Водич за родители за заштита на приватноста и личните податоци на децата на интернет

Дирекција за заштита на личните податоци

МЕТАМОРФОЗИС
Фондација за интернет и општество

Скопје, јуни 2015

Водичот за родители е изработен во рамки на заедничката соработка меѓу Дирекцијата за заштита на личните податоци и Метаморфозис, Фондација за интернет и општество и средните училишта на Град Скопје, како дел од проектот ЧАС ПО ПРИВАТНОСТ.

Водичот го изработија:

- **м-р Лилјана Пецова Илиеска, Дирекција за заштита на личните податоци, и**
- **м-р Тамара Ресавска, Метаморфозис, Фондација за интернет и општество**

Дирекција за заштита на личните податоци

Контакт:

Дирекција за заштита на личните податоци

бул. „Гоце Делчев“ бр.18 1000 Скопје, Македонија,

Тел: ++389 (0)2 3230 635

Факс: ++389 (0)2 3230 635

Имејл: info@privacy.mk

Веб: www.privacy.mk

МЕТАМОРФОЗИС
Фондација за интернет и општество

Контакт:

Метаморфозис, Фондација за интернет и општество

Ул. „Апостол Гусларот“ 40, Скопје, Македонија

Тел: ++ 389 (0)2 3109 325

Имејл: info@metamorphosis.org.mk

Веб: www.metamorphosis.org.mk

Вовед

Некои работи се менуваат со текот на годините, но некои работи остануваат исти. Децата ја имаат истата потреба за комуникација, потреба да се социјализираат, да се забавуваат, но и покрај тоа повеќе од потребно е и да се заштити нивната приватност преку превенција од злоупотреба на личните податоци.

Овој Водич не е за да Ве вознемири Вас, родителите, и да создаде страв за новиот свет на технологија што го користи Вашето дете, туку едноставно да придонесе да се подигне свеста за функционирањето на новите технологии, како може заеднички да истражувате низ „море од информации“,како да го заштитите Вашето дете од пристап кон недолични содржини и комуникации, како и кои се механизмите за пријава доколку, Вие или вашето дете, се соочите со злоупотреба на личните податоци на социјалните мрежи.

Фокусот на овој Водич е поставен кон интернетот, кон социјалните мрежи, но претставени се и други форми на комуникација и клучни места каде што е можна злоупотреба на личните податоци и нарушување на приватноста.

Покажувајќи интерес за технологиите што ги користи Вашето дете, Вие можете да учите заедно со него/неа и да знаете што прави кога „седи на интернет“.

Од авторите

Кон Водичот

Овој Водич произлезе како потреба, согледувајќи ги анализите што ги направи Дирекцијата за заштита на личните податоци во 2014 година, како и истражувањето што беше направено во рамки на проектот ЧАС ПО ПРИВАТНОСТ во 2015 година, каде што беа воочени следните резултати:

- Дури 64% од родителите мислат дека нивните деца не се запознаени со политиките на приватност на социјалните мрежи кои ги посетуваат,
- Социјалните мрежи најмногу ги плашат родителите, па 68% од нив мислат дека ова е најголемата закана;
- 60% од родителите сметаат дека поважна улога во едуцирањето имаат самите тие како родители

Сето ова за нас беше индикатор дека е и повеќе од неопходно да се пристапи кон изработка на ваков Водич каде што ќе се разработат темите за заштита на приватноста, заштитата на личните податоци, како и безбедноста на интернет на децата и сите можни предизвици што ги носи со себе користењето на интернетот. Убедени сме дека на ваков начин ќе ја доближиме информацијата до секој родител и дека ќе делуваме превентивно за подигање на јавната свест за заштита на личните податоци при користењето на социјалните мрежи. Воедно, се надеваме дека ќе им служи како упатство со корисни препораки, промовирајќи ги и механизмите за пријава кои им се на располагање на граѓаните.

Димитар Ѓеорѓиевски,
Директор, Дирекција за заштита на личните податоци

Со се поголемото секојдневно користење на интернетот и социјалните медиуми, родителите се соочуваат со еден нов предизвик, а тоа е како да ги заштитат своите деца од ризиците кои со себе ги носи интернетот, и да ги научат безбедно и одговорно да го користат. Фондацијата Метаморфозис со својата долгогодишна работа во ова поле има развиено повеќе ресурси наменети за едукација на децата и родителите за тоа како да ја заштитат нивната приватност и како безбедно и сигурно да го користат интернетот. Овој водич претставува продолжување на тие напори и придонесува кон подигнувањето на свеста кај родителите за заштитата на приватноста. Нашата цел не е да ги исплашиме родителите од интернетот и новите технологии, туку напротив, да овозможиме максимално да ползуваат од интернетот со тоа што ќе бидат во тек со промените во дигиталниот свет, ќе стекнат нови вештини, ќе ги поттикнеме да размислуваат за прашањата поврзани со ризиците и предностите од користењето на интернетот, а воедно и ќе им помогнеме да се справат со предизвиците со кои се соочуваат при едукација на децата за безбедно и одговорно користење на интернетот.

Бардил Јашари,
Директор, Фондација Метаморфозис

Содржина

Глава 1

Што е интернет?

Интернетот е збир на компјутери распространети низ целиот свет и поврзани еден со друг заради размена на информации. Доаѓа од комбинација на зборовите "**Inter**national" (меѓународна) и "**net**work"(мрежа).

„Интернетот беше првично замислен како огромна база на податоци за користење во научни и образовни цели. Оттука, главна улога на Интернет беше архивирање и комуникација. Како што растеше бројот на компјутерите поврзани со Интернет, така растеше бројот на организациите кои нудеа он-лајн информации и бројот на посетителите на веб-страниците (кои се потенцијални корисници на производите и услугите).

Денеска, Интернет овозможува повеќекратни услуги:

1. **Информации**, преку:

   - World Wide Web (пајажина распространета низ светот) (WWW) - споредливо со консултирање на дигитална библиотека
   - Новински групи - споредливо со списанија посветени на различни теми

2. **Комуникација**, преку:

   - Праќање и примање писма:
   - Програма за разговарање: преку директна врска слична со телефонски разговор, што се овозможува преку програма која овозможува разговор во реално време
   - Електронска пошта (и-меил): преку индиректна врска, слично на пошта
   - Дискусиски групи: преку размена на пораки во рамките на една група (дискусиски групи, новински групи)
   - Конференции: преку директна и истовремена врска помеѓу повеќе корисници
   - Пренос на податоци:
     - FTP услуга (протокол за пренос на датотеки), што овозможува брз пренос на датотеки
     - Прикачување на датотеки кон пренесуваните пораки со помош на електронска пошта
     - преземање од Интернет преку WWW
     - од точка до точка, што овозможува копирање на датотеки од други компјутери бесплатно или по одредена поволна цена."[1]

[1] „Прирачник за информатичка и комуникациска технологија" – 2006, USAID – проект за електронска влада, линк: http://aa.mk/WBStorage/Files/Priracnik%20IKT%20Mak.pdf

Речник на термини поврзани со интернетот

1. **Што е социјална мрежа?**

а. Он-лајн заедница на луѓе со заеднички интерес кои користат веб-страна или друга технологија со цел меѓусебна комуникација и споделување на информации, ресурси, итн.

б. Веб-страна или он-лајн услуга која ја овозможува комуникацијата.

2. Кога Вашето дете оди „**онлајн**“ значи дека се поврзува на интернет. Иако WWW, е само дел од интернет, сепак поимите како: **Web** (веб**), Internet** и **Net**, често се користат за да означат исто – поврзување кон глобална мрежа на информации и комуникација.

3. Поимот **Web** означува и збир на повеќе **Websites (веб-сајтови)** на интернет. Содржи знаење и информации за секоја можна тема или предмет на интерес. Веб-сајт е страница на www. којашто содржи информација. На пример, веб сајтот на Дирекцијата за заштита на личните податоци е www.dzlp.mk. Ова е **веб адресата** на оваа институција.

4. Социјално вмрежување е користење на веб-сајтови или други онлајн технологии со цел комуникација и споделување на информации, итн.

Неодамна излезе и истражувањето за тоа кои се Топ десет најпопуларни страници за социјално вмрежување:

Facebook 900,000,000 – посетители месечно

Twitter 310,000,000 - посетители месечно

LinkedIn 255,000,000 посетители месечно

Pinterest 250,000,000 - посетители месечно

Google Plus+ 120,000,000 посетители месечно

Tumblr 110,000,000 - посетители месечно

Instagram 100,000,000 посетители месечно


VK 80,000,000 посетители месечно

Flickr 65,000,000 посетители месечно

Vine 42,000,000 - посетители месечно

Meetup 40,000,000 - посетители месечно

Tagged 38,000,000 - посетители месечно

Ask.fm 37,000,000 - посетители месечно

MeetMe 15,500,000 - посетители месечно

ClassMates 15,000,000 - посетители месечно

Комуникациите на социјалните мрежи најчесто содржат кратенки, кои им се познати само на најмладите. Па така, на нет може да се најде и листа на најчесто користени акроними од тинејџери (овде во Прилог 1) кои се посебно дешифрирани за збунетите родители.

Политики за приватност на социјални мрежи

Политики за приватност се правила, кои нè информираат сите нас, како корисници на интернет, за тоа на кој начин и зошто се собираат податоците. Доколку сакаме да знаеме како да раководиме со информациите и како да ја заштитиме нашата приватност на интернет, треба да се прочитаат внимателно и да се следат во континуитет бидејќи подлежат на промени.

На пример, во многу од услугите се бара од вас да отворите ваша корисничка сметка на Гугл. Кога ќе го направите тоа, за да се најавите на вашиот профил од вас се бараат лични податоци како што се: име, презиме, имејл, телефонски број или кредитна картичка за складирање на вашиот профил, итн. Ако сакате во целост да ги искористите можностите за споделување на содржини кои се нудат, од вас се бара да креирате јавен профил на Гугл или постоечкиот да го направите јавен, што вклучува јавен приказ на вашето име и презиме и фотографија.

Дополнително, веб-сајтовите собираат податоци со самото користење на нивните услуги. Имено, тие прибираат податоци за уредот, на пример моделот на вашиот хардвер, верзија на оперативниот систем, информации за мобилната мрежа, вклучително и вашиот телефонски број.

На пример, кога ги користите услугите на Гугл, податоците за Вашата локација, IP адреса, Wi-Fi точки на пристап, итн. може да бидат собрани и обработени. Воедно, може да се соберат податоци за идентификација на Вашиот пребарувач или Вашиот уред, преку користење на колачиња (Cookies).

Колачињата (cookies) се мали текстуални фајлови со податоци, коишто може да бидат снимени на вашиот хард- диск од страна на некои од веб-страниците кои ги посетувате и најчесто се користат за рекламни цели, но истовремено го следат („ловат“) вашето движење (додека сурфате) на веб страната.[2]

[2] http://www.google.com/policies/privacy/

Секогаш, ама секогаш!, читајте ги Политиките за приватност на социјалните медиуми, на услугите кои ги нудат, бидејќи таму се наоѓа и лекот како да се заштитите доколку Вашата приватност или приватноста на вашето дете е нарушена.[3]

[3] https://www.facebook.com/about/privacy/

Глава 2

Што е приватност? Кои се личните податоци кои го откриваат нашиот идентитет?

Правото на заштита на личните податоци и правото на приватност се различни човекови права. Поради големото значење на приватноста за поединецот, во најголемиот дел од земјите во светот ова право е регулирано со Уставот како највисок конститутивен акт на државата, каков што е случајот и со Република Македонија.

Во нашиот Устав, во делот посветен на Граѓанските и политичките слободи и права, се опфатени неколку човекови права кои се компоненти на правото на приватност, бидејќи приватноста е поширок, сложен концепт, односно сублимат на неколку поединечни права. Во таа смисла, важно е да се споменат следните права:

- На секој граѓанин му се гарантира почитување и заштита на приватноста на неговиот личен и семеен живот, на достоинството и угледот (член 25).
- На секој граѓанин му се гарантира неповредливост на домот. Правото на неповредливост на домот може да биде ограничено единствено со судска одлука кога во прашање е откривање или спречување на кривични дела или заштита на здравјето на луѓето (член 26).
- Се гарантира слободата и тајноста на писмата и на сите други облици на комуникација. Од ова право може да се отстапи само врз основа на судска одлука и во соодветна законска постапка (член 17).

Издигнувањето на правото на приватност на ранг на уставно загарантирано човеково право укажува на огромното значење на ова право за поединецот, кое со себе носи определени права/овластувања и обврски/одговорности и тоа како за поединецот-носител на правото, така и за останатите поединци, но и за државата и нејзините институции. Ова се трите члена во Уставот на РМ што гарантираат заштита на приватноста. Законот за заштита на личните податоци се однесува само на правата на граѓанинот за заштита на неговите/нејзините лични податоци.

Во Република Македонија не постои посебен закон што се однесува на заштита на приватноста, додека пак во САД постои посебен Закон за заштита на приватноста на децата[4] и се однесува на собирање на лични податоци онлајн од страна на физички или правни лица под американска јурисдикција од деца под 13-годишна возраст. Тоа значи дека се дефинирани податоците што операторот на веб-сајтот мора да ги вклучи во политиката за приватност, кога и како да се бара согласност од родител или старател, и кои се обврските на операторот со кои мора да ја заштити приватноста на децата и безбедноста на интернет, вклучувајќи ги ограничувањата за маркетинг за оние кои се под 13 години.

[4] https://en.wikipedia.org/wiki/Children%27s_Online_Privacy_Protection_Act

Личните податоци кои го откриваат нашиот идентитет вообичачено се:

- Име и презиме
- Адреса на живеење
- Матичен број
- Пол, итн. односно сé што може да доведе до идентификација и верификација на идентитет на едно лице.

Кои се опасностите кои ги демнат децата на Интернет?

Со развојот на новите техонологии и начинот на комуникации, најмногу се грижиме дека децата ќе стапат во контакт со погрешни луѓе онлајн, дека ќе имаат пристап до недолична содржина или материјали и дека на кој било начин ќе бидат злоупотребени.

Следуваат некои од најчестите ризици за вашите деца на интернет и злоупотреби на лични податци со кои може да се соочите, како и препораки како може да се справите со истите.

Кражба на идентитет

Кражба на идентитет е форма на крадење на податоци за лична идентификација на друга личност пришто крадецот се преправа дека е некој друг, превземајќи го идентитетот на другата личност, најчесто со цел да пристапи до ресурсите на истата или да добие средства и други бенефиции во името на таа личност.

Кражбата на идентитетот често се користи како метод за извршување на криминални активности и вклучува неовластено користење на Вашите лични податоци, најчесто вклучувајќи и банкарски податоци, кои можат да бидат искористени за да ве ограбат или да извршат криминал во Ваше име. Кражбата на идентитетот може да биде изведена онлајн, физички со користење на печатени документи, или со комбинација од двете.

Кражба на идентитет на деца се случува кога лични податоци и матичен број на малолетник се користат од страна на друго лице за лична корист, најчесто финансиска. Натрапникот може да биде член на семејството, пријател, па дури и некој странец.

Некои од начините за кражба на идентитет се:

- Кражба на лични податоци од компјутерите со користење на злонамерен софтвер, особено тројански коњ или други форми на шпионски софтвер

- Погодување на цифри на матичниот број со користење на информациии најдени на социјалните мрежи како Facebook (На пример, датуми на раѓање објавени јавно на Фејсбук)
- Јавно објавени фотографии кои лесно можат да се преземат од веб-сајтови
- Спријателување со непознати на социјалните мрежи и искористување на нивната доверба за да се стигне до лични податоци.

Затоа, советувајте ги вашите деца:

- Да не споделуваат лични податоци со нивните пријатели, познаници и други луѓе.
- Секогаш да имаат ефективен и ажуриран антивирус и софтвер против шпиунирање на уредот преку кој пристапуваат на интернет.
- Никогаш да не откриваат лични податоци како одговор на имејл порака, писмо или телефонски повик ако не се сигурни дека барањето е од безбеден извор
- Да ве информираат веднаш доколку добијат сомнителна електронска порака која содржи барање за откривање на било каков вид на личен податок

Што е фишинг?

Фишингот е облик на измама кој опфаќа збир на активности на неовластени –испраќачи, преку користење лажни пораки од е-поштата и лажни веб страници на поголем дел од финансиските организации, обидувајќи се од корисниците да добијат доверливи лични податоци како што се ЕМБГ, корисничко име, ПИН броеви и сл. За жал, голем е бројот на корисници кои не се запознаени со овој вид на измама. Штом еднаш ќе дојдат до доверливите податоци, злонамерните испраќачи или сами ги користат или ги продаваат. Во пораките најчесто се повикуваат на лажни веб страни, кои според изгледот целосно одговараат на веб страните на легитимните компании (фирми).

Најчести форми на фишинг се:

- Лажно предупредување од банката или друга финансиска организација во која од корисникот бараат да ги наведе личните податоци, за да спречат да не дојде до укинување/затворање на сметката.
- Измами од аукциски веб страни, во кои корисникот се убедува да уплати одредена сума на пари за да купи одреден производ, а всушност со тоа корисникот мислејќи дека купува некој производ, врши уплата на лажна сметка.
- Лажна порака од администраторот во која се бараат податоци од корисникот, како што е лозинката.
- Разни известувања во кои се обидуваат да изнудат пари за лажни добротворни цели.
- Пораки со кои се намамува корисникот да уплати одредена сума на пари на лажна сметка (На пример, порака за драстично намалување на цената на одреден производ кој може да се купи само на Интернет).
- Пораки кои Ве известуваат дека сте добиле на лотарија и дека им се потребни Вашите лични податоци за да може да ја подигнете наградата.

Како да препознаете фишинг порака?

Измамниците често го копираат визуелниот изглед на вистинските веб страни на банките и други компании. Во последно време лажните пораки се во целост идентични со оригиналите, меѓутоа постојат одредени детали кои ја откриваат измамата:

- Правописни и граматички грешки;
- Се бараат лични податоци;
- Се бара инсталирање на програма за која се тврди дека ќе го поправи пронајдениот сигурносен пропуст;
- Лажни линкови и пораки;
- Не користење на SSL и дигитален сертификат;
- Содржината на пораката е HTML образец;
- Нереални ветувања;
- Грешки во предметот на пораката;
- Се бара итен одговор;
- Не гласат на одредена личност;
- Нереални ветувања;
- Грешки во предметот на пораката;
- Се бара итен одговор;

Говор на омраза

Говорот на омраза е пристрасен, непријателски, злонамерен говор насочен кон еден човек или група луѓе поради некои карактеристики[5] кои ги имаат или кои им се припишуваат дека ги имаат. Во најширока смисла, говорот на омраза се употребува за сите форми на изразување што шират, поттикнуваат, промовираат или оправдуваат омраза заснована на нетолеранција, врз која и да е дискриминаторска основа.

Говорот на омраза е злоупотреба на слободата на изразување што се состои во повреда на правата на другите.

Под **говор на омраза „он-лајн“** („сајбер-омраза“) се подразбира која било употреба на технологијата на електронски комуникации за ширење антисемитски, расистички, ксенофобични, дискриминаторски, екстремистички или терористички содржини.

Изразот говор на омраза „он-лајн“ е поширок од изразот говор на омраза на интернет затоа што ги опфаќа не само интернет-содржините (веб-страници, социјални мрежи, кориснички-генерирани содржини, блогови, он-лајн игри, е-пораки итн.) туку и содржините на мобилните телефони.

Како изгледа говорот на омраза?

Низ призмата на хумор, француските корисници на Твитер објавија пораки со омраза кон Евреите групирани под хаштагот „#добаревреин“, „#мртовевреин“ („#unbonjuif“, „#unjuifmort“).

Француските здруженија поднесоа тужба против компанијата Твитер поради јавно поттикнување на дискриминација, омраза или насилство. По тужбата, компанијата беше обврзана да ги даде податоците со кои може да се идентификуваат интернет корисниците кои биле автори на твитовите.

Што да направите доколку вашето дете е жртва на говор на омраза онлајн?

- Пријавете кривично дело во полиција или Јавно обвинителство. Според Кривичниот законик од РМ, ширењето омраза е кривично дело за кое следува казна од 1 до 10 години затвор. Во МВР тоа може да се пријави и анонимно, во најблиската полициска станица, преку телефонот 192 или до Одделението за компјутерски криминал на по е-пошта на cybercrime@moi.gov.mk.
- На социјалните мрежи Фејсбук и Твитер:
- Одговорете на постовите или твитовите кои шират омраза, со укажување на авторот што всушност прави, како и користење на хаштагот #немрази или #mosurrej.
- Искористете ги механизмите за пријавување „на копче“ понудени од медиумот преку кој се комуницира пораката

[5] Врз основа на едно или повеќе обележја, специфични за нивниот физички, физиолошки, ментален, економски, културен или социјален идентитет.

Не заборавајте: Говорот на омраза најмногу вирее кога никој не му се спротивставува. Бидејќи насилниците се често и кукавици, тие често се повлекуваат при прв знак на отпор. За некои од можностите за пријавување на говор на омраза може повеќе да прочитате во делот „Упатства“ на веб-сајтот „Не мрази“ (nemrazi.mk/category/upatstva).

Што е сајбернасилство?

Социјалното дружење и многуте можности што ги нуди интернетот се обележје на 21 век. Животот на децата се одвива на неколку места истовремено, како што се училишните ходници, домовите на нивните пријатели, но и на интернет.

Повеќето деца и тинејџери поминуваат голем дел од времето на својот мобилен телефон или на компјутер, четувајќи со своите пријатели, ставајќи слики, видеа и музика на различни социјални мрежи, кои им овозможуваат дружење и забава. Можеби имаат онлајн-пријатели кои никогаш не ги сретнале во живо, со кои играат игри и разменуваат пораки.

Онлајн-насилството, наречено сајбернасилство, се случува кога децата и тинејџерите, користејќи интернет, мобилни телефони или други технолошки уреди, објавуваат навредливи информации во вид на текст, слики или други видови содржини, со намера да повредат или да посрамотат друга личност.

Како може да изгледа сајбернасилството?

- Вознемирување – константно праќање навредливи, вознемирувачки и груби пораки и порнографски материјали
- Имитирање - пробивање во туѓи кориснички сметки и праќање лажни, засрамувачки пораки во туѓо име
- Омаловажување - пишување гласини или други неточни изјави кои може да ù наштетат на жртвата, како и слики со понижувачка содржина и срамни лични информации и нивно праќање или објавување на интернет
- Измамување и јавно откривање – споделување туѓи лични информации или измамување некого за да ги сподели своите тајни со цел да ги препраќа на други
- Вулгарно обраќање – праќање пораки со вулгарна содржина
- Сајбердемнење – константно заплашување на жртвата за својата безбедност

<u>Што ако вашето дете е жртва на сајбернасилство?</u>

- Посоветувајте ги вашите деца да ја блокираат комуникацијата со сајбернасилниците, да не отвораат и не одговараат на електронската пошта или пораки од некој кој знаат дека е сајбернасилник.
- Побарајте да ви ги покажат пораките доколку се соочуваат со одреден проблем и заедно разговарајте за содржината на истите

- Чувајте ги или печатете ги сите пораки од насилниците како докази, кои можете да им ги прикажете на интернет- провајдерите на услуги, па дури и на полицијата, кои потоа соодветно ќе може да се справат со силеџијата.
- Доколку личните податоци на вашето дете се злоупотребени на интернет, можете да го пријавите случајот во Дирекцијата за заштита на лични податоци (www.dzlp.mk).
- За тешки случаи на сајбернасилство, кои вклучуваат закани за физичко насилство, можете да се обратите во полиција.
- Пријавувајте ги злоупотребите на веб-сајтовите и социјалните мрежи, кои имаат соодветни опции насочени кон блокирање на одредена личност или порака (Report или Block) или пријавување на несоодветни содржини, или со обраќање директно до администраторот.
- Најважно од се, зборувајте со вашите деца за тоа што прават на интернет.

Онлајн грабливци

Интернетот е многу поанонимен од реалниот свет. Луѓето може да го скријат својот идентитет па дури и да се преправаат дека се некој друг. Ова може да претставува вистинска опасност за децата и тинејџерите кои се онлајн. Онлајн грабливците може да се обидат да ги намамат децата и тинејџерите во сексуални разговори, па дури и на лични средби. Грабливците понекогаш може да им испратат несоодветни содржини или да побараат од децата да им испратат фотографии. Затоа, важно е да ги подучите вашите деца секогаш да внимаваат кога се онлајн.

Тинејџерите се генерално на поголем ризик од онлајн грабливци, бидејќи се љубопитни и сакаат да бидат прифатени, може да разговараат доброволно со грабливец, дури и ако знаат дека тоа е опасно. Понекогаш тие може да поверуваат дека се вљубени во некого онлајн, зголемувајќи ги шансите да се согласат на средба лице в лице.

Како да препознаете дека вашето дете е можеби жртва на онлајн грабливци?

- Доколку вашето дете е наведувано од грабливец тоа може да поминува повеќе време во соби за четување.
- Вашето дете добива телефонски повици од луѓе кои не ги познавате или се јавува на броеви кои не ги знаете.
- Вашето дете добива подароци по пошта од други градови или надвор од државата од луѓе кои не ги знаете.

!Грабливците честопати им испраќаат писма или подароци на нивните потенцијални жртви.

Што да ги советувате вашите деца:

- Да избегнуваат сугестивни имиња или фотографии кои може да го привлечат вниманието на грабливците. На пр. Sexygirl15, hotboy2001.
- Доколку некој им ласка и дели комплименти онлајн треба да бидат внимателни. Предаторите може да искористат ласкање за да се обидат да започнат врска со тинејџери. Ова не значи дека треба да се сомневаат во сите, но треба да бидат внимателни.

- Да не разговараат со било кој кој сака да разговара за премногу лични работи. Доколку некој сака да разговараат за работи кои се сексуални или лични, треба да го прекинат разговорот.
- Да имаат на ум дека луѓето не се секогаш онакви какви што се претставуваат. Грабливците може да се преправаат дека се деца или тинејџери за да разговараат со деца онлајн, може да искористат лажна фотографија или да додадат други информации на профилот за да изгледаат поубедливо.
- Никогаш да не се договараат да се сретнат со некого кого го запознале онлајн. Грабливците може да се обидат да договорат средба со дете или тинејџер. Дури и ако личноста изгледа учтиво и безопасно, ова може да биде многу ризично.
- Веднаш да кажат на родител или возрасен на кој му веруваат доколку наидат на проблем. Доколку некој направи да се почувствуваат неудобно онлајн, треба веднаш да кажат на родителите или на возрасен на кој му веруваат. Воедно, треба да ги зачуваат имејл пораките и другата комуникација со грабливецот, бидејќи може да бидат потребни како доказ.

Не заборавајте:

- Зборувајте со вашите деца за онлајн грабливците и опасностите на интернет.
- Поставете го компјутерот во заедничка просторија каде ќе имате увид и ќе може да го надгледувате вашето дете додека е на интернет.
- Поставете временска граница за користењето на компјутерот.

Зависност од видео игри

Зависноста од видео игри претставува прекумерна употреба на компјутерски или видео игри, што има влијание на секојдневниот живот на личноста.

Некои од емоционалните знаци на зависност од видео игри се чувство на немир или вознемиреност кога не се игра, преокупација со мисли за претходните онлајн активности или очекување на следната сесија, лажење на пријателите или членовите на семејството за времето поминато во играње игри, изолација од другите со цел да се помине повеќе време во играње.

Знаци според кои може да ја препознаете зависноста од видео игри:

- Преокупираност – Детето поминува многу време во размислување за игри, дури и кога не игра или планира што може да игра следно.
- Повлекување – Чувство на немир, иритабилност, нерасположеност, нервоза, анксиозност или тага кога детето ќе се обиде да го намали времето кое го поминува во играње или престане со играта или кога не може воопшто да игра.
- Толеранција – Детето чувствува дека мора да игра се повеќе и повеќе, да игра повозбудливи игри или да користи помоќна опрема за да го постигне нивото на возбуда како и претходно.

- Намалување/престанување – Детето чувствува дека треба да игра помалку, но не може да намали или да скрати од времето кое го поминува во играње игри
- Откажување од други активности – Детето губи интерес или се помалку учествува во други рекреативни активност (хобија, средби со пријатели) поради игрите
- Продолжува и покрај проблемите – Детето продолжува да игра игри иако е свесно за негативните последици, како што се недостаток на сон, доцнење на училиште, трошење пари, караници со другите или запоставување на важни задачи
- Измама/ прикривање – Детето го лаже семејството, пријателите и другите за времето кое го поминува во играње

Што да направите ако вашето дете поминува премногу време во играње на видео игри?

- Ограничете го времето кое детето го поминува пред компјутер.
- Разговарајте со вашето дете за негативните страни од прекумерното играње игри и недостаток на социјализација
- Погледнете го најновиот филмски хит во кино, задолжете го вашето дете да ги напумпа гумите од велосипедот, поттикнете го вашето дете да излезе и да се забавува со другарчињата
- Потсетете го дека постои живот и надвор од видео игрите – не заборавај да го живееш.

Што велат професорите?

Кои се предизвиците со кои се соочува еден ученик кој има профил на социјалните мрежи?

Одговори побаравме од неколку координатори на проектот ЧАС ПО ПРИВАТНОСТ:

м-р Николина Ивановска, професор по психологија во Средно училиште на Град Скопје „Никола Карев“
„Поседувањето на профил на социјална мрежа од страна на еден малолетен ученик има свои предности и недостатоци. Паралелно со оние веќе познати предности во насока на социјализација, брз пристап до новости и информации итн, на несвесно ниво често се занемаруваат и одредени недостатоци кои имаат големо влијание врз развивањето на личноста кај малолетникот. Не ретко се среќаваме со случаи кај кои вреднувањето на себеси е врз основа на број на собрани лајкови на фотографија, а тоа директно влијае врз посериозни сегменти од развојот на личноста поради расчекорот помеѓу идеалната и реалната слика за себе и можност за појава на психолошки растројства кај малолетникот.

Етикетирањето, говорот на омраза, масовното ширење на некаков став од страна на одредена група, исто така имаат огромно влијание врз развојот на личноста, а ова влијание за жал се занемарува од страна на возрасните. Како наставници и родители не секогаш посветуваме доволно внимание на опасностите затскриени под одредени наслови, личности кои стојат зад одредени профили, огромниот број на нечии лажни профили со кои нашите деца се во контакт итн.

Се чувствува дека владее некој колективен став на не доволно сериозно пристапување кон социјалните мрежи од страна на возрасните и нивното влијание врз децата со што доаѓа во прашање воспитниот и образовниот процес врз детето.

Како педагози и родители должни сме да бидеме во тек со модернизацијата на технологијата и развивањето на социјалните мрежи кои се двигател на современото општество и само на тој начин, разбирајќи ги и следејќи принципите на овие мрежи може да влијаеме врз развојот на нашите деца, а со тоа и да создаваме личности кои успешно ќе ги детектираат и избегнуваат опасностите на кои се изложени.“

Анита Армагинијан- Тасевска, училишен педагог во СУГС „Арсени Јовков“ порачува:

„Современото општество носи со себе промени кои сите ние ги чувствуваме како родители, како наставници, па дури и нашите деца. Овие промени се видливи околу 12-та до 15-та година, а кај децата се јавува и потребата да се биде активен на социјалните мрежи.

Дали сме подготвени како родители, наставници и стручни соработници да им објасниме на нашите деца и она што е најважно, да им посветиме време на децата, да видиме што објавуваат на социјалните мрежи како индикатор за промените кои ги доживуваат? Социјалните мрежи ни

нудат различни информации, слики, претстави за нешто ново, интересно, но се наметнува прашањето колку децата или средношколците сето ова го сфатиле и можат да го користат?

Мислењето на родителите најчесто оди од крајност во крајност, од допуштање на децата да прават сè, до ограничувања и забрани. Не смееме да заборавиме дека децата на училиште доаѓаат со скапи мобилни телефони и таблети, сакајќи да си го покажат својот статус, но и често пати ги употребуваат за време на наставата, сакајќи да ги имаат сите информации и пораки кои се пренесуваат на социјалните мрежи.

Како родител, наставник и стручен соработник сметам дека на децата треба да им го оставиме детството да го живеат како деца, да си играат со играчки и со своите другарчиња, бидејќи тој период не можеме да го вратиме никогаш повеќе.

Моето мислење е дека во овој период детето или средношколецот е подготвен да споделува информации со своите врсници, но зависи од зрелоста и одговорноста на детето од една страна и незабележителната контрола на родителот од друга страна.“

Како размислуваат родителите?

Какви се ставовите на родителите за објавување на фотографиите од децата на социјалните мрежи?

Сузана Аврамовска, родител на средношколец од СУГС „Панче Караѓозов“ вели: „Не сум против објавувањето на фотографии од деца на социјалните мрежи, доколку содржината на тие фотографии не е вулгарна и/или не го загрозува идентитетот на детето, на профил кој е заштитен од лицата кои не се во листата на пријатели... За прашањето дали треба да имаат личен профил, барем до 15 години сум против... а од 15 години треба да е под надзор на родител. Најважно нешто во врска со социјалните мрежи е да не дозволиме децата да го заменат реалниот живот со виртуелниот.“

Родител на средношколец од СУГС „Јосип Броз Тито“ (анонимно) смета дека: „Објавата на фотографии од страна на детето и негови соученици не го гледам како проблем, се додека не се работи за недолични содржини или материјали кои би можеле со самата објава да навредат некого или доколку повикува на говор на омраза. Она што најмногу ме плаши како родител е доколку моето дете биде доведено во несакани ситуации или вовлечено во разговори со недолична содржина. Сметам дека разговор со него најмногу би помогнало во такви ситуации, иако не сум против и сам да истражува за одредени прашања на интернет. Како и да е, избегнувам да ставам негови фотографии, бидејќи мојата листа на пријатели не е иста како листата на неговите врсници. Со тоа сметам дека исклучувам можности за злоупотреба, но и ако сам не внимава ништо не правиме.“

Глава 3

Механизми за пријава

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ - Постапка за поднесување иницијатива за вршење инспекциски надзор - Граѓаните поднесуваат до Дирекцијата барања[6] и претставки[7] кои се однесуваат и на злоупотреби на социјалните мрежи. Дирекцијата постапува по барањата и претставките кои се однесуваат на најчестите видови на злоупотреби на социјалните мрежи како што се пријави за бришење на лажни профили на Facebook, бришење на хакирани профили. Дирекцијата постапува и по претставки за откривање на ИП адреса кои ги препраќа до Министерството за внатрешни работи, неовластено објавување на фотографии, претставки поради злоупотреба на податоци за малолетници и други. Секоја година бројот на барања и претставки кои граѓаните ги упатуваат до Дирекцијата се зголемува[8].

Доколку се соочите со злоупотреба на вашите лични податоци или личните податоци на Вашето дете или се сомневате за злоупотреба, може да пријавите во Дирекцијата за заштита на личните податоци на info@privacy.mk или на тел: 02/3230-635

Претставката се обработува веднаш, се разгледува и се доставува до лицето кое е задолжено за тоа. Ако претставката се однесува на злоупотреба на личните податоци на социјалните мрежи и странката бара бришење на креиран лажен профил или хакиран/пробиен профил, ДЗЛП по приемот (вклучително и достава на потребната документација) преку овластените лица, остварува комуникација со административниот тим на соодветната социјална мрежа за стручна помош околу бришењето. По добиениот одговор веднаш се информира подносителот.

Ако Дирекцијата не е надлежна за поставеното прашање, претставката се доставува до надлежната институција и за тоа се известува подносителот на барањето. Ако претставката е поднесена до повеќе органи истовремено, органите меѓу себе соработуваат.

Ако претставката е нејасна или не може да се постапува по неа, потребно е да се побара од подносителот да ја прецизира или да достави докази. Исто така, може да се побара подносителот да се произнесе по претставката, вклучително да биде повикан во ДЗЛП за дополнително утврдување на фактичката состојба. Во секој случај Дирекцијата известува за мерките превземени по претставката.

---

[6] http://www.dzlp.mk/mk/prizlnlp

[7] Под претставка, односно предлог, во смисла на Законот за постапување по претставки и предлози, се подразбира секое писмено или усно обраќање на подносителите до органите кои постапуваат по претставките, односно предлозите заради заштита и остварување на своите права и интереси, јавните интереси утврдени со закон или заради поведување на друга иницијатива од јавен интерес.

[8] Види Годишен Извештај на ДЗЛП за 2013 и 2014 година,
http://www.dzlp.mk/sites/default/files/u4/Godisen_izvestaj_DZLP_2013.pdf
http://dzlp.mk/sites/default/files/u1002/MK.pdf

Ако евентуално постапување по претставка претпостави можност или отвори сомнеж за постапување на други сектори во дирекцијата (на пр: инспекција) или институции надвор од неа (на пр: Јавен обвинител, МВР, итн.) лицата одговорни за постапување по претставките потребно е да достават иницијатива/барање/информација до соодветниот службеник во Дирекцијата.

ОФИЦЕР ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО УЧИЛИШТЕТО - Доколку пак се соочите со злоупотреба на личните податоци на Вашето дете во училиштето, може да го информирате и Офицерот за заштита на личните податоци во училиштето во кое учи детето. Имено, секое училиште има законска обврска, согласно член 26-а од Законот за заштита на личните податоци, секој контролор е должен да определи Офицер за заштита на личните податоци кој ги врши следниве работи: учествува во донесувањето на одлуки поврзани со обработката на личните податоци, како и со остварувањето на правата на субјектите на личните податоци, ја следи усогласеноста со законот и со прописите донесени врз основа на законот, итн. што значи има обврска да биде запознат и да реагира доколку е потребно со измени во одредени прописи и процедури во училиштето доколку не обезбедуваат мерки за тајност и заштита на личните податоци на учениците кои учат во тоа училиште. Офицерот е воедно и алката која е важна во процесот на информирање за заштитата на личните податоци не само на учениците, туку и на наставниците/вработените во училиштето.

Глава 4

Корисни софтвери и додатоци за заштита на приватноста на вашите деца

Софтверот за родителска контрола е одличен начин за контролирање, ограничување и за надгледување на активностите на децата додека се на интернет. Но, нивната безбедност не е единственото нешто што може да се доведе во прашање како резултат на несоодветно користење на интернетот. Безбедноста на целото семејство, па и на компјутерот кој сите го користите, исто така, можат да бидат загрозени. Затоа, треба да разговарате со вашите деца и да им упатувате корисни совети, како и да научите како да се грижите за вашиот компјутер за да го обезбедите неговото правилно функционирање. Некои корисни софтвери кои може да ви помогнат да се погрижите за безбедноста на вашето дете додека користи интернет се следните:

- **Crawler Parental Control** е еден од ретките бесплатни, сеопфатни и целосно функционални софтвери за родителска контрола. Веднаш по инсталирањето се дава администраторска лозинка, која на родителот му овозможува да ги направи саканите приспособувања за секој корисник на компјутерот поединечно. Софтверот овозможува контролирање на времето што корисникот го поминува на интернет, како и ограничување на времето што тој воопшто смее да го помине на компјутер. Може да се наведат одредени веб-сајтови кои корисникот не смее да ги посетува, такви кои за него ќе бидат дозволени, како и зборови кои доколку се пронајдат на некоја веб-страница, ќе го оневозможат пристапот до неа.

  Crawler Parental Control овозможува и ограничување на пристапот на корисниците до одредени папки или пак до цели дискови на компјутерот. Ова ограничување може да биде целосно или да важи за одредени периоди од неделата и од денот, а постои и опција за одредување дозволен број часови кои корисниците смеат да ги поминат во текот на месецот, неделата и денот. Секако може да се блокираат и одредени програми, како и да се забрани пристапот до одредени системски локации заради спречување промени кои можат да ја оневозможат правилната работа на системот.

  За сево ова, вие како родител, доколку сакате можете да добивате извештаи.

  Линк за преземање: http://download.cnet.com/Crawler-Parental-Control/3000-27064_4-10549693.html

- **Glubble** е многу популарна фамилијарна алатка, која се користи како додаток за интернет-прелистувачот Mozilla Firefox. Иако неговата употреба е ограничена само за овој прелистувач, може да се користи на сите оперативни системи. Со помош на овој додаток, прелистувачот се дели на два дела, при што едниот го користат и администрираат родителите, додека вториот им е наменет на децата. За секое дете може да се изработи посебен профил, кој ќе овозможува активности на интернет приспособени на неговата возраст.

  На почетокот родителот задава администраторска лозинка, благодарение на која ќе може да ги прави саканите приспособувања, како и да го користи прелистувачот за своите потреби. Во

моментот кога некое од децата ќе сака да користи прелистувач, едноставно треба да си го избере својот профил, при што ќе добие сосема нова средина, преку која ќе може да сурфа низ предефинираната листа едукативни и забавни веб-сајтови, да побара посетување нови, посебно интересните сајтови со само еден клик да ги сместува во колекцијата омилени или да остава пораки до останатите членови на семејството. Можностите за пребарување се ограничени на безбедни поими. Досегашните избрани содржини кои се дел од Glubble се на англиски јазик, но вие едноставно можете да ги додавате и македонските.

Линк за преземање: https://addons.mozilla.org/EN-us/firefox/addon/glubble-fox-family

- **K9 Web Protection** е бесплатна алатка за филтрирање веб-содржини и воспоставување родителска контрола врз активностите на децата додека се на интернет. За неговата употреба потребна е лиценца, која бесплатно можете да ја добиете преку имејл доколку ја поминете постапката за регистрација.

Што можете да приспособите со K9 Web Protection?

Со ова мало парче софтвер, пред сè, можете да го одредите нивото на заштита за саканиот кориснички профил на системот, чие прекршување ќе го оневозможите со лозинка. Можете да избирате меѓу неколкуте дадени нивоа на заштита, кои вклучуваат забрана за посетување одреден тип содржини или пак листата забранети содржини да ја приспособите сами. Понатаму, можете да воспоставите периоди од денот во кои ќе го забраните користењето на прелистувачот, како и периоди во кои ќе го дозволите.

Одредени веб-сајтови можат да бидат забранети за пристап, додека други да бидат секогаш дозволени. Забраната може да се воспостави и врз основа на дадени клучни зборови, како и да се избере начин за известување и казнување доколку се направи обид за пристап до некоја од забранетите содржини.

Веројатно, една од позначајните работи што ги овозможува овој софтвер е деталниот систем за известување, преку кој можете да добиете целосно јасна слика за активностите на интернет на вашето дете.

Линк за преземање: http://www1.k9webprotection.com

- **WebFilter Pro** е додаток за прелистувачи кој овозможува едноставен начин за блокирање на содржина за возрасни, прокси сервери и различни веб-сајтови за социјално вмрежување без наметнување на временски ограничувања или други несакани санкции. Корисниците можат да блокираат се од голотија до обложување и игри. Овој додаток овозможува конфигурирање на индивидуални бели и црни листи овозможувајќи пристап до одредени веб-сајтови кои не спаѓаат во било која од многуте категории за филтрирање на овој додаток.

Линк за преземање: https://addons.mozilla.org/en-Us/firefox/addon/webfilter/ и https://chrome.google.com/webstore/detail/webfilter-pro-the-best-fi/ejgfoklefkbjadjcgjmnhfbdfjolojnn?hl=en

- **FoxFilter** е додаток дизајниран со цел да им овозможи на корисниците филтри за блокирање врз основа на индивидуални клучни зборови и веб-сајтови (на пр. Плејбој, голотија, пцовки), понудувајќи можност за додавање на веродостојни веб-сајтови во модерирана листа на содржини. Поставките на овој додаток овозможуваат скенирање и на содржината на веб-сајтот како и насловот и УРЛ-то, а корисниците можат да прилагодат известувања и предупредувања за типот на содржина врз основа на секој блокиран сајт.

Линк за преземање: https://addons.mozilla.org/en-us/firefox/addon/foxfilter/ и https://chrome.google.com/webstore/detail/foxfilter-the-content-fil/nopeodilnmhhlfageeohjojginlgeljk

- **Nanny за Google Chrome, LeechBlock за Firefox** - Како што децата растат, се чини дека некои грижи исчезнуваат. Но, менаџирањето на времето постанува поголем извор на грижи, особено за тинејџерите чии животи се повеќе почнуваат да се вртат околу социјалните интеракции, односно сајтовите за социјално вмрежување. Овие екстензии блокираат конкретни веб-сајтови во одредено време од денот со цел да се оневозможи одвлекување на вниманието и да се подобри продуктивноста. На пример, можете да го блокирате Фејсбук од пладне до 6 часот попладне.

Овие два додатоци исто така ви овозможуваат да предодредите колку време вашите деца може да поминуваат дневно на одредени веб-сајтови, што значи дека може да алоцирате час или два на одреден веб-сајт, наместо целосно да го блокирате пристапот до него.

Линк за преземање: https://chrome.google.com/webstore/detail/web-nanny/pbdfeeacmbjblfbnkgknimpgdikjhpha?hl=en и https://addons.mozilla.org/en-us/firefox/addon/leechblock/

- **TinyFilter** е екстензија за Гугл Хром која е многу едноставна и блокира пристап до одредени веб содржини врз основа на збирка од клучни зборови кои забрануваат пристап до секој веб-сајт кој ги содржи зборовите на црната листа. Оваа екстензија може да блокира веб-сајтови врз основа на посакуван УРЛ, но примарната улога е филтер на содржини врз основа на зададен клучен збор.

Линк за преземање: https://chrome.google.com/webstore/detail/tinyfilter-reliable-conte/nlfgnnlnfbpcammlnibfkplpnbbbdeli?hl=en

- **Golden Eye** е моќен софтвер за шпионирање и надгледување на сите активности на компјутер: внесување лозинки и други податоци, посетени веб-страници, користени апликации и сето тоа потврдено со слики фатени во моментот на користење. Овој софтвер чини $29,95.

Линк за преземање: http://www.monitoring-spy-software.com

- **Safe Eyes** ги обединува сите опции потребни за родителска контрола: ограничува пристап до одредени типови веб-сајтови и програми, го ограничува времето за разни активности на

интернет, чува забелешки за активностите и известува за прекршувањата на неколку начини. Лиценцата за овој софтвер чини $49,95.

Линк за преземање: http://www.internetsafety.com

- **Web Watcher** е еден од најдобрите софтвери за интернет- филтрирање, блокирање програми, временско ограничување и напредно надгледување на активностите на детето додека го користи компјутерот. Лиценцата за него чини $97.00.

Линк за преземање: http://www.webwatchernow.com

- **Cyber Patrol** е програма за родителска контрола со богат избор на опции за филтрирање, блокирање програми, менаџирање на дозволеното време и надгледување, наменета за понапредни корисници. Оваа програма може бесплатно да ја тестирате за 14 дена, а годишно чини $39.95.

Линк за преземање: http://www.cyberpatrol.com

- **Net Nanny** есофтвер за родителска контрола со филтрирачки карактеристики, можности за блокирање чет- програми и програми за делење фајлови, групи (newsgroups) и послаби можности за надгледување на активностите. Може да го тестирате 15 дена бесплатно, а годишно чини $39.99 годишно.

Линк за преземање: http://www.netnanny.com

- **Parental control bar** овозможува филтрирање на несакани веб-содржини и нуди едноставен премин од родителскиот режим заштитен со лозинка во режимот за децата.

Линк за преземање: http://www.parentalcontrolbar.org

- **KidZui** е прелистувач за деца на возраст од 3 до 12 години.На децата им овозможува доживување на мултимедијалните интернет-искуства, додека на родителите им овозможува родителска контрола.

Линк за преземање:http://www.kidzui.com

Совети за заштита на приватноста на вашите деца

Поставете неколку основни правила - Децата треба да знаат под кои услови, во кои периоди и на кој начин смеат да користат интернет. Овие услови одредете ги вие. Почнете, на пример, со тоа дека може да одат на интернет само доколку претходно си ги завршат училишните обврски.

Компјутерот на централно место - Поставете го компјутерот на централно место во собата или во училницата за да можете да погледнувате од време на време што прават вашите деца. Ова е важно за да можете да забележите доколку вашите деца случајно наидат на содржини кои не се соодветни на нивната возраст и интереси.

Поставете временско ограничување – Препорачливо е децата да не поминуваат повеќе од 1 до 2 часа пред компјутерскиот монитор на ден. За децата до 7-годишна возраст, најдобро е да прелистувате низ содржините заедно со нив, додека за постарите деца, важно е да одредите каде смеат, а каде не смеат да одат додека се на интернет, пред да почнат со активности на интернет.

Научете ги децата на безбедно и одговорно однесување на интернет

- Кажете им на вашите деца дека не смеат да ги делат своите лични податоци со непознати луѓе на интернет и потсетете ги дека треба да ги користат поставките за приватност на нивните лични страници за социјално вмрежување. Информациите што ги оставаат за себе таму, треба да бидат приватни, односно ограничени за пристап. Доволно е ваквите информации да бидат видливи само за нивните пријатели и семејството. Тие не би сакале да ги прикажат информациите кои утре можат да им застанат на патот до факултетот на кој ќе сакаат да студираат или работата што ќе сакаат да ја работат. Потсетете ги и дека не е културно да се откриваат лични податоци за нивните другари и семејството. Кога објавуваат фотографии, треба да ги прават приватни и да не им поставуваат тагови (етикети со кои се опишуваат присутните на фотографијата).
- Децата треба да запомнат дека лозинките се само за нив и да внимаваат никогаш да не ја вклучуваат опцијата за автоматско помнење на корисничкото име и лозинката кога проверуваат имејл или кога користат програми за разговор од јавен компјутер.
- Научете ги децата да не се среќаваат во живо со луѓето што ги запознале на интернет. Доколку вие се согласите вашето дете да се сретне со некој свој пријател на интернет, најдобро е да појдете со нив и средбата да се оствари на јавно место. Тинејџерите кои веројатно нема да сакаат да одат со возрасен, треба со себе да земат барем еден свој пријател.
- За децата многу е полесно да се однесуваат непристојно на интернет, отколку во живо. Кон ова придонесува можноста за користење прекари, кои ги кријат вистинските виновници за некоја лоша порака, а ваквите пораки, пак, можат лесно и брзо да се рашират до сите деца од училиштето. Оваа појава е позната под името сајбернасилство (cyberbullying).
- Едно правило до кое децата мора да се придржуваат гласи: ако некому нешто не би му кажал во лице, не му го кажувај ниту преку имејл, СМС, чет и инстант-пораки и не го поставувај на нечија страница.

- За да се заштитат самите од несакани, навредливи или заплашувачки имејл-пораки, посочете им дека можат да ја користат опцијата за филтрирање непосакуван имејл преку сервисот што им ја овозможил нивната имејл- адреса. Повеќе информации за блокирање имејл- пораки од непожелни испраќачи ќе најдете на: http://www.bezbednonainternet.org.mk/blokiranje или http://bezbednonainternet.org.mk/component/option,com_docman/task,doc_download/gid,66/Itemid,38/lang,mk/
- Научете ги децата да објавуваат содржини со одговорност. Тие треба да ги погледнуваат условите за користење на сервисите пред нешто да решат да објават со помош на нив. Исто така, доколку забележат некоја несоодветна содржина, доколку постои опција, можат да ја означат како таква за да оневозможат и други деца да наидат на неа. Ваква можност на пр. има сервисот You-Tube, кој овозможува поставување знаменца на несоодветните видеа, по што тие можат да бидат избришани.
- Потсетете ги децата дека сè што е објавено на интернет, не значи дека мора да биде точно. На содржините треба да се гледа критично, информациите треба да се проверуваат од повеќе извори, како и да се проверува авторот на текстот кој планираат да го земат како основа за својот училиштен проект или за некоја своја лична активност. Научете ги како да разликуваат веродостојна од неверодостојна содржина и потсетете ги дека копирањето текстови од некој веб-сајт може да претставува плагијат.
- Согласно бон-тон правилата, може да биде добра идеја рутински да ја проверувате историјата на компјутерот и телефонот на вашите деца како и да побарате да Ви ги кажат сите лозинки за сите профили... Но, имајте на ум дека кршењето на правото на приватност може само повеќе да го оддалечи Вашето дете од Вас.
- Верувајте му на Вашето дете доволно и не ја нарушувајте неговата/нејзината приватност без оправдана причина.
- Воспоставете граници, правила и насоки на однесување кои се дозволени на социјалните медиуми, како и времетое кое смеат да го поминат на социјалните медиуми. Психолозите предупредуваат дека тинејџерите со паметни телефони/уреди имаат тенденција да бидат повеќе заинтересирани за сајбер светот и несвесни за реалниот свет околу нив, но како родител можете да поставите правила за да се спречи тоа.
- Постојано информирајте се за можните закани на интернет. Опасностите на интернет се многу повеќе од само интернет предатори или кражба на идентитет. Всушност, тинејџерите не се единствените ранливи интернет корисници.
- Дури и родителите може да направат грешки на социјалните медиуми!!! Никогаш не го најавувате претстојниот одмор, и почекајте додека не се вратите дома за да ги објавите фотографии од најубавата плажа ова лето!
- КОЛКУ ПОВЕЌЕ СТЕ ВКЛУЧЕНИ ВО СВЕТОТ ОНЛАЈН ТОЛКУ ПОВЕЌЕ ЌЕ ЗНАЕТЕ ЗА СВОЕТО ДЕТЕ И КАКО ДА РАЗГОВАРАТЕ СО НЕГО. ГЛАВНАТА ПОРАКА Е: БИДЕТЕ ВКЛУЧЕНИ!

Корисни ресурси

- www.privacy.mk
- www.metamorphosis.org.mk
- www.bezbednonainternetorg.mk
- www.nemrazi.mk

Прилози

Прилог 1 – Најчесто користени акроними од тинејџери

1. **143** I love you
2. **2DAY** Today
3. **4EAE** For ever and ever
4. **ADN** Any day now
5. **AFAIK** As far as I know
6. **AFK** Away from keyboard
7. **ATM** At the moment
8. **B/C** Because
9. **B4** Before
10. **BF / GF** Boyfriend / Girlfriend
11. **BFN** Bye for now
12. **BOL** Be on later
13. **BRB** Be right back
14. **BTW** By the way
15. **DM** Direct message
16. **DWBH** Don't worry, be happy
17. **F2F or FTF** Face to face
18. **FB** Facebook
19. **FF** Follow Friday
20. **FTL** For the loss / For the lose
21. **FTW** For the win
22. **FWB** Friends with benefits
23. **FWIW** For what it's worth
24. **FYEO** For your eyes only
25. **FYI** For your information
26. **GLHF** Good luck, have fun
27. **GR8** Great
28. **HAK** Hugs and kisses
29. **HAND** Have a nice day

30. **HT or H/T** Hat tip or heard through
31. **HTH** Hope this helps / Happy to help
32. **IANAL** I am not a lawyer
33. **IDK** I don't know
34. **IIRC** If I remember correctly
35. **IKR** I know, right?
36. **ILY / ILU** I love you
37. **IMHO** In my honest opinion / In my humble opinion
38. **IMO** In my opinion
39. **IRL** In real life
40. **IU2U** It's up to you
41. **IYKWIM** If you know what I mean
42. **J/K** Just kidding
43. **J4F** Just for fun
44. **JIC** Just in case
45. **JSYK** Just so you know
46. **K or KK** Okay
47. **LMBO** Laughing my butt off
48. **LMK** Let me know
49. **LOL** Laughing out loud
50. **MM** Music Monday
51. **MSM** Mainstream media
52. **NAGI** Not a good idea
53. **NM** Never mind
54. **NMU** Not much, you?
55. **NP** No problem or Now playing
56. **NSFW** Not safe for work
57. **NSFL** Not safe for life
58. **NTS** Note to self
59. **OH** Overheard
60. **OMG** Oh my God
61. **ORLY** Oh, really?

62. **PAW** Parents are watching
63. **PLS or PLZ** Please
64. **PPL** People
65. **PTB** Please text back
66. **QQ** Crying.
67. **RAK** Random act of kindness
68. **RL** Real life
69. **ROFL** Rolling on the floor laughing
70. **RT** Retweet
71. **RUOK** Are you okay?
72. **SMH** Shaking my head
73. **SRSLY** Seriously
74. **SSDD** Same stuff, different day
75. **SWAK** Sealed with a kiss
76. **SWYP** So, what's your problem?
77. **TIA** Thanks in advance
78. **TIME** Tears in my eyes
79. **TMB** Tweet me back
80. **TMI** Too much information
81. **TMRW** Tomorrow
82. **TTYL** Talk to you later
83. **TY or TU** Thank you
84. **VSF** Very sad face
85. **WB** Welcome back
86. **WTH** What the heck?
87. **WTPA** Where the party at?
88. **WYCM** Will you call me?
89. **YGM** You've got mail
90. **YMMV** Your mileage may vary
91. **YW** You're welcome
92. **OMG** Oh my god

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.738-053.2:004.738.5(036)

ПЕЦОВА Илиеска, Лилјана
Водич за родители за заштита на приватноста и личните податоци на децата на интернет / [водичот го изработиле Лилјана Пецова Илиеска, Тамара Ресавска]. - Скопје : Метаморфозис : Дирекција за заштита на лични податоци, 2015. - 34 стр. : илустр. ; 28 см

Фусноти кон текстот

ISBN 978-608-4564-54-6 (метамор.)
ISBN 978-608-4682-22-6 (Дирекција)
1. Ресавска, Тамара [автор]. - I. Илиеска, Лилјана Пецова види Пецова Илиеска, Лилјана
а) Деца - Заштита на лични податоци - Интернет - Водичи
COBISS.MK-ID 98897674