat za video-chat, sličan Skypeu i Google Hangoutsu. Djeca ga mogu koristiti za pohađanje internetskih tečajeva, posjećivati s prijateljima i rodbinom, a mogu se i pridružiti se udaljenim događajima poput rođendana. Osnovna, besplatna verzija Zooma, nudi mnoštvo opcija, poput mogućnosti da nastavniku bez riječi signalizirate kako imate pitanje, pametujete na virtualnoj ploči i surađujete na projektima bilježeći dokumente na ekranima drugih učenika. Prelaskom na internetsko učenje tijekom pandemije koronavirusa, pokazala se potreba za nadogradnjom dodatnim mjera privatnosti i postavki sigurnosti.

MICROSOFT

Microsoft nudi dvije različite aplikacije za videokonferencije. Skype je namijenjen korisnicima, uključujući djecu i studente, a Microsoft Teams namijenjen suradnji poslovnog tima. Teams for Education također je uključen u paket proizvoda Microsoft Education i ima dodatne zaštite privatnosti za studente.

GOOGLEOV PAKET APLIKACIJA

Googleov paket aplikacija ima nekoliko različitih aplikacija za video konferencije koje bi nastavnici mogli koristiti za učenje na daljinu. Svaka od aplikacija nudi vrlo slično iskustvo, ali istovremeno namijenjene su različitim korisnicima. Google Meet namijenjen je za poslovne sastanke, a Google Chat za razmjenu tekstualnih poruka kod suradnje poslovnog tima. Google Hangouts namijenjen je održavanju kontakta s prijateljima i obiteljima, a Google Duo mobilnim uređajima i može raditi između iOS i Android uređaja. Google Voice namijenjen je samo za telefonske pozive. Alati za učenje na daljinu, koji su uključeni u paket proizvoda Google for Education, imaju dodatne zaštite privatnosti za studente.

CISCO WEBEX

Cisco Webex namijenjen je učenicima i nastavnicima te se može koristiti u poslovne svrhe. Idealan je za održavanje nastave na daljinu jer ima i funkciju snimanja predavanja koje učenici mogu naknadno pogledati. Kako bi ga učenici mogli koristiti na svojim prijenosnim računalima, školski administrator treba instalirati Cisco Webex Meetings aplikaciju.

APPLE FACE TIME

je udaljena web stranica s resursima za učenje, koja omogućava video kao način podučavanja kako bi se nastavnicima (i roditeljima) pružili savjeti o učenju. Također, poboljšao je svoje mogućnosti iCloud suradnje kako bi omogućio ljudima da dijele cijele mape i dodao je značajke u svoj iWork softver poput mogućnosti uređivanja izvan mreže.

Nacionalno istraživanje provedeno u sklopu projekta “EU Kids Online 2020”.

Rezultati istraživanja iz 19 zemalja (EU Kids Online 2020: Survey results from 19 countries), pokazuju rizike i prilike koje internet pruža djeci u Europi. Istraživanje je provedeno u razdoblju od jeseni 2017. do ljeta 2019. u 19 europskih zemalja, a odnosilo se na elektroničko nasilje, gledanje štetnog sadržaja na internetu, zloupotrebu podataka, pretjeranu upotrebu interneta, seksting i upoznavanje nepoznatih osoba na internetu. Istraživači tvrde kako online aktivnosti ne mogu biti uvjerljivo definirane niti kao općenito pozitivne niti kao općenito negativne te kako učinci neke online aktivnosti mogu imati pozitivne posljedice na jedno, a negativne na drugo dijete. Jedan od takvih primjera je susretanje osoba koje su djeca prethodno upoznala samo preko interneta.

5% djece izjavilo je kako su nakon susreta s osobom koju su prije toga poznavali samo putem interneta, bili blago ili vrlo uzrujani.

96% djece barem ponekad dobiva savjete o sigurnom korištenju interneta od roditelja, nastavnika i prijatelja. Treba istaknuti i da nakon negativnih iskustava na internetu, većina djece u Hrvatskoj najčešće razgovara s roditeljima.

U odnosu na djecu iz ostalih 18 država, djeca u Hrvatskoj najrjeđe se suočavaju sa zlouporabom osobnih podataka. U Hrvatskoj, Španjolskoj, Norveškoj, Poljskoj i Srbiji dječaci češće od djevojčica prijavljuju elektroničko nasilje. Kao i u većini drugih država, i u Hrvatskoj kontakte s nepoznatim osobama na internetu češće ostvaruju starija djeca te češće dječaci od djevojčica.

Dok je u Češkoj, Njemačkoj, Španjolskoj i Srbiji 30% i više djece primilo poruke seksualnog sadržaja, u Hrvatskoj, Italiji, Slovačkoj i Estoniji s takvim se sadržajima susrelo 10% i manje djece. U Hrvatskoj je 2% djece poslalo ili objavilo poruku seksualnog sadržaja. Primjerice, u Njemačkoj je takve sadržaje poslalo ili objavilo 18% djece.

Što je pokazao Hrvatski nacionalni izvještaj

IZVOR: HRKIDS.ONLINE

4. Svako četvrto dijete u dobi od 9 do 14 godina te svako treće dijete u dobi od 15 do 17 godina je u potpunosti ili uglavnom zabrinuto za svoju privatnost na internetu.

10. Svako deseto dijete u dobi od 15 do 17 godina prihvaća sve zahtjeve za prijateljstvom drugih ljudi na društvenim mrežama. Istodobno, gotovo svako četvrto dijete te dobi svakoga tjedna traži na internetu nove prijatelje ili kontakte.

5. Svako peto dijete u dobi od 9 do 17 godina u potpunosti ili uglavnom ne zna promijeniti postavke privatnosti, npr. na društvenim mrežama.

2/3 Gotovo 2/3 djece u dobi od 9 do 17 godina na internetu je u proteklih godinu dana vidjelo seksualne fotografije ili film gole osobe, a da im nije bila namjera vidjeti ih. S tim se susrelo 3/4 djece u dobi od 9 do 11 godina, više od 2/3 djece u dobi od 12 do 14 godina te gotovo 2/3 djece u dobi od 15 do 17 godina.

Kada ih je zadnji put na internetu nešto uznemirilo ili im zasmetalo, više od pola djece u dobi od 9 do 17 godina je zatvorilo aplikaciju, svako treće dijete je blokiralo osobu kako ih ona više ne bi mogla kontaktirati, svako četvrto dijete ignoriralo je problem, a svako peto dijete promijenilo je postavke privatnosti.

3. Gotovo svako treće dijete u dobi od 9 do 17 godina je u posljednjih godinu dana (od trenutka provedbe istraživanja) komuniciralo na internetu s osobama koje nisu upoznali uživo. To je činilo svako deseto dijete u dobi od 9 do 11 godina, svako četvrto dijete u dobi od 12 do 14 godina te gotovo svako drugo dijete u dobi od 15 do 17 godina.

Roditelji češće o aktivnostima na internetu razgovaraju s djecom mlađe dobi. Istodobno, roditelji puno češće nadziru aktivnosti na internetu mlađe djece, ali i mlađoj djeci češće daju savjete što učiniti ako ih netko uznemirava na internetu.

Rezultati hrvatskog dijela istraživanja ukazuju na potrebu edukacije i podučavanja djece i mladih o njihovoj sigurnosti i mogućim rizicima. Osnovni cilj edukacije je potpora djeci i mladima kako bi što ranije i što uspješnije naučili kontrolirati sadržaje s kojima se susreću na internetu te kako bi se znali snaći u njima potencijalno neugodnim i uznemirujućim situacijama.

Zaštita osobnih podataka na internetu

Prije registracije na društvenoj mreži važno je pročitati postavke privatnosti.
Zaštita osobnih podataka, u realnom i virtualnom svijetu, postala je ozbiljnija i značajnija. Primjenom Opće uredbe o zaštiti podataka (poznatije kao skraćenica GDPR) nametnute su obveze i pravila svima koji prikupljaju i obrađuju osobne podatke.
Svatko mora prije samog prikupljanja podataka biti upoznat s osnovnim informacijama o tome tko i u koju svrhu prikuplja podatke, do kada će ih čuvati i obrađivati, kome će biti dostavljeni te koja su njegova prava.
Prije ostavljanja bilo kakvih osobnih podataka na internetu i društvenim mrežama dobro je proučiti pravila privatnosti, opće uvjete i sva druga upozorenja. Nakon javne objave nekog podatka, taj podatak zapravo više nije naše vlasništvo.
Ako se za pristup određenim aplikacijama ili uslugama traži davanje suglasnosti/privole, dobro proučimo za što dajemo suglasnost (npr. za lociranje) i imajmo na umu kako je uvijek sigurnije dati što manje osobnih podataka.

TREBA IMATI NA UMU KAKO GDPR PROPISUJE DA U SLUČAJU NUĐENJA USLUGA INFORMACIJSKOG DRUŠTVA (NPR. INTERNET TRGOVINE), PRIVOLU ZA OBRADU OSOBNIH PODATAKA DJETETA MLAĐEG OD 16 GODINA MOŽE DATI SAMO RODITELJ ILI SKRBNIK!

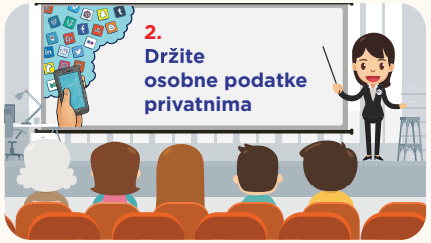
UPOZORENJE

DJECI, MLADIMA I RODITELJIMA

- Nemojte javno objavljivati i razmjenjivati osobne i intimne podatke (lokaciju, fotografije, datum rođenja, adresu i slično)
- Ne objavljujte tuđe podatke (npr. fotografije prijatelja i članova obitelji) bez suglasnosti te osobe

RODITELJIMA,

- Nemojte objavljivati osobne podatke i fotografije djece na internetu
- Ne objavljujte lokacije i mjesta gdje vaša djeca borave (škola, vrtići i slično)

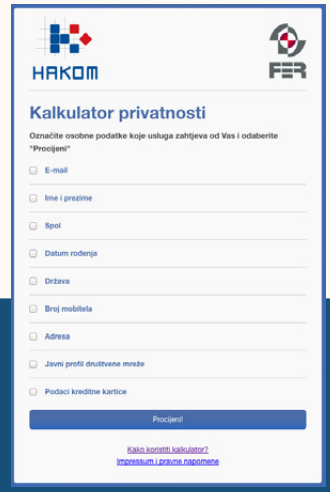


Često objavljujemo sadržaj, ali moramo biti svjesni kako objavljeni sadržaj zauvijek ostaje "negdje u nekom virtualnom prostoru" pa je moguće da jednom u budućnosti djetetu neće biti ugodno zbog njegovih slika i sadržaja koji su bili dostupni roditeljevim prijateljima, ali i drugim ljudima.

KALKULATOR PRIVATNOSTI

Provjerite potencijalni rizik za vlastitu privatnost prilikom korištenja interneta i davanja osobnih podataka. Uobičajeno se u većini slučajeva traži registracija tijekom koje korisnik mora predati svoje osobne podatke, najčešće e-mail adresu, ime i prezime. Putem aplikacije Kalkulator privatnosti možemo se educirati, a navedena aplikacija potaknut će nas na razmišljanje o problemima sigurnosti i privatnosti na internetu.

privatnost.hakom.hr



Usluga “roditeljske zaštite“

Usluga „Roditeljska zaštita“ nudi mogućnost zabrane pristupa neprimjerenim internetskim sadržajima za djecu. Zaštita osigurava filtriranje internetskog sadržaja, ograničavanje poziva ili slanje poruka prema nepoznatim brojevima ili roditelji sami kreiraju popis brojeva s kojima dijete može komunicirati.

Ako primamo SMS ili MMS poruke sa sadržajem neprimjerenim djeci i namijenjene isključivo odraslima, o tome možemo obavijestiti svog operatora ili prijaviti primitak takve poruke na adresu elektroničke pošte **nezeljeni.sms@hakom.hr**. Brojevi s kojih se šalju takve poruke će se nakon provjere u najkraćem mogućem roku blokirati.

Mogućnost isključenja korištenja pojedinih usluga. Zabrana slanja i/ili primanja SMS i MMS poruka u okviru usluge s posebnom tarifom (6xx xxx, 8xx xxx i sl.) može se besplatno zatražiti od operatora.

Moguće je postaviti zabranu odlaznih poziva nakon dogovorenog limita potrošnje.
Novčani limit potrošnje za usluge s posebnom tarifom koje su namijenjene djeci (iznos 50,00 kn).

Roditelji, možete ograničiti vrijeme koje dijete provodi na mobitelu uz besplatne aplikacije.
Osim toga, aplikacije nude i opciju praćenja djetetovih aktivnosti na uređaju.
Svakako razgovarajte s djetetom prije nego instalirate aplikaciju i zajedno dogovorite pravila.

Svaki operator koji pruža i usluge televizije omogućava roditeljsku zaštitu koja se može aktivirati po potrebi i željama korisnika. Također, omogućena je i zabrana pristupa gledanju neprimjerenih TV programa i filmova, poput pornografskih ili nasilnih sadržaja.

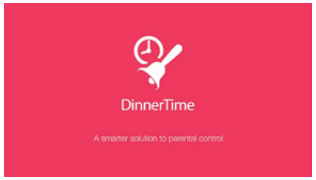
Pravila trebaju uzeti u obzir dob djeteta i definirati doba dana te ukupno vrijeme koje dijete smije provesti na računalu ili mobitelu, vrstu igrice ili aplikacije koje će koristiti. Kod mlađe djece preporučljivo je koristiti opcije roditeljskog nadzora i filtriranja sadržaja, ali svakako djecu informirajte o postavkama filtera.

POSTAVITE OKVIRNA PRAVILA U DOGOVORU S DJETETOM

Ukoliko dijete/tinejdžer osjeti prevelik utjecaj na svoju privatnost ili pomisli da ga se „špijunira“, izgubit će povjerenje u roditelje te će lako naći način kako će od roditelja sakriti ono što ne želi da se zna. Ova situacija može biti jako opasna u slučaju da se dijete ili tinejdžer zaista nađe u problemu jer se zbog narušenog povjerenja neće htjeti obratiti roditelju za pomoć.

Roditelji mogu ograničiti vrijeme koje dijete provodi na mobitelu uz besplatne aplikacije. Osim toga, aplikacije nude i opciju praćenja djetetovih aktivnosti na uređaju. Međutim, treba uzeti u obzir djetetovo pravo na privatnost i što je dijete starije takve aplikacije manje su primjerene.

Dinner time aplikacijom upravlja se putem roditeljskog mobitela koji može biti Android, ili iPhone, a djetetov mobitel mora biti Android. Moguće je u bilo kojem trenutku uključiti pauzu od korištenja uređaja te ograničiti ukupno vrijeme koje dijete može provesti koristeći uređaj ili određene aplikacije.



Kids Place aplikacija stvara sučelje za dijete i omogućuje sortiranje aplikacija koje dijete smije koristiti na mobitelu. Onemogućuje preuzimanje novih aplikacija, korištenje telefonskih poziva, SMS poruka i ostalih radnji koje mogu izazvati trošak. Za izlazak iz Kids Place aplikacije i ulazak u roditeljsko sučelje potreban je PIN koji roditelj sam bira. Aplikacija je prikladna za mlađu djecu.

Sigurnost i zaštita na internetu za djecu, mlade, roditelje i stručnjake u obrazovnom procesu

Internetska platforma "SINI – Sigurni na internetu" (https://sini.hr/) izrađena je s ciljem da se internet učini sigurnijim i boljim mjestom. Edukativnim materijalima i važnim informacijama, na zanimljiv i inovativan način, aplikacija približava područje sigurnosti i zaštite na internetu, a namijenjena je djeci i mladima, roditeljima i stručnjacima, koji rade i surađuju u obrazovnom sustavu. Aplikacija je doprinos stvaranju sigurnijeg okruženja u kojem građani, posebno djeca i mladi, sigurno koriste mobilne uređaje i nove tehnologije. Nastala je kao rezultat suradnje Centra za nestalu i zlostavljanu djecu s Hrvatskom regulatornom agencijom za mrežne djelatnosti (HAKOM-om) i tri hrvatska operatora elektroničkih komunikacijskih usluga, A1 Hrvatska, Telemach Hrvatska i Hrvatskog Telekoma.

Edukativni članci i materijali namijenjeni su djeci, mladima, roditeljima i skrbnicima, a posebno je značajno kako ova platforma omogućava stručnjacima s područja cijele Republike Hrvatske na jednostavan i zanimljiv način stručno usavršavanje kroz formu online webinara. Ova mogućnost posebno je značajna stručnjacima u odgojno - obrazovnom procesu u onim dijelovima Hrvatske gdje stručno – edukativne aktivnosti na temu sigurnosti i zaštite djece i mladih na internetu nisu dostupne.

Kako bi mogli pristupiti edukativnom sadržaju putem SINI aplikacije, stručnjaci trebaju proći proces registracije, što će im omogućiti pristup različitim webinarima, a čije je prosječno trajanje od 30 do 60 minuta. Nakon odslušanog webinara polaže se ispit kako bi se dobio certifikat na temelju kojeg se sudjelovanje prijavljuje nadležnim Komorama. Kako bi se osigurao stručan i kvalitetan sadržaj, koji je dostupan putem internetske aplikacije, kontinuirano se okupljaju stručnjaci iz akademske zajednice i drugih relevantnih institucija i organizacija koji se u svom svakodnevnom radu bave područjem sigurnosti i zaštite djece i mladih na internetu te obrađuju različite teme koje prikazuju u webinarima.

Aplikacije koje smo razvili Susretnica – što je to?

Osim na internetu povrijediti nekoga (čak i nehotično) možemo i uživo.

Što sve znamo o pristupačnosti usluga i uređaja? Ovdje skrećemo pozornost na još jednu važnu kategoriju korisnika kojom se HAKOM bavi, a to su osobe s invaliditetom. Za njih smo, u suradnji sa FER-om, razvili i aplikacija Kviz koju ti preporučamo pogledati na www.hakom.hr. Naučit ćeš tamo sve o preprekama kojima su izložene osobe s invaliditetom, ali i testirati znanje roditelja o korisničkim pravima.

Baš nas zanima koliko će tvoja obitelj prikupiti točnih odgovora!

Sada skrećemo pozornost na najnoviju aplikaciju **Susretnica**. Često odrasli, a pogotovo djeca, ne znaju kako pravilno pristupiti osobi sa invaliditetom u svakodnevnim situacijama. Zato, olakšajmo sebi tako da bolje upoznamo druge. Odaberite između avatara Ane ili Marka i dopustite im da vas povedu putem jače integracije svih članova društva!

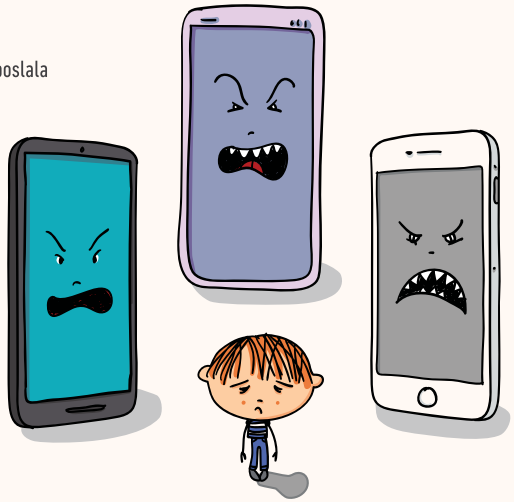
http://www.ict-aac.hr/index.php/hr/novosti-aplikacije/512-objavljena-nova-aplikacija-ict-aac-susretnica

Metode elektroničkog nasilja i uznemiravanja

Cyberbulling (elektroničko nasilje) - djeca se najčešće zlostavljaju putem mobitela i društvenih mreža Elektroničko nasilje uključuje različite oblike napada na pojedinca, slanje prijetećih poruka, osnivanje grupa koje podržavaju mržnju na društvenim mrežama. Osim zajedničkih karakteristika koje imaju „tradicionalno" i „moderno" vršnjačko nasilje poput agresivnosti, namjere da se nekoga povrijedi te nemogućnosti žrtve da se obrani, vršnjačko nasilje putem interneta sa sobom nosi nove opasnosti za žrtvu. Jedna od najvažnijih karakteristika vršnjačkog nasilja putem interneta jest činjenica da ono nikad ne prestaje.

NEKE OD METODA ELEKTRONIČKOG NASILJA KOJIMA SE ZLOSTAVLJAČI SLUŽE SU:

- Grubo online sukobljavanje, uznemiravanje, ogovaranje i klevetanje i socijalno isključivanje
- Lažno predstavljanje
- Uzimanje tuđeg identiteta i slanje poruka i drugih sadržaja u tuđe ime
- Iznuđivanje i širenje povjerljivih informacija
- Javno objavljivanje podataka koje je žrtva u povjerenju poslala počinitelju nasilja. Također, počinitelj može manipulirati žrtvom da napiše nešto privatno koje onda javno objavljuje ili dijeli dalje bez dopuštenja
- Prijetnje i uhođenje
- Opetovano slanje prijetećih poruka te neprestani pokušaji uspostavljanja i nastavljanja neželjenog kontakta zbog kojih se žrtva počinje bojati za vlastitu sigurnost i dobrobit. Posebno je izraženo prilikom komunikacije s nepoznatim osobama i u slučajevima seksualnog nasilja putem interneta



- Videosnimanje
- Snimanje ili fotografiranje u situacijama koje su za djecu ponižavajuće ili neugodne; izazivanje i snimanje tučnjave ili drugih nasilnih sadržaja te njihovo širenje
- Izmjena fotografija
- Izmjena osobnih fotografija bez dozvole i objava na internetu

Sljedeći znakovi u osnovnoj školi i kod kuće mogu ukazivati da je dijete uključeno u nasilje među djecom, a mogu biti prisutni i kod djeteta koje je uključeno u elektroničko nasilje (Rivers, Duncan, Besag, 2009, prema Križan, 2018.).

RODITELJI

Znakovi koji ukazuju da je dijete možda doživjelo vršnjačko nasilje:

- učestala tišina
- povlačenje iz obiteljskih interakcija
- vidljiva tuga
- povlačenje od prijatelja i od aktivnosti u kojima je prije uživalo
- učestaliji izostanci iz škole (žaljenje na glavobolje i bolove u trbuhu)
- loš školski uspjeh (niže ocjene)
- gubitak apetita
- poremećaji spavanja (uključujući mokrenje u krevet)
- informacije iz škole o izgubljenim domaćim zadaćama ili problemima u ponašanju kao što su tučnjave s drugim učenicima
- prestaje koristiti računalo ili mobitel ili povećanje vremena provedenog na internetu u odnosu na prije
- čini se nervozno ili razdražljivo kada koristi računalo ili mobitel
- spominje nepoznate osobe
- pridavanje sve veće važnosti aktivnostima i osobama na internetu
- zatvaranje stranica, chatova i/ili skrivanje mobitela kada roditelji uđu u sobu ili kada se druga osoba približi
- stres prilikom čitanja poruka, odnosno primanja različitih sadržaja
- izbjegavanje razgovora o uporabi računala i interneta
- brisanje korisničkih računa ili otvaranje puno novih
- puno novih kontakata na mobitelu i/ili društvenim mrežama

UČITELJI

Znakovi koji ukazuju da je učenik/učenica možda doživio/doživjela vršnjačko nasilje:

- izbjegavanje kontakta očima i vidljiva tuga
- pojava nekontroliranih izljeva bijesa ili frustracije
- promjene u obrascima ponašanja s prijateljima i aktivnostima za vrijeme odmora
- nedostatak angažmana u razrednim ili grupnim aktivnostima u kojima je prethodno bio/bila aktivno angažiran/a
- učenici ga/je ismijavaju kada govori
- pridavanje manje pažnje školskom i domaćem radu

KAKO RODITELJI MOGU POMOĆI?

01. Razgovarajmo sa svojim djetetom. Otvoreno i često, čak i kad ne sumnjamo da postoji problem. Pokažimo mu da nam može vjerovati i da se na nas uvijek može osloniti. Razgovarajmo o internetu i ponašanju na društvenim mrežama. Međusobno poštovanje i uvažavanje su temelj svakog odnosa – online i offline. Objasnimo djetetu da ne smije postojati razlika između ponašanja u stvarnom i virtualnom svijetu – u oba slučaja vrijedi pravilo da druge ljude trebamo uvažavati i poštivati i prema njima se primjereno ponašati te od njih očekivati isto.

02. Budimo upoznati s ponašanjem svog djeteta na internetu. Kao što želimo znati s kim naše dijete provodi vrijeme u stvarnom svijetu, trebali bi znati i s kim provodi vrijeme u virtualnom svijetu.

03. Zamolimo dijete da nam pokaže koje stranice posjećuje i što tamo radi. Poučimo ga da u virtualnoj komunikaciji uvijek treba biti oprezan. Računalo držimo na pristupačnom mjestu gdje možemo imati nadzor nad djetetovim aktivnostima i odredimo vrijeme koje može provesti na internetu. Potaknimo dijete da koristi računalo za učenje i druženje. Dajmo mu do znanja da nam se može obratiti svaki put kad na internetu primijeti nešto neprimjereno ili uznemirujuće.

04. Roditeljima često nije lako prihvatiti mogućnost da je njihovo dijete počinitelj elektroničkog nasilja. Saznajte što se točno dogodilo i koje je uređaje, aplikacije ili društvene mreže dijete koristilo. Nikada nemojte prijetiti, osuđivati i vrijeđati dijete.

05. Objasnimo djetetu da svako zlostavljanje, bilo fizičko ili verbalno, uzrokuje bol drugoj osobi. Pomognite djetetu da razvije suosjećanje i da pokuša zamisliti kako bi se ono osjećalo ukoliko bi bilo izloženo nasilju. Ponudite djetetu pomoć pri promjeni i ispravljanju ponašanja.

06. Vrlo često zlostavljano dijete postaje zlostavljač. Seksualno uznemiravanje i zlostavljanje je protuzakonito i žrtva nikada nije kriva za ono što se dogodilo.

Opasnosti na internetu

Računali kriminalci se koriste malicioznim (zlonamjernim, štetnim) programima pomoću kojih zaobilaze zaštitu naših računala kako bi pristupili našim računalima i podacima.
Dnevno se otkrije nekoliko stotina tisuća novih malicioznih datoteka, a računalne obrane jednostavno ne mogu držati korak s takvom bujicom zlonamjernih programa. Zbog toga je potrebno biti upoznat s opasnostima na internetu – informiranost je najbolja obrana!
Putem elektroničke pošte, slanjem poruka za koje se na prvi pogled čini da dolaze od neke poznate tvrtke (Facebook, Ebay, Paypal, Snapchat i drugi) ili sličnim načinima. Svrha takvih poruka je da nas potaknu na unošenje svojih osobnih podataka u aplikaciju čime kriminalcima dajemo pristup našim podacima. A jednom, kada imaju podatke o nama, oni su u mogućnosti načiniti značajnu štetu, primjerice uzeti kredit u naše ime, obaviti kupnju s našim karticama, predstavljati se kao mi i slično.


From: Skype Notify <gaetano@pmw.de>
Date: 20 November 2015 at 00:25
Subject: Deferred messages priming
To:

Skype

Deferred message.

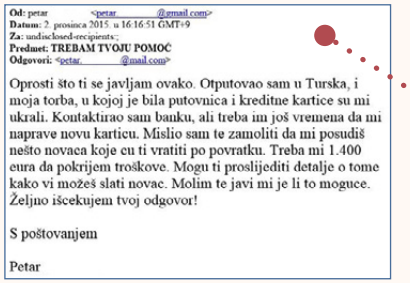
View messages

Yours truly
Skype support

© 2015 Skype and/or Microsoft. The Skype name, associated trade marks and logos and the "S" logo are trade marks of Skype or related entities. Skype Communications S.a.r.l. 23-29 Rives de Clausen, L-2165 Luxembourg

SAVJET:

u slučaju da primimo sličnu poruku nije preporučljivo kliknuti na link već u pregledniku unijeti adresu servisa, npr. www.facebook.com, ulogirati se i provjeriti čekaju li nas doista propuštene poruke


Od: petar <petar.@gmail.com>
Datum: 2. prosinca 2015. u 16:16:51 GMT+9
Za: undisclosed-recipients:;
Predmet: TREBAM TVOJU POMOĆ
Odgovori: <petar.@mail.com>

Oprosti što ti se javljam ovako. Otputovao sam u Turska, i moja torba, u kojoj je bila putovnica i kreditne kartice su mi ukrali. Kontaktirao sam banku, ali treba im još vremena da mi naprave novu karticu. Mislio sam te zamoliti da mi posudiš nešto novaca koje cu ti vratiti po povratku. Treba mi 1.400 eura da pokrijem troškove. Mogu ti proslijediti detalje o tome kako vi možeš slati novac. Molim te javi mi je li to moguce. Željno iščekujem tvoj odgovor!

S poštovanjem

Petar


From: Skype Notify <gaetano@pmw.de>
Date: 20 November 2015 at 00:25
Subject: Deferred messages priming
To:

Kako prepoznati lažnu poruku?

Neki od znakova po kojima se može prepoznati da je poruka lažna:

- ne obraća se osobno nama već počinje nekim općenitim pozdravom npr. „Hi there“, ili „Hey you“ ili „Bok!“,
- poruka ima gramatičke pogreške (često je slučaj da nam se pošiljatelj obraća u pogrešnom licu),
- ime servisa i adresa s koje piše da je poruka došla nisu isti,
- u ovom primjeru poruka izgleda kao da je došla od Skype-a no Skype ima domenu @skype.com, a ova poruka je došla s @pmw.de

Kako zaštiti e - mail adresu, Twitter račun i slično?

- koristimo različite lozinke za servise na internetu (nemojte koristiti istu lozinku za e - mail adresu, Facebook i druge stranice koje posjećujete). Kako ne bi pamtili stotine lozinki preporuča se poslužiti programom za upravljanje lozinkama. Isto, izbjegavajte birati za lozinku osobna obilježja poput mjesta rođenja, imena kućnog ljubimca ili majčinog djevojačkog prezimena. Do tih je podataka vrlo lako doći preko Facebook profila, koji su često otvoreni, ili profila na drugim društvenim mrežama na kojima ljudi objavljuju vrlo osobne podatke ne razmišljajući o tome na koje se sve načine mogu upotrijebiti protiv njih.
- popularne stranice i servisi poput Facebook-a, Google-a i Twittera nude mogućnost tzv. potvrde u dva koraka (Two Step Verification), koja štiti korisnički profil ili e-mail adresu od neovlaštenog upada jer šalje dodatni kod na naš mobitel koji treba unijeti ukoliko se prijavljujemo s dotad nepoznatog uređaja.
- budimo oprezni kad nas putem društvenih mreža kontaktiraju nepoznate osobe i na oprez potičimo i djecu. Prije nego ih prihvatimo za prijatelje provjerimo jesu li to zaista osobe za koje se predstavljaju. To možemo učiniti i tako da uzmemo profilnu fotografiju i unesemo ju u Google pretraživač jer prevaranti često koriste tuđe fotografije za lažne profile *<SIDEBAR upute za pretraživanje koristeći fotografije: Kada smo na Google pretraživaču prijeđemo na pretraživanje po slikama, kliknemo na ikonicu fotoaparata u rubu tražilice, odaberemo tab „Prenesite sliku" i iskoristimo fotografiju s profila za pretraživanje. >*
- Ako istu fotografiju pronađemo na više različitih mjesta, pod jednim ili više različitih imena – sve nam je jasno :) . Netko se ne predstavlja svojim pravim imenom!
- **Isključite** bluetooth odmah po prestanku upotrebe jer on predstavlja veliki sigurnosni rizik i lak posao za hakere kada žele doći do podataka na vašem uređaju.
- 3 godine kazne zatvora čeka onoga tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ili drugome učini dostupnim tako pribavljene podatke.

Znaš li da je u okviru završnog rada na FER-u izrađena aplikacija ICT-AAC Lozinka koja se sastoji od kviza, testera i generatora lozinke? Testirajte je na linku: http://www.ict-aac.hr/index.php/hr/ict-aac-razvijene-aplikacije/web-aplikacije/ict-aac-lozinka i ojačajte znanje & digitalnu zaštitu :)!

Prijevare putem interneta

- Internet prijevare se mogu dogoditi i putem aplikacija za komunikaciju poput **Vibera, Whatsapp-a** ili drugih, kada dobijemo poruku s poveznicom i tekstom koji nas informira da smo nešto osvojili ili da samo trebamo posjetiti poveznicu kako bi preuzeli nagradu, video ili neki drugi sadržaj.
- Budimo oprezni kada u svijetu nastanu situacije koje odjekuju po medijima – bilo da se radi o slavnim osobama, terorističkim napadima ili humanitarnim akcijama – kriminalci često koriste takve situacije za slanje elektroničke pošte u kojoj će vas pokušati nagovoriti da otvorite određenu stranicu ili skinete neku datoteku. Djeca se najčešće nagovaraju da otvore neku stranicu na kojoj ih „čeka" nagrada, a koja, naravno, ne postoji. Prijevara može biti i telefonskim putem na način da vas prevaranti pokušavaju navesti da otkrijete svoje osobne, financijske podatke ili da im uplatite novčana sredstva. Prevaranti mogu biti i „zainteresirani" za romantičnu vezu i često koriste društvene medije ili e-poštu za uspostavljanje kontakta.
- Dodatan oprez potreban je i kod instaliranja raznih aplikacija, bilo na pametnom telefonu ili Facebook-u. Provjerimo kojim sve osobnim podacima aplikacija traži pristup na našem uređaju. Ako su zahtjevi nerazumni, pa tako npr. aplikacija naziva „Toster" zatraži pristup vašim fotografijama i kontaktima, ne bi je trebali preuzeti!
- Kako nas netko na internetu može pokušati prevariti? **http://privatnost.hakom.hr/**

SAVJET:

Osvijestite i djecu da ne preuzimaju bilo kakve aplikacije, odnosno da ih zajednički pregledate i prokomentirate prije same instalacije i korištenja.

Društvene mreže i programi za razmjenu poruka

Današnja djeca i mladi teško mogu zamisliti život bez svakodnevnog korištenja društvenih mreža. Pravila lijepog ponašanja na društvenim mrežama prilagođavaju se novim tehnologijama, ali ono staro pravilo, koje vrijedi i u stvarnom životu, vrijedi u svakoj prilici: "Ponašajmo se prema drugima onako kako želimo da se drugi ponašaju prema nama."

SAVJET:

Opća pravila sigurnijeg korištenja društvenih mreža i programa za razmjenu poruka:

- što je nezakonito u stvarnom životu nezakonito je i na internetu
- ne ostavljajmo privatne informacije, bilo na fotografijama bilo u opisima
- ne otkrivajmo svoju lokaciju ako nije potrebno
- osigurajmo da se lokacija sa fotografije ne može otkriti korištenjem informacija s fotografije
- ne koristimo oznake (hashtags #) koje mogu otkriti privatne podatke ili lokaciju npr. #Ulica113
- ne dijelimo nasilne ili nepristojne fotografije. Pripazimo što šaljemo u svijet. Ne samo što stvaramo sliku o sebi već utječemo i na druge
- ne sudjelujmo u nasilju putem interneta. Ne omalovažavajmo i ne vrijeđajmo
- roditeljima se ne preporuča dijeliti fotografije svoje djece, no, ako ih dijelimo, ograničimo tko ih može vidjeti
- ako koristimo javni ili tuđi uređaj za pristup internetu ne zaboravimo se odjaviti s aplikacija koje koristimo
- način komuniciranja potrebno je prilagoditi drugom korisniku ili grupi korisnika kako bi razmjenjivanje informacija uspjelo
- proučimo postavke za sigurnost i privatnost. Maksimalno otežajmo neželjeno širenje naših privatnih informacija
- poštujmo privatnost - kako vlastitu, tako i ostalih korisnika
- ponašanje na internetu je ogledalo korisnika
  Naše ponašanje utječe na ukupnu kvalitetu društvene mreže
- nemojmo reagirati u ljutnji
- ako je moguće uključimo dvofaktornu autentifikaciju - (dodatnu prijavu putem koda odaslanog na uređaj po izboru - najčešće naš mobilni uređaj)

TIK TOK

Tik Tok je novija društvena mreža, odnosno aplikacija, koja u ovo vrijeme doživljava svoj veliki boom. Možemo je usporediti s YouTube, Instagram ili Facebook aplikacijama, no iz nekog razloga se Tik Tok probija i ističe u tako velikoj konkurenciji.
Ciljna grupa ovoj aplikaciji su osobe u starosnoj dobi između 16 i 24 godine, međutim koriste je već djeca od 8 godina pa na dalje. Aplikaciju mogu samostalno koristiti djeca već od navršenih 13 godina, ali ako to učine ranije profil im se briše.
Tik Tok je aplikacija koja svojim korisnicima daje mogućnost kreiranja kratkih video snimki. Riječ je o društvenoj aplikaciji, pa će jednom napravljen video biti dostupan za gledanje vlasniku video materijala, ali i drugim osobama s kojima je povezan. Aplikacija je prisutna još od 2016., no tek je u zadnjem periodu doživjela veliku svjetsku popularnost. Najčešći videozapisi koje korisnici objavljuju su plesne tematike, ima tu i komičnih skečeva, a kao i na svakoj društvenoj mreži i izazova.
Ako vaše mlađe dijete želi koristiti aplikaciju, postoji odjeljak aplikacije za djecu mlađu od 13 godina koji uključuje dodatne opcije sigurnosti i privatnosti. Djeca mogu vidjeti samo uređene, čiste videozapise i ne smiju komentirati, pretraživati ili objavljivati vlastite videozapise. Međutim, to ga čini neprivlačnim za većinu djece, a zaobilaženje sigurnosnih uvjeta zahtijeva samo unošenje lažnog datuma rođenja, pa nije savršen.

TikTok omogućuje roditeljima postavljanje vremenskih ograničenja, filtriranje sadržaja za odrasle i onemogućavanje izravnih poruka za dječje račune. Možete omogućiti vremenska ograničenja i filtar sadržaja na dječjem telefonu i zaštititi postavke zaporkom, ali da biste onemogućili izravnu razmjenu poruka, morate upotrijebiti značajku obiteljskog uparivanja u aplikaciji. (Obiteljsko uparivanje također vam omogućuje pristup vremenskim ograničenjima i postavkama filtra sadržaja.) Za sinkronizaciju postavki trebat će vam djetetov telefon.

SAVJET: Slično kao i poput ostalih društvenih mreža, ima feed (Feed je stream sadržaj kroz koji se možete pomicati) na kojemu se nalaze najpopularniji zapisi, a nakon registracije moguće je i 'lajkati' objave. Račun može biti javan ili privatan, odnosno može se odabrati tko će moći pregledavati sadržaj, a umjetna inteligencija odabire koji će se sadržaj pojavljivati na vašem feedu.

FACEBOOK

Facebook je web mjesto na društvenim mrežama na kojem korisnici mogu objavljivati komentare, dijeliti fotografije i objavljivati veze do vijesti ili drugog zanimljivog sadržaja na webu, razgovarati uživo i gledati videozapise u kratkom obliku i tu mrežu djeca najmanje koriste. Možete čak i naručiti hranu na Facebooku, ako je to ono što želite raditi. Dijeljeni sadržaj može biti javno dostupan ili se može podijeliti samo s odabranom grupom prijatelja ili obitelji ili s jednom osobom.
Facebook pruža prilagodljiv skup kontrola privatnosti, tako da korisnici mogu zaštititi svoje podatke od navale na treće osobe.

SAVJET: Treba znati da inicijalno Facebook čini listu naših prijatelja koja je javno dostupna.
Kako bi to promijenili, potrebno je označiti postavku „Obitelj i odnosi". Tamo su navedeni naši prijatelji, a klikom na gumb s penkalom pa na „Uredi privatnost", dolazimo do mjesta gdje definiramo tko vidi listu naših prijatelja. Najbolje je odabrati opciju „Prijatelji". Važno je napomenuti da Face, na isti način, nudi kontrolu nad objavom svake pojedine informacije.Više o tome kako zaštiti svoj Face možemo naći na poveznici http://www.cert.hr/dokumenti/zastitite_privatnost_na_facebooku

YOUTUBE

YouTube je mrežna usluga za razmjenu videozapisa gdje se isti mogu postavljati, pregledavati i ocjenjivati te sa sigurnošću možemo reći da je to najbolje mjesto za učenje i stjecanje novih vještina. Za postavljanje sadržaja potrebna je registracija, a za pregledavanje nije, osim za sadržaj koji nije primjeren za osobe mlađe od 18 godina.
YouTuberi među mlađom populacijom često imaju sve veći utjecaj od popularnih osoba, a neki više vjeruju virtualnim uzorima nego obitelji i prijateljima. Kvalitetni i popularni YouTuberi mogu pozitivno utjecati na djecu, ovisno o sadržajima kakve stvaraju i objavljuju. Posebnu pažnju treba posvetiti aplikaciji YouTube Kids ima gdje svatko može stvoriti YouTube kanale bez dodatnih provjera, a sadržaj je generiran od strane korisnika.

SAVJET: YouTube – moguće je regulirati postavke uključivanjem „restricted mode – on". Kako bi se to učinilo, potrebno je registrirati se na YouTube – registracija je besplatna. Na dnu prozora će se pojaviti alatna traka i opcija za uključivanje „restricted mode". Kako ni jedan filter nije 100% pouzdan, ipak je potrebno nadzirati dijete dok pretražuje video sadržaj, pogotovo kada je riječ o maloj djeci. Svakako provjerite jeste li prijavljeni u YouTube i je li opcija „restricted mode" uključena prije nego što djetetu prepustite da samo bira video sadržaj.

- Ne objavljujmo video pod osobnim imenom – možemo izmisliti nadimak za svoj kanal
- Imajmo na umu da djeci mlađoj od 13 godina nije dozvoljeno izraditi YouTube račun
- Dobro razmislimo hoćemo li objaviti video „Javno" – sami odlučujemo tko će vidjeti naš video..
  Opcija "Privatno" omogućava odabir ljudi koji mogu vidjeti video, a opcija "Nenavedeno" da video mogu vidjeti samo oni kojima se link pošalje.
- Možemo drugima ograničiti da dijele naš video, kao i isključiti komentare na svakom videu
- Ako vidimo videozapis za koji smatramo da sadrži neprikladan sadržaj možemo ga označiti zastavicom i prijaviti.
  Vodimo računa o pravu drugih – ukoliko objavljujemo video na kojima je vidljiva druga osoba moramo i od nje zatražiti i dobiti pristanak za objavu
- Vodimo računa o glazbi u pozadini – glazba spada pod autorski sadržaj i zaštićena je autorskim pravom – video i glazbu drugih autora možemo koristiti ako je izričito navedeno da je besplatno ili smo zatražili i dobili dopuštenje
- Zapamtimo "Bakino pravilo": Upitajmo se je li ono što snimamo ili objavljujemo nešto što bi željeli da vidi naša baka, učiteljica ili roditelj? Ako ne, onda vjerojatno nije dobra ideja objaviti takav video.

ZNATE LI:

- da je 23. travnja 2005. postavljen prvi video naziva „Me at the ZOO", autora Jaweda Karima koji je jedan od osnivača te mrežne usluge? https://youtu.be/jNQXAC9IVRw
- da je Matej Lončarić stručnjak za YouTube sadržaj u Republici Hrvatskoj i pokretač projekta i kanala JoomBoos (kanal koji okuplja najpoznatije YouTubere u Hrvatskoj i regiji)
- da je preko JoomBoos kanala startala kampanja za Anti Cyberbullying čiji sudionik je i HAKOM #SAMOLJUBAV
- da inicijativa Boli Me. pruža podršku mentalnom zdravlju mladih i otvara Muzej empatije...
- Svakako preporučamo posjetu ovoj oazi mira i jednakosti na: https://www.bolime.hr/, a možete ih zapratiti i na: https://youtu.be/6dGGqWRpxDQ

INSTAGRAM

Instagram je jedna od najpopularnijih društvenih platformi za razmjenu slika. Tinejdžeri vole Instagram iz više razloga, ali što je najvažnije, tu su njihovi prijatelji. Također mogu pratiti omiljene slavne osobe, ostale osobe koje su im zanimljive i, naravno, održavati vlastiti profil (ili profile) kojim svojim prijateljima - a ponekad i svijetu predstavljaju sliku o sebi.

Ovisno o tome koga pratite ili što tražite, možete pronaći i puno sadržaja za odrasle. A komentari na objave mogu biti neprimjereni, pogotovo ako je račun javan. Djeca ponekad osjećaju kako moraju održavati savršen profil, pa neprestano skeniraju postove u potrazi za lajkovima i brišu one koji ne zadovoljavaju njihove kriterije. Ipak, uz neke smjernice oko postavki, ograničenja upotrebe i neprekidne razgovore o sadržaju i komentarima, Instagram može biti korisno mjesto za djecu koje im omogućava da se povežu i budu kreativni. Vrste sadržaja koje će djeca vidjeti uglavnom ovise o tome koga slijede: ako prate samo prijatelje i ne traže ništa, možda će vidjeti samo slike svojih prijatelja kako se zabavljaju. Ali djeca rijetko ograničavaju svoje feedove na ljude koje poznaju, pa će vjerojatno vidjeti sadržaj za odrasle. Ako prate poznate osobe, vjerojatno će vidjeti i marketinške oglase. Koristi li se pozitivno, Instagram je mjesto na koje djeca odlaze da bi se povezala s prijateljima. Tinejdžeri ga također koriste za kreativnost, objavljivanje umjetnina, poezije i videozapisa, kako bi pokazali svoje talente. Ako se koristi uravnoteženo s drugim aktivnostima i sa svrhom, djeca se mogu osjećati zadovoljno i prihvaćeno, primjerice, ako dobivaju pozitivne komentare na svoje umjetničke fotografije, slike, pjesme i slično.

SAVJET:

Kako zaštiti svoj Instagram profil?

1. Kako bi zaštitili privatnost možemo blokirati sljedbenike koje ne poznajemo: na listi sljedbenika odaberemo onog kojeg želimo blokirati i nakon pritiska na tri točkice u gornjem desnom kutu odaberemo opciju blokiranja (Block).
2. Možemo i zatvoriti profil za nepoznate. Na profilnom prozoru, kliknemo na tri točkice u desnom kutu i pri dnu tog prozora nađemo opciju Privatni račun (Private account) koju uključimo. Tada samo odabrane osobe mogu pristupiti dijeljenim fotografijama i sadržaju.
3. Uključimo odobravanje označavanja u tuđim fotografijama (tagging). Na taj način moći ćemo odobriti koje se tuđe fotografije na kojima smo označeni mogu pojavljivati na našem profilu.
4. Sigurnost samog Instagram profila može se povećati uključenjem dvofaktorne autentifikacije, tj. kada se netko želi prijaviti na Instagram na nekom uređaju, tada mora upisati i dodatni kod koji stiže na odabrani broj mobitela naveden u profilu. Nakon pritiska na tri točkice u gornjem desnom kutu pritisnite „Two-Factor Authentication“

SNAPCHAT

Snapchat je popularna društvena mreža za razmjenu poruka koja omogućava korisnicima razmjenu slika i videozapisa (zvanih snaps) koji bi trebali nestati nakon što ih pogledaju. Oglašava se kao “nova vrsta fotoaparata” jer je osnovna funkcija snimanje slike ili videozapisa, dodavanje filtara, leća ili drugih efekata i dijeljenje s prijateljima. Na Snapchatu fotografije, a ne tekst, obično započinju komunikaciju. Jednom kada prilagodite svoj snimak, možete ga poslati bilo kome s popisa prijatelja ili dodati u svoju priču, što je zapis dana koji vaši prijatelji mogu gledati 24 sata. Uz pojedinačno slanje poruka, Snapchat nudi i grupno slanje SMS-ova i grupne priče kojima svi u grupi mogu pridonijeti. Možete izbrisati tekstualne poruke koje šaljete, iako će u grupnom chatu drugi ljudi vidjeti da ste nešto izbrisali

Nestaju li poruke zaista na Snapchatu? Ovisi. Ako postavite vremensko ograničenje na trenutak, ono će nestati nakon što ga pregledate. No, primatelji mogu snimiti snimku zaslona slike koristeći svoje telefone ili aplikaciju za snimanje zaslona treće strane. Snimanje zaslona telefona obavijestit će pošiljatelja da je slika snimljena. No, aplikacije trećih strana ne pokreću obavijest. Iz tih razloga najbolje je da tinejdžeri shvate kako ništa što se radi na mreži stvarno nije privremeno. Prije slanja neugodnog snimka sebe ili nekoga drugog, važno je imati na umu kako bi ta snimka mogla kružiti školom već sutra ujutro.

Budući je tako lako pronaći prijatelje na Snapchatu (ovisno o vašim postavkama) ili razmijeniti kodove, tinejdžeri mogu na kraju biti s virtualnim strancima na popisu prijatelja. Iz različitih razloga to može biti rizično, pa je najbolje razgovarati sa svojim tinejdžerima o tome kada je sigurno dodati ljude.

SAVJET:

Kako zaštiti svoj Snapchat profil?

1. Pod opcijama (Settings) pronađimo „See My Location“ i odaberimo „My Friends“ ili još bolje „Ghost Mode“ – (mogućnost ne prikazivanja lokacije)
2. Obratimo pažnju na obavijesti za vrijeme komunikacije putem Snapchat-a – Snapchat će nam javiti ako je netko s druge strane napravio screenshot Vaše poruke
3. Pripazite na javno dijeljenje svog Snapchat korisničkog imena čak i ako ste ograničili tko Vas može kontaktirati
4. Sačuvane poruke koje se nalaze u sjećanjima (Memories) možemo dodatno učiniti sigurnijima tako da ih označimo s „My Eyes Only“ što će napraviti posebnu, PIN-om zaštićenu galeriju, tako da ako nekome i pokazujemo prijašnje poruke one koje smo označili s „My Eyes Only“ neće biti među njima

Videoigre

Videoigre su igre koje omogućuju istraživanje i kreativno izražavanje - umjesto nametanja krute strukture – jako su dobre za učenje jer potiču kritičko razmišljanje, rješavanje problema i sistemsko razmišljanje (učenje kako stvari rade zajedno). Dogovorite s djetetom vrijeme koje ono smije dnevno provoditi na internetu i igranju videoigara.

Roblox

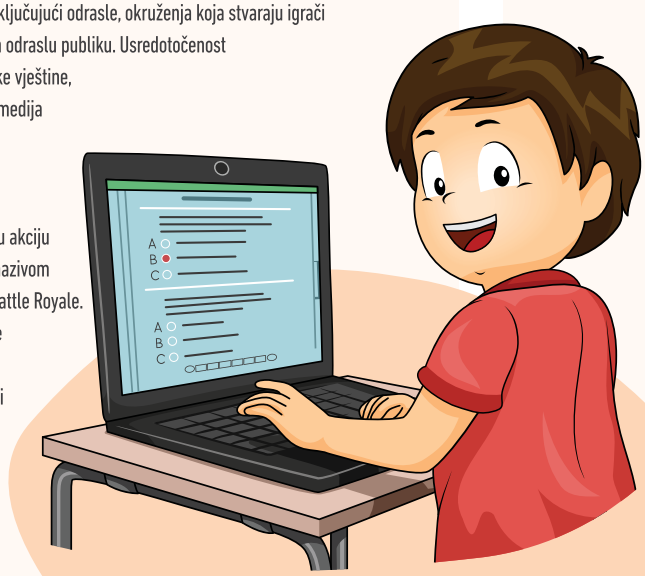
Videoigra unutar koje možete igrati igre i mape koje su dizajnirali drugi korisnici i stvarati i dijeliti vlastite igre koristeći Robloxov vlastiti alat za razvoj igara. Jednom kada se prijavite, možete igrati beskonačan broj igara, graditi i dijeliti kreacije i razgovarati s drugim korisnicima - i sve besplatno. Ako vaša djeca igraju Roblox, trebat će im Robux i vjerojatno će se htjeti pretplatiti na Builders Club, koji pruža dodatne značajke uz članarinu. Roblox potiče korisnike na interakciju putem svoje funkcije Chat & Party. Sav je chat filtriran, što znači da je neprimjeren jezik zamijenjen hashtagovim simbolima. Razgovori s djecom mlađom od 13 godina filtrirani su više. Roblox također zapošljava moderatore koji paze na neprikladan jezik i sadržaj. Kao i u bilo kojoj drugoj videoigri, benefita ima mnogo, ali s obzirom da se radi o online igri, uvijek postoji opasnost od zlonamjernih ljudi.

MINECRAFT

Minecraft je avanturistička videoigra. Stil se naziva "sandbox" (pješčanik) jer pruža kreativni krajolik bez fiksnog cilja i beskrajnih je mogućnosti. Njegov kockasti dizajn također je prilično dječji: glave likova su četvrtaste, boje se pojavljuju u komadima, pa čak i drveće izgleda kao da je uzgojeno u Lego laboratoriju. Kao i svako igralište, Minecraft ne dolazi s uputama, a relativno ga je jednostavno podići i igrati. Igru učite istraživanjem, eksperimentiranjem, gledanjem YouTube videozapisa i čitanjem drugog sadržaja stvorenog od obožavatelja. Minecraft je vrlo siguran za djecu. Primjerice, u kreativnom načinu za jednog igrača nema interakcije s drugima i sukoba. No, s vremenom se većina djece želi igrati s drugima, a igranje više igrača donosi određene rizike. Iako su Minecraft zajednice uglavnom pozitivne, a moderatori poslužitelja odgovorni su za održavanje reda, djeca se mogu izložiti psovkama, maltretiranju, pa čak i govoru mržnje. Ni Minecraft nije imun na grabežljivce, a budući da ljubitelja igre ima u svim dobnim skupinama, uključujući odrasle, okruženja koja stvaraju igrači mogu sadržavati bitke, seksualne scenarije i drugi sadržaj primjereniji za odraslu publiku. Usredotočenost Minecrafta na izgradnju može ojačati koncepte geometrije, jer jača logičke vještine, kreativnost, pa čak i suradnju igrača, ali obrazovna vrijednost bilo kojeg medija ima puno veze s onim tko vodi učenje.

Fortnite

Fortnite je videoigra koja uzima elemente iz „sandbox" igara i dodaje brzu akciju pucnjave iz trećeg lica. Postoje dva načina igre: samostalna verzija pod nazivom Save the World i izuzetno popularna verzija za više igrača pod nazivom Battle Royale. Za neke roditelje crtani, beskrvni stil radnje u Fortniteu čini nasilje manje problematičnim od agresivnih krvarenja u drugim popularnim pucačkim igrama. Ali s obzirom kako se radi o online igri, opasnost se može pojaviti u chatu u igri - posebno u Battle Royaleu - mogla bi izložiti mlađe igrače uvredljivim riječima ili neprimjerenim sadržajima slučajnih stranaca.

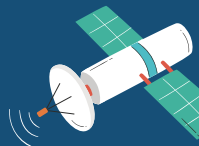


STVARAJU LI VIDEOIGRE OVISNOST?

Svjetska zdravstvena organizacija (WHO) identificirala je stanje koje se naziva poremećaj internetskih igara (IGD), a koje bi, prema njihovoj ocjeni, moglo biti vrsta ovisnosti, premda je potrebno još istraživanja. Ali IGD je rijedak i često može biti povezan s drugim stanjima kao što su depresija i ADHD, jer videoigre ne stvaraju ovisnost same po sebi. Iluzija uspjeha u virtualnom svijetu čini igre privlačnima, ali samo iz razloga što neki tinejdžeri igre ne koriste kao zabavu, već im ona služi kao bijeg od pravih problema i stvarnosti s kojom se svakodnevno suočavaju (disfunkcionalne obitelji, vršnjačko nasilje, osjećaj neprihvaćenosti).

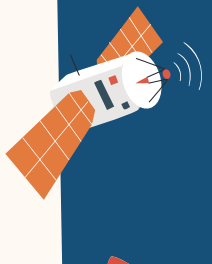
5G KAO NAŠA SKORA BUDUĆNOST

Kao i do sada, i s 5G tehnologijom vrijede sva pravila vezana uz sigurnu uporabu internetskih aplikacija kojih se treba pridržavati. A nove aplikacije i nove mogućnosti donijet će i nova pravila kako bismo i dalje sigurno plovili internetom. Također, vrijeme provedeno s pametnim uređajima bez obzira koriste li oni 5G ili 4G tehnologiju, treba ipak biti razumnog trajanja. Najbitnije karakteristike 5G tehnologije su velike brzine, visoka razina pouzdanosti te malo kašnjenje signala. To znači da će se aplikacije koje danas koristiš pokretati brže, da će zvuk i slika biti kvalitetniji i da će se razvijati nove aplikacije u svim područjima života.



Znaš li da će:

- svi građani RH moći imati jednako kvalitetan pristup internetu
- on povećati potrebu za novim radnim mjestima
- gradovi postati „pametni" (regulirati će tako razinu električne energije, popunjenost parkinga, potrebu za odvozom smeća)
- automobili međusobno „pričati" i dijeliti informacije kojma će se optimizirati promet i spriječiti nesreće
- posao i videoigre biti u „oblaku" (programu, dokumentu može se pristupiti s većeg broja uređaja, u bilo koje vrijeme i s različitih lokacija uz internetsku vezu)
- videoigre biti u „realnom" vremenu
- se unaprijediti rješenja u industriji, poljoprivredi, području javne sigurnosti, financijskih usluga, zdravstvu te energetici
- se još snažnije razvijati umjetna inteligencija (AI). Za one željne znanja na linku https://www.elementsofai.com/hr/ nalazi se tečaj o osnovama AI. On je besplatan, traje 6 tjedana, dobiva se potvrda i čak 2 ECTS boda!



Digitalne vještine biti će još važnije, a razumijevanje tehnološkog napretka nužno. Unatoč čarima virtualnog svijeta, nemojte zaboraviti ljepote stvarnog. Razvoj tehnologije omogućuje pružanje novih usluga i aplikacija čiji korisnici nisu više samo ljudi nego i uređaji koji će unositi i razmjenjivati veliku količinu osjetljivih podataka na mreži, što povećava potrebu zaštite računalne "imovine" i kibernetičke sigurnosti - cybersecurity.

HAKOM
www.hakom.hr, zastita-djece@hakom.hr

Centar za sigurniji Internet
www.csi.hr/ tel. 0800 606 606 – besplatan i anoniman telefon
za pomoć i podršku u slučaju nasilja na internetu

Hrabri telefon
www.djeca.hrabritelefon.hr/ tel:116111, 0800 0800

Poliklinika za zaštitu djece i mladih Grada Zagreba
www.poliklinika-djeca.hr/

ANONIMNA PRIJAVA ILEGALNOG SADRŽAJA
www.csi.hr/hotline/

redbutton.gov.hr

Aplikacija Ministarstva unutarnjih poslova
- namijenjena je svima, ali je posebno prilagođena djeci i omogućuje prijavljivanje sadržaja na internetu za koji sumnjate da je nezakonit i odnosi se na različite oblike iskorištavanja ili zlostavljanja djece

EU Kids Online
www.hrkids.online

Prati JoomBoos anti-cyberbullying kampanju, pridruži nam se u borbi protiv online i svih drugih oblika nasilja i pokaži da ti podržavaš **#SAMOLJUBAV!**

Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva,
Laboratorij za asistivne tehnologije i potpomognutu komunikaciju, http://lab.ict-aac.hr/

Ova brošura prvenstveno je namijenjena roditeljima i njihovoj djeci u osnovnoj školi, ali može biti koristan izvor informacija svakomu tko želi više znati o temi ponašanja i sigurnosti djece na internetu.

Brošura je rezultat suradnje HAKOM-a, Centra za sigurniji internet i Ministarstva znanosti i obrazovanja.

HAKOM
HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

csi.hr Centar za sigurniji internet

Ministarstvo znanosti i obrazovanja