

Александар Миладиновић, ма



**ПРИРУЧНИК ЗА ПРЕВЕНЦИЈУ НЕГАТИВНОСТИ
ДРУШТВЕНИХ МРЕЖА**
за родитеље



**PRAVDA
ZA SVAKO
DIJETE**



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Švicarska agencija za razvoj i saradnju SDC



Švedska
Sverige

unicef



Бања Лука, 2018. године

**ПРИРУЧНИК ЗА ПРЕВЕНЦИЈУ НЕГАТИВНОСТИ
ДРУШТВЕНИХ МРЕЖА
за родитеље**

Аутор:
Александар Миладиновић, мр

Издавач:
Министарство унутрашњих послова Републике Српске
Управа за полицијску обуку,
Бања Лука

За издавача:
Др Миле Шикман

Лектор:
Јелена Шкрбић, мастер српског језика и књижевности

Штампа:
Графид, Бања Лука

Тираж:
1 000 примјерака

Приручник је резултат активности које Министарство унутрашњих послова Републике Српске спроводи у оквиру УНИЦЕФ пројекта „Правда за свако дијете”.

На реализацији ове пројектне активности, осим аутора, ангажовани су:

1. **Вања Чекић**, ма, Служба министра,
2. Др **Мирослав Ђурић**, организациона јединица Директор полиције,
3. **Свјетлана Бијелић**, Управа криминалистичке полиције,
4. Др **Николина Грбић-Павловић**, Управа за полицијску обуку.

Ставови и мишљења изнесени у овој публикацији су ставови аутора и не одражавају нужно политике и ставове УНИЦЕФ-а, Швајцарске или Шведске.

С А Д Р Ж А Ј

Предговор	5
Феноменологија негативности на друштвеним мрежама	7
<i>Крађа профила – компромитација идентитета</i>	<i>7</i>
<i>Сквотинг (запосједање) идентитета</i>	<i>10</i>
<i>Електронско вршњачко насиље</i>	<i>11</i>
<i>„Хејтерске” активности</i>	<i>15</i>
<i>Секстинг, глуминг и сексторжн</i>	<i>16</i>
<i>Уијењивање и изнуђивање</i>	<i>19</i>
<i>Самоубиства</i>	<i>21</i>
Нетикеција – правила понашања на друштвеним мрежама	23
<i>Посебна правила понашања за дјецу на друштвеним мрежама</i>	<i>33</i>
Конкретни савјети родитељима	37
Реаговање на злоупотребе и негативности на друштвеним мрежама	45
<i>Алармирање администратора на друштвеним мрежама</i>	<i>45</i>
<i>Пријављивање кривичних дјела на полицији</i>	<i>48</i>
Превентивне активности Министарства унутрашњих послова Републике Српске на предупредивању негативности друштвених мрежа	51
Коришћена литература	53

Предговор

Приручник за превенцију негативности друштвених мрежа је намијењен родитељима ученика основних и средњих школа који имају профиле на друштвеним мрежама. С обзиром на то да су родитељи мање упознати са правилима понашања на друштвеним мрежама, а и родитељи и ученици су веома мало упознати са безбједносним изазовима, ризицима и опасностима које вребају ученике на друштвеним мрежама, циљ приручника јесте да надомјести то незнање, односно да родитељима пружи солидну основу како би виртуелну егзистенцију дјече подigli на виши заштитни ниво дајући савјете дјече, инсистирањем на поштовању одређених правила, али и надзирањем поштовања тих правила.

Родитељи ће се у приручнику упознати са најучесталијим облицима санкционисаног, забрањеног, негативног, неподноумијевааног и непожељног понашања усмјереног ка дјечи или гдје су дјеца најчешће жртве, што ће се поткријепити и илустративним примјерима. Услед обима приручника, разумљиво је да се неће навести сви облици негативности на друштвеним мрежама, већ само најучесталији, оно чега родитељи треба да буду свјесни, те савјети да се властитим ангажманом информишу и о другим, новијим облицима испољавања негативности према дјечи током њиховог коришћења интернет ресурса.

Главни дио приручника се односи на правила понашања на друштвеним мрежама, на нетикецију друштвених мрежа које је пожељно да се придржавају сви интернаути како би се предуприједило и елиминисало друштвено непожељно, неподноумијевааног и забрањено понашање на друштвеним мрежама. Посебно су прецизирана правила понашања на Фејсбуку и Инстаграму, као друштвеним мрежама које је ученичка популација готово акламативно прихватила.

Трећи дио приручника се односи на мјесто и улогу релевантних субјеката на проактивном и репресивном дјеловању негативности на друштвеним мрежама. Даје се приказ алармирања администратора друштвених мрежа на испољене негативности, те на улогу и могућности школе да реагује на одређене негативности према ученицима које своје манифестације или посљедице имају и у интернет окружењу. Такође, приказана је и процедура пријаве полицији свих понашања која имају елементе кривичних дјела, а испољавају се преко друштвених мрежа или чија је посљедица манифестована у окружењу друштвених мрежа.

Приручник за превенцију негативности на друштвеним мрежама је резултат превентивних активности које Министарство унутрашњих

послова реализује у сарадњи са УНИЦЕФ-ом у склопу пројекта „Правда за свако дијете”. Циљ ових превентивних активности које полиција спроводи у Републици Српској јесу сензибилизација, освјешћивање, информисање и едукација родитеља, наставног особља и ученика о негативностима на друштвеним мрежама, те о механизмима проактивног, превентивног и репресивног реаговања на ове негативности.

Дио садржаја је преузет из ауторове књиге "Фејсбук и криминалитет" (издавач Интернационална асоцијација криминалиста, Бања Лука, 2013. године), који је преформулисан, иновиран и прилагођен циљу и намјени приручника. Примјери наведени у приручнику су углавном "домаћи". Приликом навођења примјера, коришћена је неопходна анонимизација.

У Бањој Луци, септембар 2018. године

Аутор

Феноменологија негативности на друштвеним мрежама

Крађа профила – компромитација идентитета

Ученик је имао профил на Фејсбуку, са корисничким именом и лозинком коју је само он знао. У интернет играоници, док је са другим играо игрицу преко свог налога, на брзину је приступио и профилу на Фејсбуку да би видео шта је ново. Доласком кући, покушао је са кућног рачунара да приступи Фејсбуку, међутим, није успио. Сутрадан су га у школи његови другови вербално напали због статуса које је претходне ноћи постављао на Фејсбуку, иако је он узалудно покушавао да им објасни да он није ништа постављао на Фејсбук, јер није успио да приступи свом налогу.

...

Ученик је отишао на љетовање у Црну Гору са родитељима. Свакодневно је постављао слике на Инстаграм и на Фејсбук са властитог мобилног телефона, користећи се ролинг услугама, међутим, веома брзо је испразнио рачун. Како не би трошио џепарац на ролинг, отишао је у оближњи интернет кафе-бар одакле је приступио својим профилима, након чега је фотографије са телефона пребацио на рачунар, а потом их поставио на своје профиле. Наредног дана, из угоститељског објекта је покушао да приступи својим налозима, међутим, није успио. Како није имао на рачуну, сачекао је повратак кући да фотографије постави на своје профиле, мислећи да је интернет веза у објекту била слаба. Када је дошао кући, најбољи друг му је тражио поврат новца који му је послао у Црну Гору, с обзиром на то да је то ученик тражио преко порука послатих са властитог профила на Фејсбуку. Садржај порука је гласио: „Украли су ми телефон на мору, као и новчаник са џепарцем. Срамота ме је рећи то родитељима. Молим те, пошаљи ми нешто новца на овај рачун, а ја ћу ти вратити када се вратим. Ово је рачун од друга којег сам упознао на мору.”

...

Ученик је у стану користио властиту бежичну мрежу, међутим, с обзиром на то да је интернет веза била слаба, повезивање на интернет је неријетко било споро. Након неколико дана, видео је да је стан на трећем спрату зграде у којој је живио покривен неким другим бежичним сигналом који није био закључан.

Иако није знао чији је то сигнал, ипак је преко тог сигнала приступио интернету, а потом и свом профилу на Инстаграму. Након тога, наставио се дописивати са пријатељима и пратиоцима на друштвеним мрежама. Неколико дана потом, није се успио више повезати ни на један профил на друштвеним мрежама на којима је имао налог, да би потом преко „месенџера“ добио поруку да мора уплатити одређени износ новца, иначе ће се одређена комуникација коју је имао са дјевојкама преко Инстаграма и Фејсбука открити и поставити на тим мрежама преко његовог профила.

...

Наведени примјери су најилустративнији примјери онога што ученици називају „хаковањем” или крађом профила, што подразумева компромитацију идентитета ученика сазнањем и преузимањем његових идентификационих и аутентификационих података на профилима које има на интернет сервисима.

За компромитацију туђег профила крађом (или када се на други начин преузме контрола над туђим профилем) није потребно завидно програмерско и информатичко знање, ту крађу (могу да) реализују и корисници са просјечним информатичким знањем, познавањем рада интернета. Другим ријечима, крађу профила могу да изврше и корисници који нису посебно едуковани, односно није потребно посебно информатичко, а поготово не програмерско знање за овај вид криминалне активности, већ може да га врши и већина интернаута уколико знају основе рада на интернету, а поготово у окружењу одређених друштвених мрежа (Фејсбука, прије свега).

Реализује се разним видовима компромитације профила, без обзира на то да ли се ради о „проваљивању“ лозинке и корисничког имена или се на други начин преузима контрола над профилем жртве. Начини крађе на овај начин су бројни, а најчешће се користе тзв. „пецање“, односно фишинг, али се профили краду и уз помоћ тзв. „килогера“, крађом рачунара и телефона, одавањем корисничког имена и лозинке, „проваљивањем“ лозинке нагађањем...

Иако крађа профила може да буде и сама себи циљ, чешћи су случајеви да је крађа профила само метод, односно начин за реализацију других криминалних активности, најчешће превара и разних „хејтерских“ активности. Уколико се жели нанијети штета ученику или се он жели омаловажити, најчешће ће крађа профила имати тај циљ, без предузимања додатних криминалних активности преко тако украденог профила. Наравно, на украденом профилу ће се предузимати одређене активности којима ће се нанијети штета, најчешће неимовинска, интернауту. Међутим, чешћи су случајеви у којима се крађа профила реализује да би се преко тако украденог профила, користећи се идентитетом другог лица које је жртвама најчешће познато, односно у које жртве имају повјерење, лакше реализовале криминалне активности, попут „хејтерских“ активности или „секстинга“.

Шта се може сазнати из преузетог или компромитованог профила? На основу приступа самом профилу може се сазнати мноштво информација о самом кориснику, као и о његовој приватности, што представља сигурно један од најдрастичнијих облика нарушавања његове

приватности уопште, а поготово дигиталне приватности. Конкретно, на основу увида у садржај профила приступом туђем профилу, злонамјерни корисници могу да сазнају идентитет пријатеља тог корисника, његову комуникацију са пријатељима, укључујући и садржај, ток и учесталост те комуникације (што је свакако један од најдрастичнијих облика нарушавања његове приватности), придруженост и посјећеност одређеним страницама и групама (што такође може за њега да буде компромитујуће), податке интимне (и друге) природе ван интернет окружења (за које је разумљиво да могу да буду компромитујући, а да се не говори да такође представљају драстично нарушавање приватности). Надаље, може се компромитовати и приватност других интернаута, имајући у виду потенцијалну повезаност корисника компромитованог профила са другим корисницима. Усљед наведеног, потенцијална штета која настаје компромитацијом туђег профила не може се посматрати само у контексту његове нарушене приватности, већ то може да има негативан утицај и на његове пријатеље, па чак и на интернауте са којима није у директној комуникацији (већ у оквиру група или страница, на примјер).

На примјер, уколико корисник преко Фејсбука одржава приватну комуникацију са другим корисницима, разумљиво је (требало би) да су наведеног свјесни само он и корисник са којим одржава ту комуникацију. Међутим, компромитацијом његовог профила, злонамјерни корисник има увид у садржај те комуникације, те уколико сматра да она може да послужи у његове нелукративне сврхе компромитације профила, може да, на разне начине, представи јавности (на примјер, у оквиру Фејсбук заједнице објављивањем тог садржаја на новостима или на зиду корисника компромитованог профила или на сличан начин). Разумљиво је да ће се у овом случају нарушити и приватност, односно нанијети штета и том другом кориснику са којим је корисник компромитованог профила одржавао комуникацију која је, за њега или за обоје, на одређени начин или према одређеним субјектима или одређеној популацији компромитујућа.

Крађа профила изузетно тешко погађа ученике, поготово што су свјесни, свјеснији него њихови родитељи шта се све може компромитујуће сазнати из профила и шта се све са компромитованим профилем може урадити како би се нарушио углед ученика или како би се њему нанијела одређена увреда, понижење, омаловажавање или нека друга штета.

Сквотинг (запосједање) идентитета

Ученик који је био популаран у школи није имао профил на друштвеним мрежама. Пред крај љетњег распуста, с обзиром на то да није живио у граду гдје је већина његових другова живјела, није имао већи контакт са својим друговима, па чак ни телефоном. Када је почела нова школска година, примијетио је да га доста његових другова избјегава, док су га неки почели отворено оговарати, а неки чак и пријетити. У почетку није схватао о чему се ради, да би му потом један друг показао профил на Фејсбуку са његовим идентитетом (личним подацима и профилном фотографијом) преко којег се исмијавају, понижавају и омаловажавају његови другови из школе. Узалудно је у почетку објашњавао да то није његов профил, те да он уопште не користи друштвене мреже, да би тек након извјесног времена други ученици схватили да му је неко запосјео дигитални идентитет.

...

Од стране школског друга на Фејсбуку је креиран профил тринаестогодишње дјевојчице гдје је насилник за профилну фотографију поставио њену (фотошопирану) фотографију у доњем вешу, а профил креирао под њеним именом. Веома брзо се о њој причало као о „малољетној порно диви“, а убрзо су и формиране групе на Фејсбуку преко којих су дјевојчици слали непристојне понуде, али су јој и пријетили, понижавали је, вријеђали, исмијавали...

...

Једна средњошколка је доживјела нервни слом услед креирања лажног профила на њено име и са њеном фотографијом и другим личним подацима. Из сличних разлога, такође једна средњошколка је побјегла од куће, плашећи се реакције родитеља када виде њен непримјерен профил, односно њен профил компромитован непримјереним садржајем.

...

Претходно описани случајеви су примјер „сајбер-сквотинга“ или запосједања идентитета – облици компромитације идентитета који се састоје од неовлашћеног и неодобреног, те тајног креирања профила одређене особе, која најчешће и не посједује профил на одређеном интернет сервису или друштвеној мрежи, услед чега неће бити благовремено информисана да је о њој креиран профил.

„Сајбер-сквотинг“ подразумева да се креира профил на туђе име, а потом да се води, ажурира, а самим тим и експлоатише идентитет тог лица, што ће најчешће водити и одређеној компромитацији идентитета тог ученика. Може се очекивати да ће креатор тог профила и ступити у контакт са учеником чији идентитет на профилу користи и експлоатише, те ће му понудити могућност преузимања контроле на профилу, наравно уз одређену надокнаду. Уколико жртва не пристане на наведено, није тешко претпоставити да би креатор тог профила могао на одређене начине да компромитује идентитет ученика (слањем непристојних порука, постављањем непристојних фотографија или

снимака, алузијом на одређене карактеристике ученика, вријећањем других ученика или професора...). Наравно, креатор лажног профила тако зна да компромитује ученика на чије име је направио профил, чега је свјестан и сам ученик, те ће најчешће подлећи уцјенама креатора профила. Саму експлоатацију у овом случају не треба посматрати кроз материјални аспект (који није занемарив, али није једини), јер се жртви, с једне стране, може и на разне друге начине наносити штета, док, истовремено, и сам нападач може да остварује одређену корист преко запосједнутог профила, чак и уколико нема интеракцију са жртвом.

Један од начина „сајбер-сквотинга“ се односи и на креирање страница (ријеђе и група) у којима се именом, профилном фотографијом, подацима на страници, постављеним садржајем, комбиновано или на друге сличне начине имплицира да се ради о званичној страници одређеног удружења, групе, разреда, одјељења, школе, спортског клуба...

Креирање лажног профила је противно правилима друштвених мрежа, поготово Фејбука, услед чега је администраторе друштвених мрежа потребно обавијестити о свим лажним профилима.

Електронско вршњачко насиље

Неколико ученика петог и шестог разреда основне школе су основали групу у којој су отворено позивали на убиство наставнице математике. Оснивање групе је наишло на одобравање и других ученика, који су се учланили у групу, у оквиру које су постављали коментаре да им „наставница није по вољи“, „не воле математику“, „не разумију предавања“... У групу се учланило око 200 ученика.

...

Четрнаестогодишња ученица основне школе доживјела је шок зато што су је школски другови исмијавали на Фејсбуку због њене урођене срчане мане. Конкретно исмијавање је интензивирано након што су ученици поставили њену фотографију на којој се види разроност, што је само потенцирало низ увредљивих и подсмјешљивих коментара.

...

Ученици су преко Вибера формирали групу у којој су били сви ученици из једног одјељења (као и неколико ученика из другог одјељења), сем једног ученика који се замјерио ученику креатору групе. Након тога, креатор те групе је у оквиру групе коментарисао изглед и облачење изопштеног ученика, његово понашање, социјални статус и слично, што је немали број осталих ученика чланова групе одобравао, лајковао, те је чак и поткрепљивао изнесене наводе властитим коментарима. То је трајало око мјесец дана, што изопштени ученик није знао, иако је примјећивао да се око њега сваки дан ученици дошаптавају и да му се смију. Тек након мјесец дана, један ученик из групе који се претходно посвађао са креатором групе, изопштеном ученику је показао садржај групе и коментаре унутар ње. Епиог је да је следећег дана изопштени ученик дошао у школу са ножем, те је покушао избостити креатора групе.

...

Петнаестогодишња жртва је на Фејсбуку писала о „сексуалним нестаишлацима“ своје најбоље пријатељице, што се њој, а поготово њеном момку није свидјело, услед чега су њих двоје „унајмили“ заједничког петнаестогодишњег пријатеља, платили му око 100 евра (обећавајући да ће му увијек плаћати пиће када га сретну у граду), након чега је он убио жртву.

...

„Хејтерске активности“ (чији примјери су претходно наведени) јесу садржај електронског вршњачког насиља, увелико распрострањених облика негативности који се реализују у интернет окружењу, иако своје последице имају и у реалном окружењу, што је видљиво из претходно наведених примјера.

Фејсбук се сматра „идеалном“ локацијом за реализацију насилних активности и за пласирање насилних садржаја вршњачког насиља. Разлог је, примарно, Фејсбук окружење које насилнику омогућава анонимност дјеловања и мноштво могућности, док жртви онемогућава бијег и (ефикасну) заштиту. Поред наведеног, масовност корисника Фејсбука, поготово вршњачке популације, као и брзина ширења одређених садржаја на Фејсбуку међу корисницима и локална фокусираност и концентрисаност корисника, свакако омогућавају експанзију насилних садржаја и активности вршњачког насиља на Фејсбуку.

Насилни садржаји чији је циљ да угрозе жртву вршњачког насиља се најчешће пласирају преко новости постављањем увредљивих, понижавајућих, пријетећих и сличних негативних коментара тако да их види што већи број интернаута. На тај начин се насилни садржај (без обзира на то да ли је постављен у виду текстуалног коментара, фотографије, снимка...) веома брзо шири међу корисницима, односно за кратко вријеме га велики број корисника прихвата, неријетко га преузимајући и даље ширећи. Штавише, „лајковање“ садржаја, с једне стране, корисницима наговјештава да се ради о „занимљивом“ садржају, услед чега ће га погледати, док, с друге стране, „лајковање“ негативних насилних садржаја код жртве ствара још већу потиштеност и повученост, која вјерује да „лајковање“ значи и одобравање, односно подржавање наведеног (што, наравно, неријетко и јесте тако).

Специфичност електронског вршњачког насиља везана је и за „таговање“ (означавање) непримјерених и неприкладних фотографија жртвиним именом, уколико жртва има профил на конкретној друштвеној мрежи. Ово је посебно распрострањен облик вршњачког насиља на Фејсбуку и на Инстаграму, с обзиром на велику могућност постављања фотографија на овим друштвеним мрежама, имајући у виду да

интернауту могу постављати властите, али и туђе фотографије, па чак и непримјерене и неприкладне фотографије „скинуте“ са интернета, што дјелује посебно понижавајуће и исцрпљујуће за жртву, с обзиром на то да се ово континуирано реализује од стране насилника дужи период.

Оно што електронско вршњачко насиље чини посебно погубним за жртву јесте масовност корисника, као и локална фокусираност већине млађих интернаута, а поготово насилника, пасивних субјеката (посматрача) и жртве. Масовност интернаута је поготово велика међу вршњачком популацијом. Уколико се томе дода да већина ученика за пријатеље има интернауте и из локалне средине, јасно је да се насилни садржај свакако веома брзо шири у оквиру средине из које су, најчешће, и насилник и жртва, као и пасивни посматрачи.

Злостављач, односно насилник који продукује електронско вршњачко насиље је најчешће анониман или се крије под псеудонимом иза лажних или компромитованих профила услед чега максимизира властиту активност без опасности како од откривања, тако и од потенцијалне жртвине освете. Наведено је и један од фактора ескалације овог облика насиља.

Електронско вршњачко насиље је погубно по жртву и услед интегрисаности ученика у одређене групације, из којих, најчешће, потичу и жртва и нападач, као и сами посматрачи. Те групације се најчешће односе на школску популацију, популацију вршњака из улице или насеља, популацију који имају слична интересовања (спортска, едукативна, умјетничка...). Надаље, ова врста насиља је погубна имајући у виду чињеницу да се „публика“ у виду намјерних или случајних посматрача може повећавати екстремном брзином, превазилазећи локалне, узрасне или популацијске границе.

За разлику од класичних облика испољавања вршњачког насиља, у оквиру којег су и жртва и злостављач припадници истог миљеа (школе, улице, насеља), код електронског вршњачког насиља жртва уопште не мора да буде корисник Фејсбука, а да се према њој примијењују многобројне активности из дијапазона вршњачког насиља.

Овом облику насиља жртва је изложена константно и континуирано, без обзира на то гдје се налазила. Другим ријечима, жртва вршњачког насиља које се конкретизује коришћењем интернет сервиса је њему изложена сваки минут, сваки час и сваки дан, с обзиром на то да је компромитујући материјал посматрачима константно доступан преко профила злостављача, групе или странице креиране у те сврхе или преко других могућности на друштвеним мрежама.

Електронско вршњачко насиље је посебно погубно по жртву, с обзиром на то да, за разлику од вршњачког насиља у реалном окружењу, оно не престаје смиривањем или елиминисањем нападача. Другим ријечима, садржај вршњачког насиља, уколико се постави на друштвену мрежу или сличан ресурс интернета (без обзира на то да ли се ради о текстуалном, видео, музичком, сликовном, илустративном, графичком или сличном садржају) може да се шири и умножава међу другим интернаутима и након што га сам нападач повуче или избрише, услед чега жртва осјећа посљедице и након саме „хејтерске“ активности у виду постављања компромитујућег или омаловажавајућег садржаја. Такође, само вршњачко насиље, односно посљедице вршњачког насиља не престају дистанцирањем од миљеа у којем се налази злостављач и посматрачи, већ се оно наставља, с обзиром на распрострањеност интернаута.

С обзиром на могућности анонимног и псеудонимног дјеловања на интернету, као и на многобројне манипулације лажним или украденим идентитетима кроз лажне профиле, жртва често и не зна од кога потиче вршњачко насиље, нити ко даље продукује само насиље. Исто тако, примарна жртва може, преко лажног или компромитованог профила, да буде испровоцирана према наводном злостављачу и у циљу освете према њему продукује активности вршњачког насиља, а потом он, као секундарна жртва, намјеравајући да се освети примјењује према примарној жртви вршњачко насиље и тако унедоглед, иако ни један ни други нису иницирали само насиље.

Електронско насиље може да се манифестује, као посљедица, и конкретизацијом физичког насиља према жртви, али и према злостављачу. Физичко насиље према жртви ће најчешће предузети или злостављач или неко од посматрача у циљу повлађивања злостављачу или „доказивања“ властите слике о себи у оквиру групације којој припада, док ће жртва према злостављачу физички реаговати услед освете.

Услед освете је могуће и да сама жртва покрене и продукује многобројне облике вршњачког насиља према злостављачу, што доводи до креирања круга вршњачког насиља који најчешће има импликације и на друге интернауте, односно посматраче и једног и другог насиља.

Електронско вршњачко насиље је изузетно тешко елиминисати након његове појаве, а поготово након његове ескалације, услед чега се треба превентивно реаговати како до њега уопште не би дошло или како би се оно ефикасно предуприједило већ приликом саме почетне манифестације. Нажалост, и међу младима, а како се чини и међу

одраслима, увријежено је мишљење да насиље путем интернета може проћи некажњено и да ни одрасли, а ни дјеца не могу учинити ништа да би се тај вид насиља зауставио.

„Хејтерске“ активности

У контексту вршњачког насиља неизоставно је да се помену и тзв. „хејт групе“, поготово услед своје масовности и погубности. „Хејт групе“, односно групе мржње су групе интернаута ученичке популације које се креирају са циљем пропагирања мржње према одређеној личности, популацији људи са одређеним карактеристикама, према одређеној идеји или друштвеној вриједности... У оквиру тих група се пропагира мржња, па чак и насиље према жртвама, на разне начине, од којих су најучесталији облици вербално, сликовно, графичко, али није занемариво (у задње вријеме) ни својеврсно програмерско насиље (креирање програма, односно игрица у којима се популарише мржња према одређеној жртви). Ове групе готово увијек имају велики одјек у јавности, поготово у интернет окружењу. Посебно су „популарне“ у оквиру друштвених мрежа, односно на Фејсбуку, мада нису непознаница ни на другим услугама интернета. У задње вријеме се и Вибер све више појављује као платформа преко које се креирају тзв. „хејтерске“ групе преко којих се или у оквиру којих се пласирају „хејтерски“ садржаји и „хејтерске“ активности.

Примијетно је да се свакодневно повећава број група на Фејсбуку које самим својим именом пропагирају одређену нетрпељивост, изопштеност или друге врсте насиља према одређеној жртви из вршњачке популације. Најчешће и само име групе асоцира на нетрпељивост према жртви („Сви ми који мрзимо...“, „Ко мрзи...“, „Фотографије и снимци голе...“), што додатно наноси психичке патње жртви. Надаље, масовност ових група, као и сами коментари који нису пријатни и охрабрујући за жртву додатно утичу на угроженост саме жртве, која се све више, услед наведеног, али и низа других разлога, повлачи у себе, избјегава коришћење интернета и Фејсбука, али и избјегава друштвене контакте, па и школске обавезе. Угроженост жртве формирањем ових група је условљена и чињеницом да су чланови групе најчешће интернаути из непосредног миљеа у оквиру којег и сама жртва егзистира (школа, улица, насеље, град), што додатно утиче на њену виктимизованост. Код ових група, примјетно је да их креирају, односно да се на овај начин са својим вршњацима најчешће „обрачунавају“ кориснице (женски пол), као и

корисници млађе животне доби, па чак и корисници који имају мање од 13 година.

Један од начина испољавања овог облика електронског вршњачког насиља преко Вибера јесте и креирање група на Виберу из којих се изопштава дио ученика или само један ученик, што чини тзв. социјално вршњачко насиље потпомогнуто технологијом.

Секстинг, глуминг и сексторжн

Петнаестогодишњакиња је упала је у замку једног сексуалног грабежљивца који јој је уништио живот и на крају је довео до самоубиства. Она је набавила веб камеру како би се дружила са пријатељима и упознала нове људе. Тада је направила кобну грешку – фотографисала се у топлесу. Годину дана касније преко Фејсбука јој се јавио човјек који је некако дошао у посјед њене фотографије у топлесу. Пошто није жељела да има ишта са њим, он јој је запрјетио да ће послати фотографију свима. Знао је све о њој, њену адресу, у коју школу иде, ко су јој рођаци и пријатељи. И испунио је пријетњу. Амандину фотографију прослиједио је свима, а на Фејсбуку је чак креирао профил и за профилну фотографију ставио фотографију на којој је Аманда обнажена. Услиједило је вршњачко злостављање, промјена школе, депресија, дроге, алкохол, а све се на крају окончало самоубиством несрећне дјевојчице.

...

Момак је са малољетном дјевојком снимао сексуални однос, уз њен пристанак (и на сексуални однос, и на снимање односа), а након раскида, с обзиром на то да се наведени снимак налазио (и) код њега, он га је поставио на властити профил на Фејсбуку, с тим што је дјевојку означио на снимку. Наравно, веома брзо је снимак преузет са интернета (мада је могуће да је снимак дијелио и уз помоћ телефона).

...

Момак је, након раскида са својом дјевојком неколико њених фотографија на којима је она гола и на којима се виде груди и гениталије, поставио на Фејсбук. У судском поступку је изјавио да је то учинио зато што га је она повриједила и зато што је хтио да уради било шта да и он њу повриједи, односно да јој врати истом мјером.

...

Четрнаестогодишња дјевојка је добила захтјев за пријатељство од момка који се представљао као шеснаестогодишњак. Након што је прихватила захтјев, кренули су се дописивали. Првих пола године њихова комуникација је била „нормална“, уобичајена за њихов узраст – он се интересовало за то у коју школу иде дјевојка, како јој је у школи, рекао јој је да је и он прије ишао у исту школу, међутим, да се одселио из града, али да има другова, наводећи поименично и наставнике који су му били професори. Таква комуникација између њих се одвијала око пола године, готово свакодневно, неријетко и по сат времена. У међувремену је она њему прослиједила и неколико властитих „селфи“ фотографија. Након пола године, знајући да она тренира одбојку, тражио је да му она прослиједи фотографије у одбојкашком дресу, што је она и урадила, међутим, он је захтијевао да се она фотографише „као манекенке

спортисткиње“ – да заврне ногавице дреса, рукаве мајице, те да подигне мајицу. Иако она у почетку није хтјела тако да се слика, он је инсистирао, подилазећи јој и говорећи како је лијепа, како се тако сви сликају и како треба да је модерна, а не конзервативна. На крају је она пристала и послала му је неколико таквих фотографија. Таква комуникација, са повременим слањем таквих фотографија, се наставила током цијеле године, да би на крају године они били „у вези“, иако се никако нису срели. Годину дана од почетка комуникације, она се таговала на базену, да би он од ње тражио да му пошаље слике гдје је она у купаћем костиму. Она на то није пристала наводећи да ју је срамота, међутим, на његово инсистирање, те тврђе да ће је, када и он дође на базен, ионако видјети у купаћем, послала му је и такве фотографије, а потом му их све чешиће и чешиће слала, мислећи да их шаље „свом момку“. Након извјесног периода, он је од ње тражио да се слика гола, „јер ће је ионако видјети голу“, међутим, она на то није пристала, да би он потом „раскинуо“ са њом. Њој је било криво што је он раскинуо са њом, упорно му је слала поруке да се помире, међутим, он је одговарао да не жели да хода са конзервативном, стидљивом, традиционалном дјевојком, већ да ће себи наћи модерну, слободну и неспутану дјевојку. Усљед тога, дјевојка је пристала да му пошаље неколико својих полуголих фотографија, међутим, он је инсистирао да се она скине гола, на шта она није пристала. С обзиром на то да је увидио да она неће пристати да се слика гола, он ју је почео уцењивати да ће све фотографије, као и комплетну преписку између њих, објавити на свом и на њеном профилу. Иако се препала, те ју је било стид и срамота, то је испричала мајци која је случај пријавила полицији. Полиција га је релативно брзо идентификовала и локализовала и утврдила да се ради о четрдесетдогодишњаку.

...

Претходно наведене негативности на интернету, поготово на друштвеним мрежама, и то махом на Инстаграму и на Фејсбуку, представљају „секстинг“, „грумнинг“ и „сексторжн“. Најкраће речено, „секстинг“ представља слање сексуално експлицитних фотографија или порука сексуалног садржаја другој (најчешће непознатој) особи електронским путем, док „грумнинг“ представља врбовање, мамљење, „тимарење“, подилажење особи како би се она привољела да пошаље властите сексуално експлицитне фотографије. „Сексторжн“ представља конкретизацију и сексуалну експлоатацију тако добијених садржаја пријетњом компромитације откривањем фотографија и порука, уколико жртва не поступи по захтјевима.

Посебан аспект електронског вршњачког насиља везан је за постављање сексуално инкриминишућих и понижавајућих фотографија, видео-снимака или другог садржаја на профилу. С обзиром на масовност ученичке популације на друштвеним мрежама, постављање сексуално инкриминишућих фотографија (и другог сексуално инкриминишућег садржаја) на овим интернет ресурсима (примарно на Фејсбуку, Инстаграму и на Виберу), свакако је један од најподлијих, али и чешћих

начина чињења (нематеријалне) штете другом, најчешће (бившим) дјевојкама.

Еротски или порнографски садржај којим се жели дискредитовати жртва могуће је поставити и на прави профил особе која га поставља, без обзира на то да ли су на постављеним фотографијама, снимцима или на другом материјалу налази само особа која се дискредитује или и друге особе (па и особа која поставља порнографски материјал), а то ће се поготово радити када бивши (анонимни) момци желе да нанесу штету (бившим) дјевојкама, из одређених разлога, а посједују компромитујући материјал.

Надаље, услед могућности које пружају тзв. „алатни профили“, као и алати фотошопа, инкриминација одређене особе порнографском конотацијом на одређеним фотографијама и на снимцима могућа је и „таговањем“ жртве на компромитујућим фотографијама и снимцима. Ово се најчешће ради код жртава које имају властити профил на друштвеним мрежама, али на њему нису активне (и по неколико дана или чак седмица).

У вези са наведеним је и тзв. он-лајн сексуално напаствовање које се састоји од константног и континуираног слања порука, фотографија и снимака, те од постављања коментара и сличних активности које имају одређену сексуалну позадину или контекст. Овом активношћу, која је садржај „грумिंगа“, дјеца се суптилном комуникацијом и интеракцијом на интернету подстичу да учествују у интеракцијама сексуалне природе при чему се често излажу нежељеним порнографским садржајима. Најчешће представља фазу у којој се дијете припрема или на стварни сексуални чин с одраслом особом или на учешће у производњи дјечије порнографије, при чему злостављач злоупотребљава повјерење дјетета које у већини случајева не зна ни у које ће сврхе његове фотографије или снимци бити употребљени, нити какве ће то посљедице имати по његов даљњи живот. Садржај поруке најчешће према жртви имплицира потенцијални сексуални однос са напасником, претходну сексуалну активност жртве, сексуалну оријентацију жртве, промискуитетност жртве... Поред порука, овај вид узнемиравања преко Фејсбука врши се и постављањем, као што је већ назначено, фотографија сексуално омаловажавајућег или деградирајућег садржаја за жртву, а појављују се и прве апликације, па чак и игре (додуше, незавидног програмерског нивоа) са алузијом на сексуалну активност, сексуални однос или сексуалну оријентацију жртве. Иако се сматра да је сексуално напаствовање чин личне природе, односно да напасник и жртва имају

одређену (претходну) интеракцију (да се познају), то не мора да буде тако, с обзиром на то да напасник најчешће сексуално узнемирава већи број жртава, од којих многе (или све) и не зна. Погрешно се сматра да сексуално напаствовање није озбиљан проблем, односно да га је лако ријешити.

Уцјењивање и изнуђивање

Седамнаестогодишњи ученик је добио захтјев за пријатељство од дјевојке из сусједне школе, односно профил је био на њено име и са њеном профилном фотографијом, те личним подацима. У комуникацији, која је била сексуалне природе, она је од њега тражила да се фотографише го, те да јој шаље такве фотографије, а потом је од њега захтијевала и снимке са алузијом на сексуални однос између њих двоје. Он је на то пристајао, сматрајући да ће се тако показати као „мачо момак“, те ће имати сексуални однос са њом. Након одређеног периода, она га је почела уцјењивати да ће фотографије и снимке објавити на Фејсбуку, уколико јој он не исплати одређени износ новца.

...

Увиђајући многобројне могућности друштвених мрежа, а познајући понашање интернаута, уцјењивачи користе погодности мрежа, те преко њих постављају или објављују одређени компромитујући садржај или пријете његовим постављањем, у циљу изнуђивања одређене користи, најчешће материјалне или порнографске, од жртве. Уцјена се на овај начин најчешће предузима према млађим интернаутима, мада се као жртве могу појавити и старији, односно може се радити и о озбиљнијим облицима уцјене (наравно, не потцјењујући ни озбиљност уцјене када су жртве дјеца).

Када је у питању уцјена преко друштвених мрежа или коришћењем могућности мрежа, могу се диференцирати двије ситуације. Прва ситуација подразумијева да се уцјењивачки однос испољава кроз комуникационе ресурсе друштвених мрежа, док друга ситуација подразумијева да се одређени уцјењивачки материјал прикупља на друштвеним мрежама или уз помоћ друштвених мрежа.

Мреже се, за ове потребе, користе у циљу проналаска жртве, затим за емпатичко саживљавање са жртвом, а потом се преко друштвених мрежа жртва уцјењује или жртви блиске особе у циљу прибављања одређених материјалних или нематеријалних добара. Иако се мреже користе за врбовање жртава разних кривичних дјела и криминалних активности (педофилија, превара), проналажење потенцијалних жртава уцјене је свакако специфично, с обзиром на

природу испољавања ових кривичних дјела. Такође, и емпатичко саживљавање са жртвом, њеном улогом коју има у одређеној заједници, свакако да захтијева висок ниво комуникационих и психолошких способности самог уцјењивача.

Међутим, много чешће се повезаност уцјене са друштвеним мрежама посматра кроз одређени компромитујући садржај који се налази на мрежама, без обзира на то да ли га је поставила сама жртва или неки други корисник или и сам уцјењивач. Када је у питању садржај који је поставио ученик или његови пријатељи или други незлонамјерни интернаути, најчешће се ради о фотографијама, видео-снимцима и сличном материјалу који ученика приказује у одређеним недоличним ситуацијама, позама, присуству других лица... Наравно, усљед многобројних могућности које пружају тзв. алатни профили, као и могућности фотомонтаже, није искључено да се као компромитујући материјал на профилу жртве пронађе и овако креиран материјал. Као компромитујући материјал се може јавити и материјал који су поставили други ученици, не знајући или не схватајући да је компромитујући за конкретног ученика, те да ће га други злонамјерни интернаути искористити у циљу уцјењивања жртве. Као посебан облик уцјењивачког материјала (пored фотографија и видео-снимака), поготово када су у питању дјеца, појављују се и текстуалне поруке, односно преписи комуникације између корисника, затим комуникација унутар одређене затворене групе у којој је и жртва комуницирала.. Могуће је и да сам уцјењивач „навуче“ жртву на одређену недоличну, односно компромитујућу комуникацију (или сличну активност), те да га потом уцјењује. Конкретан примјер за наведено је врбовање жртава од стране педофила кроз претходно помињани „грумлинг“ и „секстинг“.

Посебан вид уцјењивања преко Фејсбука има „сквотинг“, као и уцјењивање у циљу поврата контроле над компромитованим (украденим) профилем, што је већ наведено.

На сличан начин, могу да се реализују и одређене изнуђивачке активности.

Самоубиства

Једна Британка је извршила самоубиство након што су се њене фотографије у топлесу појавиле на Фејсбуку, док је један Американац извршио самоубиство након што је на Фејсбук постављен снимак сексуалног односа између њега и другог мушкарца.

...

У литератури се, као узроци самоубиства, најчешће наводе усамљеност, љубавни проблеми, неизљечива болест, алкохолизам, осјећање бесперспективности, смрт блиских чланова породице, аномија, егзистенцијално безнађе, претходна самоубиства у породици... Стога је и јасно да се узрок самоубиства не може тражити унутар и на интернету. Међутим, то не значи да интернет и друштвене мреже немају никакве везе са суицидним намјерама појединих интернаута, јер је чињеница да су одређена самоубиства повезана са друштвеним мрежама, првенствено са Фејсбуком. Та веза може да се огледа кроз одређени садржај који је постављен на мрежу, те који је иницирао самоубиство, затим је могуће да се самоубиства најављују преко мреже, као и да се млађи интернауту договарају око заједничког самоубиства. Сви наведени облици су се, на жалост, и конкретизовали преко Фејсбука.

Када је у питању садржај на Фејсбуку који може да буде повод самоубиству, то су сви они постављени садржаји који на одређен начин компромитују или понижавају одређену особу која је такође (најчешће) корисник мреже, те је упозната са могућношћу брзог ширења и доступности великом броју корисника конкретног, за њу понижавајућег, садржаја. Постављени садржај је најчешће сексуалне природе, без обзира на то да ли се односи на сексуални однос, сексуалну оријентацију или на компромитујуће фотографије. Наравно, компромитујући, инкриминишући или понижавајући садржај не мора да буде само сексуалне природе, већ је могуће и да се односи на неку тајну из прошлости, на одређене склоности или недостатке особе и слично. Посебан облик садржаја који може да иницира самоубиство ученика односи се на вршњачко насиље према њему, јер реакција на константно и континуирано испољавање вршњачког насиља одређеног броја млађих интернаута може да буде самоубиство.

Мреже се користе и за најављивање самоубиства, односно за слање суицидних порука. Самоубиство најчешће најављују постављањем суицидне поруке на профил или слањем порука властитим пријатељима. За најављена планирана самоубиства преко Фејсбука се може рећи да су на Западу била „у црном тренду“. Наиме, констатован је тренд пораста

млађих интернаута који су најавили самоубиство на Фејсбуку, а затим га покушали (па и реализовали).

Не треба изоставити ни то да се преко друштвених мрежа могу иницирати или подстрекавати самоубиства других, и то из различитих мотива (медицинских, религијских, личних...). Није чак ни неопходно да подстрекач или иницијатор познаје потенцијалног самоубицу, већ је довољно да му буде пријатељ на друштвеним мрежама.

Нетикеција – правила понашања на друштвеним мрежама

На свим друштвеним мрежама су се диференцирала одређена правила којих се интернаути морају придржавати, а и свака друштвена мрежа додатно прописује и властита правила коришћења мреже.

Та правила се превасходно односе на правила комуникације, али и на низ других правила у вези са присуством корисника у једном специфичном окружењу какво је интернет окружење, а поготово окружење конкретне друштвене мреже. Без обзира на специфичност тог окружења, чињеница је да су правила пристојности, културног опхођења, начина и садржаја комуникације, те низ других правила која постоје у стварном окружењу свакако присутни, односно требало би да буду присутни и у оквиру интернет окружења, без обзира на специфичности тог окружења. Штавише, интернет окружење правила комуникације, интеракције и социјализације свакако не би требало да елиминише, већ управо да их надограђује што је условљено самом специфичношћу овог окружења, а што се свакако не треба негативно посматрати. Значи, сва неформална правила која су присутна у стварном окружењу, присутна су и у оквиру интернет окружења, с тим што су у овом окружењу релевантна и бројна друга правила која се надограђују на ова претходна.

Та правила подразумевају културан, учтив, јасан, недвосмислен, лукративан начин опхођења и комуникације са другим интернаутима. Надаље, сем комуникације, ова правила подразумевају да се корисници уздржавају од разних активности или пласирања садржаја којим би повриједили туђу приватност или туђу личност. Наравно, то се може извршити на многобројне начине, али је примарно да сам корисник то схвати, те да се уздржи од негативности, а и уколико несвјесно учини изгред – да предуприједи посљедице, односно, уколико су посљедице настале да их покуша санирати.

Ово су уопштена правила комуникације и понашања на друштвеним мрежама, која су већином или производ нетикеције или проистичу из правила приватности прописаних од стране друштвених мрежа.

Поред овако уопштених правила понашања, интеракције и комуникације, чињеница је да постоји и низ других правила која су

Правила бонтона,
културно опхођење и
комуникација,
пристојност и
слично, важе и у
интернет окружењу.

својствена само одређеним групацијама корисника, и то групацијама корисника који су посебно виктимизирани на друштвеним мрежама. Придржавајући се тих правила, умногоме се смањује, али се не елиминише њихова виктимизираност, што треба имати на уму приликом коришћења сваке друштвене мреже. Та правила се односе на дјецу и почетнике као најугроженије интернауте, што не значи да на друштвеним мрежама (поготово на Фејсбуку и Инстаграму) нема и цијели низ других популационих група које се посебно виктимизирале у односу на виктимизираност цијеле интернаутске популације.

Дјеца су посебно
угрожена на
интернету, чега
родитељи морају
бити свјесни и
посветити томе
пажњу.

„Оно што није дозвољено у стварном окружењу, није дозвољено ни на интернету, дакле ни у окружењу друштвених мрежа“ би могао бити генерални савјет у циљу превенције разних насилних активности у интернет окружењу, без обзира на то како оне биле посматране. То се примарно односи на комуникацију, али и на све друге активности и садржаје које могу да представљају агресиван чин према другим интернаутима или чак и према лицима која не користе интернет. Конкретно, указујући на пожељан и подразумијевани образац понашања корисника на друштвеним мрежама у циљу елиминисања насилних активности, интернаути би у комуникацији са другим интернаутима требало да се понашају културно, уљудно, са разумијевањем, избјегавајући конфликте и не учествујући у њима, па чак ни посредно. Уколико до таквих сукоба дође, требало би да се дистанцирају од њих, као и од актера тих сукоба, а у екстремнијим случајевима да о томе обавијесте и администратора, а у одређеним случајевима и полицију.

Оно што није
дозвољено у стварном
окружењу, није
дозвољено ни у
интернет окружењу,
односно у окружењу
друштвених мрежа.

Пожељно је да интернаути који имају профил на одређеној друштвеној мрежи континуирано одржавају властити профил, што налажу и сама правила приватности, односно, како би се умањила (секундарна) виктимизација, битно је да интернаути редовно ажурирају властите профиле. Овим се не пропагира непрестано или учестало, дуготрајно или слично виртуелно присуство, већ повремено увид у

садржај на профилима, као и у активности других интернаута како би се благовремено предуприједиле одређене непожељне активности које су на корисников профил постављене од стране других корисника или им је корисник и несвјесно приступио. Уколико интернаут таквог профила релативно често посјећује профил (па само и по неколико минута), разумљиво је да ће благовремено моћи реаговати на негативности, што ће спријечити или умногоме умањити његову виктимизацију.

Уколико се на профил жртве вршњачког насиља постави одређени компромитујући материјал (порнографски или сличан садржај, на којем се налази сама жртва), те уколико сама жртва профилу не приступа често, односно сваке седмице или још рјеђе, разумљиво је да ће приступ том садржају (па и преко њеног профила) имати мноштво других ученика, чиме је настала штета свакако много израженија. С друге стране, уколико би жртва сваки дан приступала профилу, па чак и по неколико минута свакодневно, разумљиво је да би одмах након постављања таквог материјала или релативно брзо након постављања могла да га избрише, да пријави или да на други начин онемогући продуковање насилничких замисли самог злонамјерног корисника.

...

Слично се може извести и у вези са крађом профила. Уколико се на било који начин компромитује профил ученика, те се са тако компромитованог профила продукује нежељени садржај или нежељене активности пријатељима тог профила, разумљиво је да ће много мања штета и непријатност настати уколико ученик тог дана схвати да му је профил компромитован, односно да му не може приступити (након чега би преко профила пријатеља требало да пријави проблем администратору), него да то схвати неколико дана или седмица након што му пријатељи јаве да се преко његовог профила продукује нежељени, непримјеран садржај или активности.

...

Један од најважнијих превентивних механизма у циљу заштите приватности јесте лозинка неопходна за приступ профилу. Приликом креирања лозинке, треба се придржавати сљедећих правила:

1. Лозинка мора имати најмање 12 карактера,
2. Мора бити комбинација слова, бројева и интерпункцијских знакова,
3. Мора бити комбинација великих и малих слова,
4. Тако креирана лозинка не треба да представља никакав логичан низ, већ да буде насумично одабран алфанумерички низ великих и малих слова са бројевима у самом низу.

Одабир лозинке је посебно битан приликом креирања профила. Родитељи треба да знају лозинку за приступ профилу дјетета.

Наведени низ не би требало да има било какву логику приликом креирања, нити треба да се на било који начин „веже“ за личност корисника.

У том смислу, најбоље (наравно, не и идеалне) лозинке би биле попут `4F$y0#(@oGp1, gV8z2%I5!a0W, 0%Qm7T@c1Cv3...`

У вези са лозинкама, неопходно је поменути да једном креирана лозинка не подразумејева да се она константно одржава, већ се мора повремено мијењати. Без обзира на то што то може да изискује и одређени напор корисницима, сама лозинка, без обзира на то колико била „јака“, мора да се повремено замијени новом лозинком.

Исто тако, корисник не би требало да користи исту лозинку за два или више налога која има на интернету, без обзира на то о којим налозима се ради (налог на другој друштвеној мрежи, налог електронске поште, налог за електронске финансијске трансакције, налог за електронску куповину...). Штавише, препоручује се да ни само корисничко име не буде исто, наравно, уколико то саме апликацијске могућности дозвољавају.

За ученике је веома битно да приликом креирања налога електронске поште која ће служити за креирање профила или бити корисничко име, адреса не садржи име и презиме корисника, нити годину рођења, па чак ни локацију пребивалишта или боравишта (попут, на примјер: `markomarkovic@yahoo.com`, `draganamalic2003@gmail.com`, `jecabl06@hotmail.com`). Ученици који у адресама електронске поште користе властито име и презиме, годину рођења или локацију пребивалишта, као и друге личне податке, додатно се виктимизирају у случају компромитације саме адресе, која и не мора бити крађа ове адресе, већ сам приступ адреси. Остваривањем приступа, разним софтверским алатима, али и „ручно“, злонамјерни корисници могу идентификовати одређене карактеристике потенцијалне жртве, те је на тај начин угрозити.

Назив мејла не смије да сугерише пол дјетета, годиште или локацију становања.

Анализом адресе у којој се налази година рођења (односно број за који се основано може претпоставити да је година рођења), педофил може властите педофилске активности усмјеравати ка тој особи, односно кориснику те поште.

Поред наведеног, пожељно је да корисник има више пријављених електронских налога за приступ профилу, односно да их одреди као

потенцијалне за поврат евентуално заборављене лозинке, имајући у виду да, уколико му се компромитује један налог електронске поште, те се преко њега покуша и компромитација профила, увијек остаје друга или друге адресе преко којих ће то успијети спријечити, па чак и повратити профил.

Не смије се са јавних рачунара (рачунара у школи, у угоститељским објектима, на јавним мјестима) приступати властитом профилу.

Приступањем профилима са јавних рачунара (школских рачунара, рачунара у интернет локалима, рачунарима којима има несметан приступ већи број лица), ученици се излажу многобројним опасностима, услед чега присуп профилу са јавних рачунара треба избјегавати или користити тзв. двостепену ауторизацију (опција која шаље код на телефон приликом сваког покушаја уласка на профил) или користити виртуелну тастатуру.

Приликом приступа основним страницама друштвених мрежа за упис аутентификационих и идентификационих података, не треба се користити претраживачима (не „гуглати“ странице), с обзиром на то да, разним софтверским манипулацијама, постоји могућност индексирања „фишинг“ и сличних страница на прво мјесто по посјећености које корисник најчешће аутоматски и прихвата не посматрајући саму УРЛ адресу. Да се то не би десило, основну страницу друштвене мреже треба поставити као основну, подразумијевајућу страницу (поготово код корисника који често користе друштвене мреже) или јој приступати директно преко адресе. Приликом приступа Фејсбуку, корисник мора да обрати пажњу на то да ли је адреса странице www.facebook.com или одређени поддомен ове странице, те само преко ових страница приступати.

На саму адресу је неопходно обратити пажњу и приликом приступања профилу, али исто тако и приликом приступања одређеној апликацији током коришћења друштвене мреже, приликом чега се корисник пребацује на другу виртуелну локацију, када му се поново траже идентификациони и аутентификациони подаци, иако се још увијек користи ресурсима саме мреже. У овом случају, као и у низу сличних случајева, ради се о тзв. „фишинг“ страницама којима је циљ да дођу до корисничких идентификационих и аутентификационих података неопходних за приступ његовом профилу.

Родитељи ученицима посебно морају да савјетују да не прихватају велики број пријатеља, а поготово да не прихватају пријатеље које лично не познају. У овом случају важи опште правило којим родитељи дјецу

савјетују: „Не причај са незнанцем!“ Управо то правило треба афирмисати и када је у питању интернет окружење.

Ученици се неријетко учлањују у многобројне групе на друштвеним мрежама. Међутим, прије самог приступа групи, треба се прво упознати са самим садржајем групе, активностима и комуникацијом која се у њој води, евентуалним или потенцијалним непријатностима који су имали други чланови групе или које може сам корисник да има, са корисницима који су у групи... Све наведено може да утиче на ученика да неприступањем групи евентуално избјегне бројне непријатности активним или пасивним учешћем у раду групе. Исто тако, уколико је ученик члан одређене групе за коју сматра да њени чланови не воде лукративну комуникацију или активности, пожељно би било да се искључи из групе, како би предуприједио бројне непријатности.

Постављањем одређених фотографија (или снимака) на друштвене мреже, па чак и на сам интернет, корисник који је поставио фотографије више нема контролу располагања њима, јер постоји могућност да их неко одмах преузме, копира или их на други начин учини доступним себи и за своје потребе, без обзира на то да ли ће их (одмах) компромитовати или не. Усљед наведеног, интернауту морају добро да размисле да ли ће, колико и које фотографије постављати на друштвене мреже, с обзиром на то да се једном постављене фотографије на профил корисника, те неограничавањем или либералним ограничавањем видљивости, те фотографије могу компромитовати на разне начине, а касније ограничавање видљивости, па чак и брисање тих фотографија тешко да ће имати икакав ефекат на испољену, а поготово на потенцијалну накнадну компромитацију.

И одабир фотографија мора да буде опрезан, поготово имајући у виду могућности фотомонтаже разним софтверским алатима. Међутим, интернауту на мреже постављају и властите фотографије који их директно

**Не причај са странцем!
То важи и на интернету!
Дјецу то треба научити!**

**Једном постављена
фотографија на
друштвене мреже, више
се не може скинути са
мреже.**

**Што мање фотографија
дјетета на интернету и
на друштвеним мрежама
– то боље за безбједност!**

компромитију или накнадно могу да компромитију, несвјесни или дјелимично свјесни наведеног. Ризикујући приватност (чак се и не би могло рећи да се у овом случају ризикује приватност, већ се може рећи да је само нарушавање приватности извјесно, само је питање времена и интензитета) зарад популарности, најчешће дигиталне, мада неријетко и реалне, и то углавном тренутне, а поготово краткотрајне, интернауте свакако непромишљено поступају не водећи рачуна о количини и садржају фотографија које постављају на интернет. Наравно, наведено (готово) увијек има драстичне последице.

Један од начина заразе рачунара вирусом је отварање додатака у оквиру електронске поште коју корисник добије, а која, у суштини, представља сам вирус, односно вирусни потпрограм. С обзиром на то да овај вирус у себи може да инкорпорира и одређене „килогерске“ функције, није тешко претпоставити да инфекција жртвиног рачунара на овај начин представља и потенцијалну компромитацију профила, односно несвјесно откривање идентификационих и аутентификационих података интернаута који са зараженог рачунара приступа властитом профилу.

Почетници на друштвеним мрежама, односно корисници који су тек креирали профил и на тај начин започели виртуелну егзистенцију посебно су виктимизирани корисници у овом окружењу, поготово уколико их не краси ни одређено интернет знање, односно искуство рада у интернет окружењу. Ово би поготово родитељи ученика почетника на интернету требало да знају.

За пријатеље на друштвеним мрежама, дјеца треба да прихватају искључиво позната лица!

Главни савјет почетницима интернаутима јесте да приликом креирања профила за пријатеље прихвате само кориснике које лично познају, односно у чији идентитет не сумњају, те да извјесни период са тих неколико или пар десетина пријатеља остварују интеракцију. Тек након извјесног периода, упознавањем могућности, као и добрих и лоших страна окружења друштвених мрежа, могу да „експериментишу“, односно да за пријатеље прихватају и друге познанике, као и да учествују у другим могућностима друштвених мрежа. Наравно, у свим наведеним активностима треба бити опрезан.

Веома је важно да интернауте у овом периоду за пријатеље никако не додају лица

Што мањи број пријатеља на друштвеној мрежи, дијете је сигурније!

у чији идентитет нису сигурни, без обзира на упорност тих корисника, као и евентуална убјеђивања (преко порука, наговарањем од стране познаника или других пријатеља и слично).

У почетном периоду је изузетно битно да ови интернаути ограниче властиту приватност кроз рестриктивно подешавање приватности према другим интернаутима, укључујући и властите пријатеље.

Почетници, као уосталом и сви други корисници не би требало да учествују у одређеним активностима које њима лично нису пријатне, без обзира на наговарање пријатеља, па чак и на (потенцијалну) већинску прихваћеност и инкорпорираност пријатеља у те активности. Слично је и са садржајем који почетници и други корисници не би требало да дијеле уколико га не прихватају, те не прихватају начин дијелења садржаја. Другим ријечима, све оно што корисник не одобрава или му се не свиђа у реалном животу, не би требало да потенцира на Фејсбуку.

Родитељи би дјеци требало да скрену пажњу и да приликом њихове виртуелне егзистенције обратe пажњу на то да ли се придржавају следећих правила и смјерница:

1. У потпуности се **придржавајте правила приватности** друштвених мрежа које се користе, односно родитељи и дјеца би требало да их прочитају приликом креирања профила, те да их се придржавају;
2. Све личне информације (број телефона, адресу, путању кретања) приликом креирања профила **заштитите од свих**, а поготово фотографије, сем од пријатеља, мада и фотографије можете, уколико сматрате пожељним, заштитити од појединих или свих пријатеља. Такође, родитељи би дијете требало да подуче да податке који омогућавају њихову **локализацију не би требало** да постављају на друштвене мреже (гео-таговање, фотографије испред куће, до школе...),
3. **Личне податке никад** не треба постављати у јавној преписци, али ни приликом четовања;

4. Корисничко име и лозинка се никоме не смију саопштавати;
5. Потребно је повремено мијењати корисничко име и лозинку;
6. Корисничко име и лозинка би требало да се разликују у односу на корисничко име и лозинку за приступ адреси електронске поште;
7. Уколико дијете изгуби или му се украде мобилни телефон са којег је приступао властитим налозима на друштвеним мрежама, потребно је хитно промијенити корисничко име и лозинку за приступ профилу, користећи се двостепеном ауторизацијом са новим бројем телефона;
8. Налозима на друштвеним мрежама никад не треба приступати користећи се непровјереном бежичном везом ;
9. У комуникацији са пријатељима на друштвеним мрежама, дјецу треба подучити да комуницирају као и у стварном животу, односно да су правила комуникације у смислу културе, опхођења, начина говора, стила писања иста;
10. У интернет комуникацији се никад други не смију вријеђати, називати погрдним именима, псовати и слично;
11. На властити профил би требало постављати само властите фотографије , а тек по одобрењу других и фотографије на којима се налазе и друга лица;
12. Фотографије на којима се налази више лица треба „таговати“ само уз њихову дозволу ;
13. За пријатеље треба прихватати искључиво позната лица , а и пријатељство тражити само од познатих лица;

14. Уколико се комуникација са одређеним пријатељем учини непријатна по било ком основу, дијете треба посавјетовати да је неопходно да таквог интернаута одмах **избрише са листе пријатеља**, а уколико након тога буде досађивао, да **обавијести администраторе**;

15. Дјеца не смију да креирати групе са погрдним или омаловажавајућим називима;

16. Дјеца морају знати да не смију друге да „тагују“ на омаловажавајућим или понижавајућим фотографијама;

17. Веома је битно да се дјеца едукују да **никад не уговарају састанке** уживо са пријатељима које су упознали преко интернета, а такође да на састанке не иду сами, те да **претходно обавезно обавијесте** родитеље или пријатеље са ким и гдје иду на састанак;

18. С обзиром на то да је веома **мала могућност, готово никаква, накнадних повлачења постављених фотографија** (и другог садржаја) са интернета, прије њиховог постављања треба добро размислити које фотографије поставити;

19. Дјеци се константно и континуирано мора скретати пажња да никад не учествују у дискусијама које имају **сексуални, порнографски или еротски контекст**;

О свим злоупотребама на друштвеним мрежама, треба обавијестити администраторе.

Посебна правила понашања за дјецу на друштвеним мрежама

Дјеца су посебно виктимизирана на друштвеним мрежама, због чега би требало да се посебно придржавају бројних савјета и сугестија како би адекватно заштитили властиту приватност и безбједност. Тих савјета је, наравно, изузетно много, али су се неки диференцирали као важнији, те ће овдје бити наведени.

Дјеца се либералније понашају преко интернета и то злонамјерни интернаути користе!

Дјеца су, по природи, слободнијег и неспутанијег, па и још увијек неформираниог конформистичког понашања у реалном окружењу што наравно, има импликације и на интернет окружење. Штавише, примјетно је да су и дјеца која су интровертнија у реалном окружењу, у интернет окружењу много опуштенија, неспутанија, отворенија, па и (вербално) насилнија. Иако су природност, неспутаност, отвореност, искреност, па и директност (што све карактерише дјецу), афирмативне у комуникацији, па и у оквиру свакодневних активности, чињеница је да те особине често у реалном животу, али и у оквиру интернет окружења могу негативно да дјелују и на дјецу, али и на друге субјекте који своје негативне активности испољавају према дјечи. Услјед тога, дјеца морају да обрате пажњу на начин и садржај комуникације, али и, што је много битније, на субјекте са којима комуницирају. Другим ријечима, дјеца не би требала уопште да иницирају или пристајају на комуникацију, нити на било какав вид интеракције са другим интернаутима који су им непознати, с обзиром на правило из стварног окружења да дјеца не треба да „причају са непознатима“. Ова забрана не би требало да се односи само на непосредну или посредну комуникацију, већ и на друге видове потенцијалне интеракције између дјеце и других корисника, у виду учешћа у раду одређених група, позивања у групе, прихватања апликација, прихватања захтјева за пријатељство од непознатих корисника, одговарања на поруке, узвраћања лајкова... Све видове игнорисања и дистанцирања од стране (навалентних) непознатих

Дјеца не смију комуницирати преко друштвених мрежа са непознатим лицима!

корисника, дјеца не би требало да посматрају као вид некултуре и неучтивости у интернет комуникацији, већ као вид бриге за властиту безбједност која им је (највјероватније) угрожена од стране сексуалних грабежљиваца и других злонамјерних интернаута.

Постављање фотографија на друштвене мреже треба свести на најмању могућу мјеру!

Иако властите фотографије на интернет и на друштвене мреже постављају сви корисници, чињеница је да у томе предњаче дјеца, настојећи на тај начин афирмисати властиту личност кроз својеврсно визуелно изражавање преко постављених фотографија. Иако је то само по себи спорно, чињеница је да оно имплицира много драстичније опасности од властите несигурности ових корисника. У првом реду, дијете се готово тренутно виктимизира услед многобројних могућности компромитације тих његових фотографија, што (може да) представља удар на његову приватност, односно на његову личност у реалном, али и у интернет окружењу. Међутим, чињеница је да дјеца нису свјесна потенцијалне компромитације преко тих фотографија у блиској будућности, услед чега свакако постављају фотографије са сексуално експлицитним или другим директно и компромитујућим и виктимизирајућим садржајем.

Дијете треба знати да непријатну комуникацију не треба да води преко интернета.

Доста малолетних интернаута, услед несигурности или кризе идентитета, што је повезано са периодом пубертета, преко друштвених мрежа иницира сексуалну комуникацију са другим корисницима (најчешће супротног пола) која може да има карактеристике или да временом прерасте у навалентно понашање ових корисника. Иако овакво понашање најчешће није резултат одређене зле намјере, већ „пубертетско ослобађање“ које импликације има и на друштвеним мрежама, друга страна у овој комуникацији најчешће неће ове активности тако схватити, те ће их посматрати као навалентне, иритирајуће, а у крајњем случају и угрожавајуће, услед чега може да посегне и за одређеном заштитом, било игнорисањем таквог корисника, било његовим пријављивањем или на други начин. Резултат тога може да буде одређена конфликтна ситуација између корисника који су учествовали у интеракцији, иако ни једно ни друго нису имали зле намјере, међутим, сама комуникација се

компромитовала услед различитих полазних основа код наведених корисника које карактерише неразумијевање. Како би се то предуприједило, корисник којем је непријатно да настави до тада устаљени или повећани ток и садржај комуникације, требало би да другом учеснику у комуникацији јасно стави до знања да му се сама комуникација не свиђа. Уколико се саговорник не сложи са наведеним, треба напустити комуникацију и не настављати је упркос потенцијалним захтјевима за наставак комуникације.

Малољетни интернауту не би требало да импулсивно реагује на одређене провокације од стране других корисника, без обзира на то да ли биле уперене према њима конкретно или према уопштеној групној популацији којој и сам корисник припада. Чак и код оног садржаја или активности која је усмјерена према самом кориснику, а њега директно излаже порузи или сличном облику насиља, корисник не би требало да реагује „на прву“, нити да равномјерно „одговори“ таквим насиљем, већ би га требало игнорисати (уколико се ради о „лакшим“ негативностима) или би (уколико се ради о „тежим“ негативностима) требало да упозори корисника који је пласирао тај садржај или активности на посљедице таквог понашања, захтијевајући од њега адекватно понашање. Уколико се непримјерено понашање насилника настави, односно уколико се не повинује захтјевима потенцијалне жртве, треба га пријавити администратору, а уколико се ради о тежим облицима нарушавања приватности у смислу вршњачког насиља, обавезно би о томе требало обавијестити и родитеље и наставно особље.

На интернет насиље и
провокације не
одговарати насиљем,
већ то пријавити.

Примарно је да на потенцијалне насилне или сличне негативне активности у интернет окружењу, малољетни корисник не одговори истом мјером, већ да покуша да их предуприједи или на други начин елиминише потенцијалну или већ насталу штету, имајући у виду да му идентично (осветничко) реаговање сигурно неће помоћи у посљедицама које су према њему изазване, док ће, с друге стране, и од њега самог, иако је жртва примарне активности, створити насилника у окружењу.

Код свих активности негативног садржаја које други корисници продукују према малољетним корисницима, а поготово према дјечи,

оштећени корисници би о томе требало да обавијесте родитеље и наставно особље, а у одређеним случајевима и администраторе.

Конкретни савјети родитељима

Разумљиво је да је на родитељима велика одговорност да заштите властито дијете, па и на интернету, односно на друштвеним мрежама. Међутим, родитељи најчешће нису ни свјесни опасности које дјецу вребају на интернету, а нису ријетки ни родитељи који услед властите информатичне неписмености (неинформисаности) сматрају да је дјетету „боље да је за рачунаром, него да је на улици, гдје не може да га контролише“, наивно сматрајући да, док је за рачунаром (односно, на интернету), ништа лоше не може да му се деси, имајући у виду да је „под надзором“ родитеља, односно у његовом „видном пољу“. Наравно, родитељи овдје пренебрегавају низ негативних активности које се испољавају преко интернета, а којима су посебно виктимизирана дјеца. Међутим, с друге стране, присутни су и родитељи који су (дјелимично) упознати са проблемом испољавања интернет криминалитета, услед чега дјеци апсолутно и беспоговорно бране присуство рачунару и интернету, чиме се прелази у потпуну супротност.

Услед наведеног, могло би се констатовати да постоје три групе родитеља (с обзиром на њихов однос према дјечи у погледу допуштености коришћења интернета):

- прва група се односи на родитеље који беспоговорно дјеци дозвољавају коришћење интернета, сматрајући да им се ништа лоше не може десити на интернету, односно да на интернету не вребају безбједносни ризици који су карактеристични за реално окружење у којем дијете егзистира, запостављајући повезаност виртуелног и реалног окружења, а сами су најчешће информатички необразовани, односно неписмени;
- друга група је супротност претходно наведеној, а обухвата родитеље за које се не би могло рећи да су информатички необразовани, бар не као претходна група родитеља, услед чега дјеци беспоговорно бране коришћење и интернета и рачунара,

Родитељи морају знати да је дијете угрожено и у кући, када користи рачунар или мобилни телефон.

Родитељи нису свјесни свих опасности на друштвеним мрежама, због чега се морају редовно информисати.

сматрајући да су на интернету изложени многобројним безбједносним ризицима или сматрају да је коришћење рачунара и интернета „улудо трошење времена“;

- трећа група родитеља је убједљиво у мањини, а подразумијева оне родитеље који су информатички и интернет освијешћени, те су упознати и са могућности и предностима интернета, али и са свим опасностима које вребају на интернету, поготово за дјецу. Они дјечи дозвољавају коришћење интернета, али их и надзиру, прате посјећеност садржаја интернета, али и вријеме проведено на интернету, едукујући их о опасностима и безбједносним ризицима коришћења интернета.

Овдје је неопходно поменути да, иако је карактеристика већине родитеља да их не краси велико информатичко знање, бар не веће од њихове дјеце, без обзира на то којег су дјеца узраста (чега и треба да буду

**Дјеца више од родитеља знају могућности интернета
и његово коришћење, али родитељи свакако много
више знају о животу!**

свјесни), треба поћи од много пута помињане тезе у погледу односа родитеља према дјечијем коришћењу интернета:

За другу групу родитеља се не може рећи да нису информатички образовани, односно бар информисани, као и да су информативно упознати и о опасностима интернета услед чега дјеци беспоговорно бране коришћење интернета, сматрајући да на интернету ништа битно неће ни наћи, ни научити. Ови родитељи пренебрегавају чињеницу да ће дјеца најчешће покушати прекршити или заобићи ову забрану, те ће приступати друштвеним мрежама, али без знања родитеља, чиме ће свакако бити и виктимизиранији у односу на групацију дјеце чији родитељи беспоговорно омогућавају коришћење интернета.

Као што је и видљиво, и ничим ограничена и беспоговорна забрана коришћења интернета дјечи од стране родитеља није афирмативна. Уколико се дјеци не ограничи беспоговорно коришћење друштвених мрежа, претпоставка је да ће доћи до њиховог слободнијег и дуготрајнијег коришћења, што (може да) има негативне консеквенце, али исто тако, уколико дође до забране коришћења интернета, очекивано је да ће дјеца ефикасно „премостити“ ту забрану у виду приступа друштвеним

мрежама на алтернативни начин (у школи, преко мобилног телефона, у кафе-бару...).

Као закључак се намеће оптимално рјешење по којем родитељи треба да дозволе дјеци коришћење друштвених мрежа, али уз њихов надзор и са извјесним ограничењима која треба претходно договорити са дјецом. Родитељи би претходно требало да укажу дјеци на правила понашања на интернету, алудирајући на то да иста правила понашања вриједи и на интернету као и у реалном окружењу, без обзира на виртуелни аспект интернета. То се превасходно односи на комуникацију, али исто тако и на бројне друге активности дјетета на друштвеним мрежама (забрана комуникације са непознатима, непроводирање, невријеђање...). Такође, пожељно би било да су и родитељи присутни на конкретној друштвеној мрежи, односно да имају креиран профил, како би имали увид у окружење те мреже.

Штавише, када су у питању најмлађи интернаути, разумљиво би било да родитељи посједују идентификационе и аутентификационе податке за приступ профилу, што наравно не значи да би требало без знања дјетета, односно самог корисника профила, да приступају том профилу, те да остварују одређену интеракцију са другим корисницима лажно се представљајући у дјечије име. Посједовање идентификационих и аутентификационих података би се требало посматрати само као извјестан превентивни механизам према дјетету које ће се тешко одлучити за одређене неподразумијеване активности на профилу уколико зна да му родитељи увијек могу приступити профилу.

Наравно, код старијих малољетника није очекивано да би родитељима (о)дали приступ идентификационим и аутентификационим подацима, али би требало да се родитељи претходно договоре са њима да им је коришћење друштвених мрежа дозвољено уз извјесна ограничења.

Дјеци не треба бранити коришћење интернета и друштвених мрежа, међутим, морају им се поставити одређена правила и ограничења.

Родитељи млађе дјеце морају имати приступ њиховом профилу!

Родитељи старије дјеце морају имати за пријатеље дјецу на друштвеним мрежама!

Та ограничења, између осталог, подразумевају да родитеље, уколико имају креиран профил на тој мрежи, прихвате за пријатеље. На томе би, иако је разумљиво да се не би одмах усагласили са наведеним, требало инсистирати како би се предуприједило негативно понашање дјеце, али и евентуално продуковање негативних активности од стране других злонамјерних корисника.

Један од фактора договора коришћења друштвених мрежа од стране дјеце јесте и да родитељи ограниче вријеме коришћења интернета, а поготово виртуелне егзистенције на мрежама. То

ограничење може (и треба) да се посматра кроз дневни (или седмични) временски фонд коришћења тих мрежа, као и кроз дневни (или седмични) период коришћења тих мрежа. Ограничавањем времена колико и када дјеца могу да проведу на друштвеним мрежама (као и на интернету) код њих се развија осјећај за вријеме, па неће запоставити друге обавезе (школске, али и ваннаставне).

Када је у питању конкретан период тог ограничења, разумљиво је да дјеци треба омогућити коришћење интернета у току дана (никако у вечерњим или ноћним часовима), док се за сам (дневни или седмични) фонд коришћења не би могао прецизирати оптималан период, имајући у виду многобројне факторе. Разумљиво је да би млађа дјеца требало мање да користе интернет, док би старијим малољетницима требало омогућити дуготрајније коришћење интернета, али наравно, имајући у виду и њихове бројне друге обавезе, прије свега школске, као и низ других фактора. У суштини, седмични фонд часова проведених на интернету код

дјетета не би требало да буде преко 20 часова, имајући у виду да се то односи и на дјецу испод 14 година, као и на интернауте који имају преко 14, а мање од 18 година. Наведени период подразумејева и вријеме проведено на интернету и у школи, и код куће, као и на другим мјестима. Такође, то подразумејева и вријеме које се проведе на интернету у циљу

Током ноћи дјеци треба онемогућити приступ друштвеним мрежама!

Дневни приступ интернету и друштвеним мрежама се мора ограничити у складу са узрастом дјетета, имајући у виду његове школске потребе.

испуњавања школских обавеза и едукативних активности, а не само „беспосличарење“ на друштвеним мрежама.

Резимирајући овај однос родитеља према дјечијем коришћењу интернета, треба се осврнути и на улогу родитеља у томе. Наиме, доста родитеља полази од става да би дјецу требало да контролишу док су на интернету, и то на разне начине, попут контроле преко властитих профила које су дјеца прихватила за пријатеље, преко профила других корисника (старије дјеце, рођака, пријатеља) са којима

родитељи имају комуникацију, лажних профила родитеља које су дјеца прихватила за пријатеље, преко „дадила софтвера“ постављених на рачунар са којег дјеца приступају интернету, увидом у остварени интернет саобраћај преко провајдера... Иако су јасни разлози наведених активности родитеља према дјечијем коришћењу интернета, не би се могли прихватити као афирмативни. Наиме, контролисањем дјеце на интернету, које наравно да је могуће на разне начине, код дјеце се јавља само отпор према таквој активности родитеља, услед чега је и разумљиво да ће покушати елиминисати ту контролу, а то ће им у највећем броју случајева и успјети, због бољег познавања савремених информационо-комуникационих технологија. Зато се сматра да дјецу на интернету не треба контролисати, већ надzirати, гдје појам надзора треба либералније посматрати, поготово у односу на појам контроле. У том смислу, дјетету треба да се укаже на пожељно или подразумевано понашање, односно на понашање које се од њега очекује, те да му се у том смислу укаже на начин надзора, потенцирајући повјерење у њега, али истовремено и његову свијест о пожељном и прихватљивом коришћењу и интернета и друштвених мрежа. Бројни су модалитети надзора дјеце на друштвеним мрежама, почев преко већ помињаног прихватања родитеља за пријатеље на конкретној мрежи, омогућавањем приступу профилу (наравно,

Родитељи не треба дјецу да контролишу на интернету (у томе неће ни успјети), али их требају надzirати! Могућности надзора су различите.

Дјетету се константно мора указивати на подразумевано и пожељно понашање на интернету.

повременим и у договору са дјететом), преко других профила за које дијете зна да ће их користити родитељи, од стране старијих чланова породице, преко инсталираног „дадиља софтвера“ са којим су и дјеца упозната, преко инсталираних програма или опција које онемогућавају приступ одређеним страницама или приступ интернету преко одређеног времена или периода... У суштини, од дјетета треба захтијевати пожељно и прихватљиво понашање током коришћења интернета и друштвених мрежа, имајући у њега повјерење да ће испунити те захјеве родитеља, али истовремено му стављајући до знања да ће се његово коришћење тих мрежа, па и самог интернета, повремено надзирати од стране родитеља или других лица. Наравно, дјетету треба и ставити до знања да се то неће злоупотријебити, већ да ће то увијек бити уз његово знање и сагласност.

Резимирајући претходно наведено, може се навести да је кључан однос повјерења између родитеља и дјеце, односно родитељи треба да имају повјерење у властито дијете и у његово конформистичко понашање на интернету и када није под њиховим надзором, док, с друге стране, дјеца то треба да „дијене“, те да узврате истом мјером, управо тим конформистичким, односно очекиваним, пожељним и подразумијеваним понашањем, знајући да их родитељи не надзиру, али очекују од њих такво понашање. Уколико би се овај однос константно и континуирано продубљивао и потенцирао, па чак и уз одређене несугласице, свакако да би дао много боље резултате од било какве контроле, па чак и забране коришћења интернета дјечи од стране родитеља.

Мимо проблема дозвољавања дјечи да користе или не користе друштвене мреже, овдје треба поменути и један проблем који у задње вријеме има екстремну тенденцију пораста на Фејсбуку, па и на Инстаграму. Наиме, све више родитеља фотографије властите дјеце поставља на профил у оквиру властитих албума. Иако и само постављање ових фотографија није афирмативно (имајући у виду да фотографије које не би дали непознатима да их виде, не би ни требало постављати на Фејсбук, па чак ни онда када их ограниче само за пријатеље), чињеница је да је то само „врх леденог бријега“ могуће компромитације ових фотографија, а потом и компромитације родитеља, а поготово њихове дјеце. Наиме, релативно често се многобројним могућностима софтверске манипулације на тим фотографијама оне компромитују тако што се

Фотографије голишаве
дјеце и беба родитељи не
смију стављати на
друштвене мреже.

преузму, потом се дјелимично (па чак и незнатно) измијене након чега се постављају у оквиру педофилског садржаја или у одређеном педофилском контексту. Уколико се наведеном дода и чињеница да велики проценат родитеља на Фејсбук поставља и фотографије дјецe на којима су она голишава, није тешко претпоставити колико то потенцира, односно олакшава прикупљање материјала за педофилске активности. Зато се препоручује елиминисање свих таквих фотографија са Фејсбука (за родитеље или друге кориснике који су поставили такве фотографије, те их учинили видљивим), односно непостављање таквих фотографија на Фејсбук од стране родитеља или других корисника који посједују те фотографије.

На крају, родитељи би требало да знају, али и да дјеци представе да је и сама присутност на друштвеним мрежама, без обзира на то како била заштићена, својеврсни „атак на приватност“ интернаута, односно сам интернаут се егзистирањем на друштвеној мрежи добровољно и дјелимично (најчешће и несвјесно) одриче (дијела) властите приватности. Тога треба да буду свјесни сви интернаути, а поготово они који намјеравају да се придруже друштвеним мрежама, јер без обзира на бројне механизме заштите приватности, чињеница је да само присуство у интернет окружењу утиче на редуковање и самог појма приватности, а поготово на угрожавање те приватности коју и не треба посматрати само кроз злонамјерне атакe на корисника.

Родитељи морају да знају да је и само дјечије присуство на друштвеним мрежама атак на њихову приватност!

Резимирајући савјете родитељима, примарно би се могли сублимирати кроз сљедеће:

- родитељи треба да дјецу науче да сви интернаути нису добронамјерни, већ да има и оних који ову друштвену мрежу користе да би друге преварили, нанијели им штету, да би их омаловажили, повриједили, увриједили, осрамотили и слично;
- дјеци не треба бранити коришћење друштвених мрежа, ни коришћење интернета уопште, али се са њима треба договорити да повремено омогуће увид у комуникацију коју

остварују преко „зида“, као и у листу пријатеља, те примљене поруке;

- уколико и родитељи користе одређену друштвену мрежу, обавезно би са дјецом требало да буду пријатељи;
- дјеца (поготово млађа) би требало родитељима да саопште корисничко име и лозинку, али их не би требало без пријеке потребе провјеравати, а поготово не без њиховог знања;
- дјеци се мора скренути пажња на то да, као и у стварности, на друштвеним мрежама за пријатеље не прихватају непознате особе, те да не комуницирају са непознатим интернаутима;
- дјеци се мора скренути пажња да се на интернету морају понашати као и у стварном животу, превасходно да са другима морају комуницирати као и у стварном животу,
- дјеци се мора скренути пажња да на профил не постављају фотографије које су неприличне за јавну употребу;
- родитељи се константно, и преко интернета и на друге начине, морају интересовати за злоупотребе интернета, а превасходно за злоупотребама конкретне друштвене мреже коју користи и њихово дијете.

Све злоупотребе или злостављања преко интернета, као и друге недопуштене или недоличне радње треба пријавити администраторима, као и полицији, уколико се ради о кривичном дјелу.

Реаговање на злоупотребе и негативности н друштвеним мрежама

Све активности, садржаје, профиле, странице и групе за које интернаут (и родитељи и дјеца) сматрају да су непожељни, неподноумијевани, негативни, злонамјерни или да представљају одређену криминалну активност, требало би да пријаве администраторима друштвених мрежа, а код драстичнијих случајева и полицији или другим органима формалне реакције, без обзира на то што се конкретна негативна активност није фокусирала ка њима, па чак ни ка њиховим пријатељима, али су они свјесни негативности. Потенцирањем ове дигиталне антикриминалне солидарности интернаутске популације свакако ће се умногоме отежати активности злонамјерним корисницима, што ће у перспективи свакако непосредно дјеловати и на самог корисника који је пријавио негативну активност, без обзира на то што у том моменту није био непосредно угрожен, свјестан да би се та негативност у блиској будућности могла и ка њему конкретизовати.

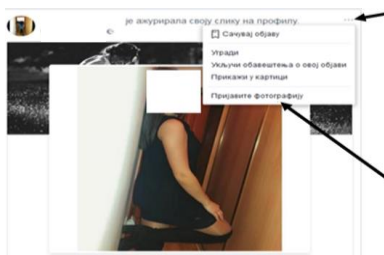
Такође, о свим овим и сличним активностима, садржајима, порукама, профилима, страницама и групама, корисници би требало да обавијесте и своје пријатеље, а везе ка наведеном треба што прије да избришу са свог зида, односно са новости како би се онемогућило несвјесно ширење оваквог садржаја.

Алармирање администратора на друштвеним мрежама

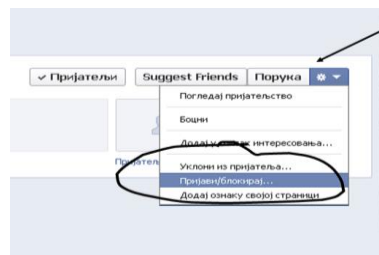
Администраторе друштвених мрежа би могли представити као интернауте са натпросјечним информатичким и интернет знањем, чија је улога, коју су добили од саме мреже, „патролирање“ у оквиру окружења друштвених мрежа, те проактивно дјеловање према узроцима потенцијалног

криминогеног понашања, превентивно дјеловање према потенцијалним изгредницима у оквиру интернет окружења, те репресивно дјеловање према злонамјерним корисницима, као и према корисницима који се не придржавају правила ове друштвене мреже.

Улога администратора је значајна за безбједност дјеце на друштвеним мрежама, због чега родитељи треба да науче како да их алармирају.



На наведеној фотографији је представљен начин на који интернаути на Фејсбуку могу да пријаве непожељни или негативни садржај који други корисници поставе на новостима



На наведеној фотографији је представљен начин на који корисници могу да пријаве корисника Фејсбука за којег сматрају да продукује негативан или непожељан садржај или је запосео туђи идентитет...

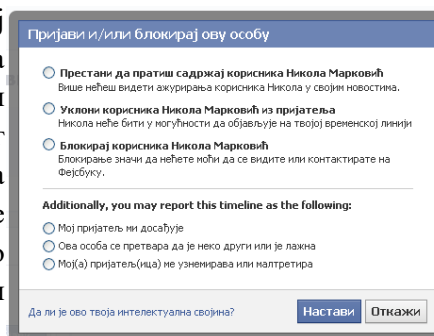
Иако је више модалитета администраторског реаговања, највидљивији корисницима јесте сама пријава одређених негативности на тим мрежама, што ће се показати на следећим фотографијама:

Пријавом конкретног корисника, пријавитељ може да одабере једну од три понуђене опције:

- да престане да прати садржај тог корисника, што значи да неће моћи да прати активности и постављени садржај тог корисника, односно на новостима му се неће приказивати конкретно ажурирање и активности пријављеног корисника.
- да уклони тог корисника из властитих пријатеља; подразумева квалитативно виши ниво блокаде од претходно наведеног, с обзиром на то да блокирани пријатељ, поред претходно наведених активности, више уопште неће моћи да контактира пријавиоца.
- да блокира конкретног корисника; подразумева да се било каква потенцијална накнадна комуникација између ова два корисника, односно између пријавиоца и пријављеног корисника онемогућава.

Поред наведеног, а битније је, корисник може другог корисника пријавити и из других разлога, а то су:

- када му други корисници досађују, под чим треба подразумевати сваку учесталу активност која је конкретном кориснику, односно пријавиоцу иритантна, досадна, непристојна, неподношљива, односно свака активност која му се на било који начин чини неприлична или нежељена, услед тога се може



десити да многобројни корисници Фејсбука буду пријављени од стране других корисника, иако им је комуникација са пријавиоцима крајње безазлена, наравно, по њиховом схватању;

- драстичнији облик од претходно наведеног, које и сами администратори много озбиљније посматрају, јеста када пријавиоци пријави другог корисника

услед узнемиравања или малтретирања или сличне активности;

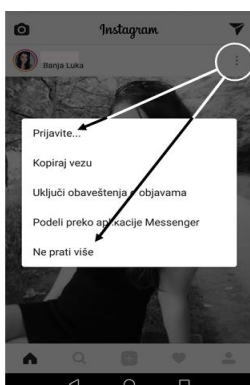
- корисници могу друге кориснике пријавити и уколико знају или сумњају да се тај корисник користи запосједнутим или лажним идентитетом, што је један од чешћих случајева ове пријаве, поготово уколико се има у виду да на овај начин корисници којима је запосједнут или украден профил могу, преко профила властитих пријатеља, да алармирају администратора у релативно краћем периоду, те да поврате контролу над компромитованим профилем или бар да донекле онемогуће даљу (потенцијалну) компромитацију са властитог профила, од стране злонамјерног корисника.

- Треба напоменути да је пожељно да корисници којима је запосједнут или на било који други начин украден профил, о томе обавијесте властите пријатеље на Фејсбуку како би они, у већем броју, алармирали администраторе на овај начин, јер је разумљиво да

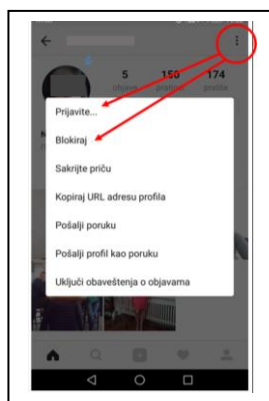
ће и сами администратори, услед великог (прилива) броја пријава у релативно краћем периоду адекватније и брже реаговати на ову негативну активност. Обично администратори реагују на одређени садржај, активност, профил или групу уколико је то пријавило 200 корисника у релативно краћем периоду, што треба имати на уму приликом пријављивања тога администратору, те алармирати овај неопходан број пријатеља.

Разлози пријављивања или блокирања корисника на друштвеним мрежама су многобројни. Родитељи треба да блокирају и пријаве све кориснике који се на било који начин непримјерено понашају.

О украденом профилу је потребно хитно обавијестити што већи број интернаута.



На наведеној фотографији је представљен начин на који интернаути на Инстаграму могу да пријаве недоличну фотографију постављену од стране других пратилаца, као и како да не прате тог корисника више



На наведеној фотографији је представљен начин на који пратиоци могу да пријаве корисника Инстаграма за којег сматрају да продукује негативан или непожељан садржај или да је запосјео туђи идентитет...

Пријављивање кривичних дјела полицији

Драстичније облике нарушавања дјечије приватности или продуковање материјала, садржаја и активности које имплицирају криминалну активност преко друштвених мрежа потребно је пријавити полицији. То се поготово односи на следеће ситуације:

- изнуђивање фотографија од дјецe, сексуалног контекста,
- уцјењивање дјетета да се слика у недоличним позама или наго, те прослеђивање фотографија,
- комуницирање са дјететом гдје се потенцира сексуална активност или је садржај комуникације сексуалне природе, без обзира на то што је дијете навело ког је узраста,
- инсистирање на састанку са дјететом,
- пријетње убиством или пријетње објављивања компромитујућег садржаја, поготово садржаја који имплицира сексуални контекст;
- креирање група или садржаја којима се посебно понижава или деградира или вријеђа дијете,
- свака друга ситуација, активност или садржај на друштвеним мрежама за које родитељ сматра да представљају кривично дјело или другу забрањену радњу.

У већини ових и сличних ситуација, односно у већини ситуација у којима се продукује одређена негативност преко интернета и друштвених мрежа на штету дјетета, битно је хитно поступање. У немалом броју

Сумњу на дјечију порнографију и педофилију, као и на друге облике кривичних дјела потребно је пријавити полицији.

случајева је битно да се благовремено пријави свака потенцијално инкриминисана активност или садржај.

Уколико је могуће, прије самог пријављивања, потребно је да родитељ или неко од укућана, чланова породице или наставника обави разговор са дјететом о свим околностима спорне ситуације, комуникације, активности или садржаја, како би пријавитељ (разумљиво је да пријаву не мора да поднесе искључиво жртва, већ могу и родитељи или неко други ко је упознат са случајем) описао што детаљније спорни или инкриминисани догађај, те како би полиција благовремено и садржајно предузела радње и мјере из властите надлежности на утврђивању квалификације пријављеног догађаја, а потом на релевантности и садржајности околности догађаја, те на идентификацији и локализацији злонамјерног интернаута.

Битно је навести да родитељи треба да пријаве сваку активност за коју сумњају да представља незаконито, односно забрањену и негативну активност или садржај преко друштвених мрежа за коју су увјерени да је усмјерена ка дјечи. Родитељи не морају бити сигурни у инкриминисаност спорног садржаја или активности, већ је довољно да сумњају у одређене активности, а на полицији је да њихове сумње провјери, потврди или одбаци.

Исто тако, битно је навести да родитељи не треба да провјеравају да ли та активност и стварно представља или не представља кривично дјело, а поготово они сами не треба да

Родитељи не требају да самоиницијативно провјеравају сумње у погледу нелегалне активности на интернету.

„истјерују правду“ користећи се властитим могућностима и знањем. То ће неријетко бити контрапродуктивно: с једне стране, те активности и комуникација могу прерасти у инкриминисану активност, чега родитељи неријетко неће бити свјесни, док, с друге стране, ријетко ће њихов ангажман довести до откривања извршиоца, већ ће упозорити злонамјерног интернаута да је његова злонамјерна активност откривена, што ће условити повећање његове опрезности.

Иако је за благовремено и садржајно поступање полиције усмена пријава у службеним просторијама полиције најадекватнија, битно је навести да родитељи, као и друга лица све пријаве за које сумњају да представљају злонамјерне активности и садржаје које се преко интернет

ресурса продукују према дјечи и за које сматрају да представљају кривична дјела могу пријавити и телефоном, као и електронским путем.

Превентивне активности Министарства унутрашњих послова Републике Српске на предупредивању негативности друштвених мрежа

Министарство унутрашњих послова Републике Српске је, препознајући проблем вршњачког насиља, а поготово електронског вршњачког насиља, и то примарно коришћењем Фејсбука, 2009. године покренуло Пројекат превенције малољетничке делинквенције у оквиру којег су се, између осталог, основношколској и средњошколској популацији држала предавања и радионице о облицима испољавања насиља, вршњачког насиља, електронског вршњачког насиља, као и других облика насиља на друштвеним мрежама. Такође, ученицима су одржана и предавања о могућностима злоупотребе информационо-комуникационих технологија, интернета и Фејсбука у овом контексту, те им је указано на могућности (и неопходност) властите заштите приликом коришћења интернета и Фејсбука, али и на могућности заштите уколико се према њима или лицима које познају констатују активности које представљају акте насиља на интернету, односно на Фејсбуку.

Пратећи и аналитички сагледајући стање безбједности у Републици Српској, те модалитет испољавања кривичних дјела и прекршаја према дјечи и малољетницима на друштвеним мрежама, наметнула се потреба ревидирања постојећег пројекта превенције малољетничке делинквенције, те је школске 2015/2016. године донесен нови и ревидирани План и програм спречавања малољетничке делинквенције у основним и средњим школама у Републици Српској, са одређеним модификацијама превентивних програма условљених актуелном безбједносном проблематиком.

Основни циљ превентивних активности обухваћених овим планом и програмом јесте упознавање циљне популације са одређеним безбједносно-ризичним облицима понашања, облицима испољавања негативности према ученицима, те са начинима адекватног и афирмативног реаговања на те негативности.

**МУП РС од 2009. године
спроводи превентивне
активности усмјерене на
предупредивању негативности
на друштвеним мрежама.**

С обзиром на стварну и претпостављену виктимизираност ученика током коришћења ресурса интернета, акценат је на едукацији ученика о безбједном коришћењу интернета, затим на упознавању дјеце са опасностима које постоје на интернету и које су усмјерене ка њима током њихове виртуелне егзистенције, али и упознавање са модалитетима властите заштите током коришћења интернета.

Циљна популација су ученици, родитељи ученика, те наставни кадар и други радници који учествују у реализацији наставе.

Превентивно-едукативне активности пројекта се односе на три садржаја:

1. Едукација о безбједносним ризицима коришћења друштвених мрежа и о друштвено пожељном коришћењу мрежа, у оквиру које се реализују посебна предавања за:
 - ученике,
 - школско особље,
 - родитеље;
2. Едукација ученика о негативностима коришћења наркотичких средстава,
3. Едукација ученика о перцепцији и начину реаговања на сексуално узнемиравање.

Родитељи могу преко савјета родитеља, школских одбора, али и самостално да се обрате школи или полицијској станици уколико желе да им се одржи предавање о овој проблематици.

Циљ едукације родитеља јесте подизање свијести о безбједносним ризицима и опасностима коришћења друштвених мрежа, као и иницирање и афирмисање друштвено пожељног понашања дјеце на друштвеним мрежама. Током превентивно-едукативних активности, требало би да се реализују следећи задаци:

- упознати родитеље са негативностима на интернету;
- научити родитеље начинима надзора над виртуелном егзистенцијом дјеце,
- упознати родитеље са индикаторима електронског вршњачког насиља,
- упознати родитеље са процедуром пријаве негативности на друштвеним мрежама.

Коришћена литература

1. Билић, Весна, Буљан-Фландер, Гордана, Хрпка, Хана, *Насиље над дјецом и међу дјецом*, Наклада Слап, Јастребарско, 2012. године,
2. Грбић-Павловић, Николина, Павловић, Гојко, *Вршњачко насиље из угла ученика основних школа на подручју бањалучке регије – Анализа емпијског истраживања*, Зборник радова "Вршњачко насиље", Висока школа унутрашњих послова Бања Лука и Ханс Зајдел фондација, Лакташи, 2013. година,
3. Ђорић, Марија, *Булинг као врста социјалног насиља*, Политичка ревија, Београд, број 3/2009,
4. Ђурић, Мирослав, *Активности у превенцији малољетничке деликвенције (социјално-психолошки приступ)*, Графомарк, Лакташи, 2012. године,
5. Ковачевић – Љепојевић, Марина, Жунић – Павловић, Весна, Ковачевић, Милица, *Родитељски надзор деце и адолесцената на интернету*, Зборник радова "Интернет и друштво", Српско социолошко друштво, Универзитет у Нишу, Институт за упоредно право, Ниш и Београд, 2014. године,
6. Миладиновић, Александар, *Фејсбук и криминалитет*, Интернационална асоцијација криминалиста, Бања Лука, 2013. године,
7. Миладиновић, Слободан, *Деца на интернету и онлајн друштвеним мрежама*, Зборник радова "Интернет и друштво", Српско социолошко друштво, Универзитет у Нишу, Институт за упоредно право, Ниш и Београд, 2014. године,
8. Муратбеговић, Елмедин, Вујовић, Срђан, *Понашање и навике дјеце на интернету: ставови дјеце, родитеља и наставника информатике*, Save the Children in North West Balkans, Сарајево, 2016. године,
9. Рамљак, Томислав, Херцег – Пакшић, Барбара, Велки, Тена, Ромстеин, Ксенија, *Мапа пута борбе против сексуалног и других облика насиља над дјецом на интернету у БиХ*, радни материјал, 2016. године,
10. Сандерс, Кристина, *Завођење дјетета – Како заштитити дјецу од сексуалног злостављања – смјернице за родитеље и учитеље*, ВБЗ, Загреб, 2005. године,
11. Сумоња, Сања, Скакавац, Татјана, *Насиље путем интернета као облик малољетничког вршњачког насиља*, Зборник радова "Вршњачко насиље", Висока школа унутрашњих послова Бања Лука и Ханс Зајдел фондација, Лакташи, 2013. године,
12. Човић, Ана, *Начини злоупотребе деце путем интернета*, Зборник радова "Интернет и друштво", Српско социолошко друштво, Универзитет у Нишу, Институт за упоредно право, Ниш и Београд, 2014. године
13. Група аутора, *Дјеца на интернету – могућности, ризици, безбједност*, Извјештај за Црну Гору, УНИЦЕФ – ИПСОС – Global Kids On Line – Влада Црне Горе, Подгорица, 2016. године,
14. *Стање дјеце у свијету 2017 – Дјеца у дигиталном свијету*, Извјештај, УНИЦЕФ.