ОБУЧИТЕЛНО ПОСОБИЕ
ЗА РОДИТЕЛИ И УЧИТЕЛИ

за безопасно използване на интернет от деца до 16 години

София
2006

Съставителство и редакция:
Богомил Николов
Елена Златева

ISBN - 10: 954-91548-5-8
ISBN - 13: 978-954-91548-5-6

Издава се с финансовата подкрепа на Програма СОКРАТЕС
Грюнвдиг 2 на Европейския съюз

Разпространява се безплатно!

СЪДЪРЖАНИЕ:

I. Обхват на проблема

В последните години се наблюдава голямо увеличение на броя хора с достъп и използващи интернет. Децата и младежите са една от най-бързо растящите групи от интернет потребители. Поради използването на съвременни информационни технологии, младото поколение се смята за най-информираното поколение в цялата човешка история. Младите потребители не питат- те просто знаят всичко за желаният продукт или услуга. От една страна това е панацея за потребителската защита и универсално средство за информиране. От друга страна все повече и повече деца използват информационни технологии. В наши дни е нормално да се види 5 годишно дете, разглеждащо интернет страници, а очакванията са, че тази тенденция ще продължи. Проблема за детската интернет виктимизация и нейната превенция се очертават като основна необходимост в процеса на изграждане на информационното общество. Изключително важно е родителите, изпълнителната и законодателната власт, прокурорите и службите оказващи подкрепа на жертвите да знаят колкото се може повече за интернет престъпленията срещу деца, за да могат да действат адекватно и да предпазят децата от интернет виктимизация и измами.

Полша

В Полша, както и в другите страни, нивото на познаване от страна на хората на рисковете произтичащи от интернет е ниско. Всяка инициатива- ако изобщо съществува такава, не е достатъчно популярна за да предостави безпрепятствен достъп на възрастните до нея.

По време на конференция Центъра за изследване на общественото мнение (СВОР) представи резултатите от едно от своите изследвания- "Младежи и интернет - употреба и рискове". Тези резултати разтревожиха обществеността:

- В 50% от домакинствата, където живеят деца и младежи, младите хора използват интернет, докато само 26% от възрастните го правят
- Сред децата интересът към интернет расте с възрастта
- Повечето подрастващи редовно използват интернет
- Най-често децата използват интернет в училище (76%), вкъщи (50%) или в дома на приятел (34%)
- Основната причина за използването на интернет и подготвянето на домашно или търсенето на интересна информация по всякакви теми (79%)
- В повече от 50% от домакинствата, когато децата използват интернет те го правят за да участват във виртуални игри, за да слушат музика или за да изпращат електронни писма (около 50%)
- По мнение на 38% на анкетираните възрасти, те са напълно наясно за причината, поради която техните деца използват интернет, 45% по-скоро знаят. 1/5 от участвалите в проучването възрастни не знаят, за какво децата им използват интернет. Нивото на ориентираност на родителите зависи от възрастта на децата

Резултатите представят общото мнение на полските родители. Дори и тяхната информираност, относно употребата на интернет от техните деца да не е малка, повечето се страхуват от рисковете и опасностите свързани с интернет

- На първо място – сексуални рискове (42%)
- Загуба на контрол, непознаване на приятелите на детето в интернет
- Агресивно, вулгарно, расистко съдържание, както и съдържание представящо насилие.
- Измами, загуба на време, рискове за здравето.

Ако искаме добре да пазим децата, от рисковете произтичащи от интернет, ние трябва да кандидатстваме за образователни програми за възрасти. Използването на интернет трябва да е съвестно и безопасно.

Литва

Литва има най-нисък процент интернет потребители от балтийските републики- до средата на 2002 21% от населението използват интернет. Въпреки това общият брой на домашни компютри се удвоява на всеки три години. В настоящия момент в Литва има 28,2% проникване на интернет и 968 000 интернет потребители.

Изследване на TNS Gallup показва, че интернет се използва от 63% от литовските деца и тийнейджъри. 43% от тях са на възраст между 11 и 14 г. Една трета от децата започват да използват интернет на възраст между 7 и десет години, а 5% на по-малко от 7 г.

Изследването също така показва и че, въпреки че родителите знаят малко относно интернет безопасността, те осъзнават важността на проблема.

Правителството е стартирало няколко програми, касаещи нуждата от комуникационни технологии и компютърна грамотност сред населението. През май 2000 г. отделът по информация и информатика, създаде стратегия за развитие на литовското информационно общество и очерта насоките за няколко години напред.

В Литва, както и в останалата част на света, все повече хора използват мобилни услуги и интернет. По време на присъединяването на Литва в Европейския съюз като пълноправен член, е важно населението на Литва, и в частност децата, да бъдат защитени от вредното съдържание в интернет. Независимо някои правни усилия, Литва трябва все още да създаде успешни определения за това. Единствената гореща линия в Литва третираща този въпрос е осигурена от полицията и между март 2003 и март 2004 е получила само едно обаждане!

Центъра за социални и психологически услуги, Министерство на образованието и науката на Република Литва и BITE GSM (вторият по големина мобилен оператор в Литва, който е I основен доставчик на интернет в страната), са много солидни и имат обширен опит в

работата си заедно в областта на развиването на информационен център за дигитална безопасност за Литва.

Има и втори, новосъздаден информационен център в Литва, наречен "draugiskas Internetas". Програмата се осъществява от трима партньори: Телекомуникационната компания Bite Lietuva, Министерството на образованието и науката и Центъра за социални и психологически услуги. Широк кръг от правителствени органи и неправителствени организации, също изразиха подкрепата си и желанието си за сътрудничество.

България

Следните интересни факти, бяха изнесени по време на изследване, осъществено от Националния център за изследване на общественото мнение, проведено сред български учители, родители и деца:

Преглед

Българските деца използват интернет за забавление (50%), информация (38%), и общуване (38). Докато са онлайн те използват електронна поща, чат канали, форуми, интернет страници и програми за сваляне на информация от интернет.

Оценка на родителите и учителите

- От една страна повечето от родителите (68%) и учителите (66%) оценяват високо важността на интернет за техните деца. От друга страна, 70% от родителите не използват интернет или използват интернет рядко.
- Около 40% от родителите и 50% от учителите в България са запознати с потенциалния риск за децата, свързан с попадането на неподходящо интернет съдържани.
- Само 12% от родителите и 10% от учителите са наясно с потенциалният риск, свързан с интернет натрапниците.
- Над 30 % от родителите и 40 % от учителите не свързват интернет с каквито и да е рискове.

Проблеми на безопасността

- Между 40% и 60% от децата, използващи интернет са попадали на неподходящо съдържание- насилие, сексуално ориентирано съдържание, или са превръщани в жертви на сексуални натрапници.
- При 74% от българската младеж липсва осъзнаване на рисковете, свързани с интернет.

- Между 64% и 96% от българските деца не разпространяват лична информация в мрежата, но независимо от това 20% от тях са изпращали снимка, телефон или личен адрес на непознат чат партньор. Същият процент деца биха се срещнали със своят чат събеседник в реалния живот.
- 25% от децата не биха споделили с родителите или учителите си неприятното изживяване по време на пребиваване в интернет.

Грамотност и отговорности

- 50% от българските родители идентифицират учителите, като най-подходящи интернет обучители, и същият процент учители желаят да върнат това обучение вкъщи. Децата (41%) смятат, че тази подготовка и образование трябва да са част от училищния процес.
- 22% от децата смятат, че учителите са достатъчно квалифицирани за да осъществяват такава подготовка
- 36% от родителите и 31% от учителите не желаят да налагат никакви ограничения на децата, по време на престоя им в интернет.
- 66% от родителите мислят, че е по-безопасно да се използва интернет вкъщи, но 86% от тях не следят децата си.

Гореспоменатите резултати демонстрират силен интерес и висока оценка на интернет, като средство за получаване на информация от страна на младежите. За нещастие резултатите показват и липсата на осъзнаване на необходимостта от интернет безопасност от страна и на родители и на учители. Тези изводи водят до следващият знаков проблема за интернет безопасността в България: локализиране на филтърния софтуер; информационна кампания за родители и учители.

II. Как можете да обясните на детето си рисковете от интернет, ако самите вие никога не сте го използвали?

Не е нужно да сте компютърен гений за да обясните на децата си рисковете от. Единственото, което трябва да направите е да вземете правилата, на които ги учите всеки ден и да ги приложите за интернет. Съществуват няколко основни правила, на които трябва да наблегнете:

- Не разговаряй с непознати и не приемай подаръци.
- Прибирай се направо вкъщи.
- Искам да познавам приятелите ти
- Не давай на хората лична информация за теб, твоето семейство или приятелите ти.
- Не бъди груб с хората.
- Не взимай нищо което не е твое.

Да видим сега как всичко това звучи приложено за интернет

Не разговаряй с непознати и не приемай подаръци - трябва да научите децата си, че всеки в интернет е непознат. Без значение от колко време е тяхното виртуално приятелство, колко време прекарват в онлайн разговори или колко близки се чувстват, човекът от другата страна на линията все пак е непознат. Въпреки, че чатът или разменянето на съобщения е едно от най забавните неща, което децата и тийнейджърите могат да правят онлайн, това може да бъде и доста рисковано ако не сте ги научили, че всеки когото не познават лично е непознат и те не трябва да му споделят неща, които биха казали само на приятелите си.

Понякога за децата е много трудно да разберат това правило, защото когато чатят, особено ако го правят от домашния компютър и в присъствие на родителите си те се чувстват напълно защитени.

Механизмът на нормално подозрение към непознати, който се включва когато са навън просто не работи в този случай.
През последните години, интернет се превърна в едно от любимите места за сексуалните престъпници, защото мрежата дава високо ниво на анонимност, като в същото време създава фалшиво чувство за близост, на което те разчитат. Недоброжелателите обикновено се опитват да убедят децата, че нормалните правила не важат тук. Уверете се, че децата ви не мислят така. Също така наблегнете на факта, че не е нито нормално нито редно да получават подаръци от непознати, независимо дали искат да им ги дадат лично или да им ги изпратят вкъщи. Това може да е трик, чрез който недоброжелателят иска да се срещне с детето ви или да научи домашния ви адрес.

Прибирай се направо вкъщи - това е едно от първите правила, които научаваме от родителите си и на свой ред предаваме на децата си. То важи с пълна сила и за интернет. Ако оставите децата си да се шляят безразборно из интернет това може да им навлече неприятности. Шляенето из интернет не е много по-различно от шляенето след училище по улиците, където може да се срещнат с неподходящите хора или да се окажат на неподходящо място. Ако искате да предпазите децата си поставете лимит на времето, което могат да прекарват в интернет, след като приключат с използването му за учебни цели. Давайте им не повече от час- час и половина на ден за разглеждане на страници, чат или правене на другите неща, които обичат. Искате децата ви да се прибират веднага след училище! Уверете се, че правят същото и в интернет.

Искам да познавам приятелите ти - това е нещо, което казваме когато децата ни си имат нов приятел в истинския живот. Защо да не го прилагаме и за мрежата? Не давате на децата си да прекарват времето с хора, които не познавате- не го правете и за интернет. Трябва да познавате хората, с които детето ви комуникира и да се уверите, че приятелството им е уместно. Разберете дали човекът от другата страна е този, за който се представя и дали е от типа хора, с които бихте искали детето ви да общува. Не възможно е

да познавате всички, на които детето ви се натъква в мрежата, но поне се постарайте да познавате тези, с които се среща често и тези, които му влияят.
За това има много важна причина. Както вече споменахме, ако детето ви се запознава с нов човек на улица или в училище то е малко или много недоверчиво, но когато това се случва в дома му то се чувства защитено и забравя за предпазливостта. Има и още една огромна разлика. Ако детето ви се запознава с някого в реалния живот, то може лесно да забележи ако той е възрастен, доакто това е невъзможно онлайн. Повечето недоброжелатели в мрежата се представят за връстници на децата, с които разговарят, за да приспят подозрението им. За вас би било по-лесно да разкриете възрастният, който се крие зад маската на дете.

Не давай на хората лична информация за теб, твоето семейство или приятелите ти - повтаряйте на децата си, за да не го забравят, че те всъщност не познават човека, с който си говорят онлайн. Дайте им сравнението, че да споделят лична информация по интернет е като да четат личния си дневник на глас на улицата. Дори да си мислят, че човека с когото споделят заслужава доверието им, може да има и други, които да „подслушват" разговора им.

Ако децата ви дават лична информация по мрежата , това може да ги застраши. Поставете ясни правила по въпроса, като преди това се уверите, че децата ви разбират какво точно имате предвид под лична информация. Следете стриктно за спазването на правилата. Ако не го правят могат да застрашат себе си, както и банковата ви сметка например.

Понякога децата се объркват, защото ние ги учим да не пренебрегват хората и да не са груби с тях, а същевременно им казваме да не разговарят с непознати. Направете ясно разграничение между тези правила и обяснете, че могат да не отговарят на някои въпроси , без да обидят някого.

Не бъди груб с хората - децата са си деца и понякога се обиждат помежду си, без да мислят за последствията. На практика

това се случва толкова често, че онлайн обидите и грубите съобщения вече си имат име. Наричат се "flaming"(от английски-пламтящ, яростен), а в българското пространство човек, който изпращат такива съобщения или публикуват неприятни съобщения по форуми се нарича *трол*. Тази размяна на злобни съобщения може да се превърне в дълга и неприятна война, за всички участващи. Ако подозирате, че детето ви е част от такава война, обяснете му, че това наранява нечии чувства точно толкова, колкото и ако го правеше лице в лице. Ако установите, че детето ви е жертва на подобни атаки вземете нещата в свои ръце. Уведомете интернет доставчика си, както и човекът отговорен за реда и добрия тон на страницата, където се водят „битките".

Не взимай нищо което не е твое - днес все повече и повече деца използват интернет, при това го правят за какво ли не- от писането на домашни и събирането на информация до изработването на собствени интернет страници и сваляне на музика, филми и програми. Правейки това, през повечето време нарушават закона. Докато сърфират те си свалят неща от рода на музикални файлове или снимки, които не им принадлежат. Повечето деца, както и голяма част от родителите смятат, че ако споменеш мястото, откъдето с ги взел всичко е наред. Това не е вярно. Ваша работа е да научите децата си, че краденето на музика от интернет е толкова лошо, колкото и краденето на диск от музикален магазин, защото и в двата случая взимат нещо, което не им принадлежи. Напоследък все повече хора биват съдени за нарушаване на интелектуалното право.

III. Индикатори показващи, че детето ви може да е жертва на интернет.

Дори ако сте научили децата си на всички правила за безопасност те пак могат да бъдат изложени на риск, особено когато става въпрос за онлайн „сексуални хищници". Съществуват някои индикатори и поведенчески модели, които биха могли да ви подскажат, че детето ви контактува с някой от тях. Бъдете особено нащрек ако детето ви често изгася монитора когато влезете в стаята, прекарва дълги часове в чата, особено през нощта и води подозрителни телефонни разговори. Трябва да се отнесете още по-сериозно ако в дома ви започнат да пристигат неочаквани подаръци и детето ви отказва да сподели от кого са или изобщо отказва да споделя каквото и да е за часовете прекарани в интернет. Тогава е крайно време да инсталирате някакъв филтриращ или наблюдаващ софтуер на домашния си компютър. Информация за такъв тип софтуер можете да намерите по-нататък в тази брошура.

На помощ на родителите се притичват и психолозите, които са изработили профил на типичната жертва на сексуален тормоз. Повечето я определят като гете (обикновено момиче, но може да бъде и момче) на възраст между 12 и 15 години. Те или се бунтуват срещу родителите си в опит да извоюват своята независимост или пък са все още много незрели и наивни. Обикновено жертвите са необщителни и нямат много приятели в истинския живот. Те отчаяно искат да бъдат оценени и търсят любов и внимание (особено тези, които идват от разбити семейства). Повечето пъти жертвите не осъзнават, че разговарят с възрастен. По тази причина когато бъдат подготвени психически за този факт от страна на сексуалните хищници, когато истината излезе наяве, момичетата си мислят, че са влюбени в този човек независимо от всичко. Когато говорим за момчета, най-често също биват подлъгани по един или друг начин, но в някои случаи те самите искат да изпитат хомосексуално преживяване.

Сега нека обърнем внимание на всички предупредителни знаци и да видим какво ни говорят те.

1. **На детето ви му липсват приятели**. Това може да означава, че то използва интернет дюза да намери любов и разбиране, които му липсват в истинския живот. Често това се дължи ниско самочувствие, в следствие на външния вид. В интернет ти нямаш лице и можеш да бъдеш този, който искаш.

2. **Детето ви е на възраст между 12 и 15 години**.
Оказва се, че децата на тази възраст са предпочитани жертви за онлайн сексуалните престъпници. След шестнадесетгодишна възраст рискът от „сексуални хищници" за вашето дете започва бавно да намалява, защото то започва да се държи повече като възрастен, развива по-критично мислене, в следствие на което става по-малко привлекателно за тях. Това обаче не означава, че ако детето ви е на 16 можете спокойно да пренебрегнете този риск.

3. **Детето ви прекарва повече от 1-1.5 часа в интернет забавлявайки се**. Някои психолози твърдят, че времето прекарвано от детето ви в интернет е правопропорционално на склонността му да се занимава с рискови дейности в интернет. Трябва да бъдете особено внимателни, ако детето ви попада в тази група и вече му разрешавате да ходи на различни места без да е придружено от възрастен.

4. **Детето ви е прекалено обгрижвано и наивно, или пък точно обратното- склонно е да поема рискове и да ви провокира**. Това са двете категории, които са най рискови от гледна точка на сексуалните престъпления. Първата категория деца лесно падат в капана на недоброжелателя, защото той лесно спечелва доверието им с обещания за приятелство или любов. Втората категория е застрашена поради бунтарския си дух и желание да се докажат като възрастни.

5. **Детето ви крие от вас какво точно прави в интернет**. Вие лесно можете да се досетите ако това се случва. Ако монитора или направо целия компютър често биват изгасяни, когато влезете в

стаята; ако не споделя нищо за интернет приятелите си; ако в дома ви започнат да пристигат странни подаръци или детето ви води подозрителни разговори с хора, които вие не познавате това е сигурен знак, че става нещо нередно.

Накарайте детето си да ви покаже списъка с онлайн приятелите си и прегледайте всички имена. Уверете се, че детето ви наистина знае кои са тези хора.

Ако детето ви има личен профил в интернет вижте го и проверете дали той не съдържа неуместна или прекалено лична информация.

6. **Детето ви напоследък се е отдръпнало от старите си приятели, променило е поведението си и има нови приятели, за които вие не знаете нищо.** Това може да е индикатор, че се случва нещо важно и дори да не е касае за „онлайн сексуален хищник" най-вероятно все пак става въпрос за нещо сериозно, което заслужава вашето внимание.

IV. Обучителен план

1. Кратко представяне на компютърните и интернет технологии

Интернет

В общия смисъл, **интернет** (с малко *и*) е компютърна мрежа, която свързва няколко мрежи. Интернет е съкращение от интернетуърк, или буквално преведено на български — междумрежа. Като съществително собствено име, Интернетът е обществено-достъпна международно свързана система от компютри (заедно с информацията и услугите, които те предлагат на потребителите), която използва протоколния стек (Transfer Control Protocol) TCP/IP. Така че, най-големият интернет е просто наричан Интернет. Процесът на свързване на мрежи по този начин е известен като *internetworking*.

World Wide Web (WWW)

WWW е хипертекстова система за представяне на мултимедийна информация от влизащи в състава на Интернет компютри, наричани мрежови сървъри (уебсървъри, web servers). Под мултимедийна информация се разбира съвкупност от текст, графични изображения, видеоклипове, звукозапис и анимация. В това отношение, това е най-добрата услуга в Интернет.

Началото на WWW е поставено в Швейцария през 1989 г. в института CERN за ядрени изследвания, от Тим Бърнърс-Лий, който предлага идеята за разпределената хипермедия. Днес той е ръководител на консорциума W3C (Word Wide Web Consortium), който поставя различни стандарти за WWW.

Информацията във WWW се представя чрез хипертекстови документи, наречени *уебстраници* (или просто *страници*, *webpages*),

всяка от които се намира на сървър някъде в Интернет и се открива от клиента чрез URL — електронния адрес на страницата.

Уебсайт

Уебсайт (или просто *сайт*, *website*) се нарича съвкупност от страници за дадено лице или организация, които обикновено са разположени на един мрежов сървър (уебсървър).

Уебстраниците (често погрешно наричани "интернет страници") се разглеждат чрез уеббраузър програма (накратко *браузър*, *browser*). Браузърите се свързват и обменят информация с уеб сървърите по специфични протоколи. Кой е конкретният протокол може да се разбере по началото на мрежовия адрес:

Уеббраузър

Уеббраузър, за кратко **браузър**, (*Web browser*) се нарича компютърна програма, която се използва за възпроизвеждане на документи с хипермедия и уеб навигация — процес на придвижване от един хипертекст към друг, обикновено следвайки линковете (*електронните връзки между части от един и същ или различни хипертекстове*). Казано с простички думи това е компютърната програма, която се използва за да отваряне и разглеждане на интернет страниците.

Известни браузъри са Internet Explorer, Mozilla Firefox, Opera, Safari (под Mac OS), Slim Browser. Към 2005 г. най-популярен, ползван и известен е Internet Explorer. Напоследък нараства популярността и на други браузъри (напр. Mozilla Firefox), поради множеството подобрения, нововъведения и рационализации, включително в бързината, удобството и особено сигурността и неприкосновеността на потребителите в сравнение с Internet Explorer.

Интернет търсачка

Интернет търсачка или просто търсачка е програма, проектирана да открива желаната информация , намираща се в локална мрежа или в интернет. Тази програма дава възможност да си извършва търсене по зададени от потребителя критерии , които обикновено представляват дума или фраза. Като резултат търсачката предоставя списък от файлове или интернет страници, които съдържат зададените фрази или дума. За бързата и ефикасна работа на търсачките се използват индекси (ключови думи прикрепени към интернет страницата. Някои търсачки са в състояние да индексират и информация намираща се във форуми, големи бази данни или отворени директории.

Някои от най- известните търсачки са www.google.com, www.yahoo.com и MSN Search

IRC

IRC е съкращение от *Internet Relay Chat*. Това е услуга в Интернет, която предлага възможността за общуване в реално време с хора от цял свят. За услугата е характерно, че от самото начало е създадена за комуникация на много хора едновременно помежду си (т.нар. "*много-към-много*", от англ. *many-to-many*), за разлика от други подобни услуги като ICQ, MSN Messenger или най-обикновен телефон, които се използват главно за общуване между двама човека ("*един-към-един*", от англ. *one-to-one*). Естествено IRC също предлага възможност за обмен на съобщения само между двама човека, но това не е силата му. И тук, както при споменатите услуги, това, което напишете или кажете, се изпраща веднага на човека срещу Вас.

Всеки потребител в IRC има уникален "псевдоним", наречен още *ник* (от англиийски *nick(name)* - прякор, псевдоним), който го разграничава от другите потребители и го определя еднозначно. В IRC можете да водите *лични* (*private*) разговори (гореспоменатите един-към-един), както и да разговаряте с повече от един потребители

в т.нар. *канали* (*channels*), наричани още *чатстаи* (*chat rooms*). Имената на всички канали в IRC започват със знака "#" (диез), и по този начин се различават от никовете на потребителите.

IRC е създаден във Финландия от Ярко Ойкаринен (Jarkko Oikarinen, ник WiZ) през 1988 г. В същността си представлява мрежа (network) от един или повече сървъра (servers), които са свързани един с друг (естествено една мрежа може да се състои и само от един единичен сървър, който не е свързан с други такива). Всяка IRC мрежа е отделен "свят", т.е. когато се свържете с някоя IRC мрежа, виждате само това, което става в нея и можете да говорите само с други хора от същата мрежа. В две различни мрежи може да има канали с еднакви имена и хора с еднакви никове, които нямат нищо общо по между си, не се виждат взаимно и не могат да разговарят един с друг. Това отново е основна разлика от други услуги за онлайн комуникация като ICQ, Skype или пък Yahoo Messenger, при които *абсолютно* всички потребители се регистрират на едно и също централно място и няма различни мрежи.

Блог

Блогът (съкратено от английското *weblog*) е вид уебсайт, където се пише, както в дневник, а новите попълнения са в обратен хронологичен ред. Блоговете често предлагат коментари или новини за определена тема, като храна, политика или местни новини; други служат като лични дневници. Типичният блог съдържа текстова част, снимки или рисунки, връзки с други блогове и уебсайтове, които по някакъв начин са обвързани с общата тематика на блога. Като цяло този вид уебсайтове наблягат главно върху текста, но има и такива, които наблягат върху фотографията, аудио или видео файлове. В английския език думата *blog* се използва и като глагол, когато се прави ново попълнение.

Има няколко типа блогове, които са разделени главно според основната тема, дискутирана в тях:

- ***Личните дневници*** са най-често срещаните и имат свойствата на обикновените дневници- попълващият ги описва събития от деня,

мисли и вълнения. Публикуват се лични снимки. Нерядко са добавени и връзки с други сайтове, на които е попаднал собственикът на блога.

- *Тематичните дневници* играят роля на „любителски вестници“. Авторът им споделя мнение във връзка със събития, които са свързани с основната тема на блога (като НЛО или войната в Ирак). Публикува се информация от други сайтове, като се посочва от къде идва тя (най-вече чрез връзки).

Интернет телефония

VoIP ("Войп" от Voice over Internet Protocol или Глас чрез Интернет протокол) е технология, която позволява провеждането на разговори на далечно разтояние (телефония) благодарение на инфраструктурата на Интернет. Терминът може да се отнася до връзка между два компютъра, два телефонни апарата, или компютър и телефонен апарат, стига сигналът да се пренася в част от пътя си чрез IP пакети.

Преимущества

Телефония през Интернет има две първостепенни преимущества, работещи за потребителите.

• **Намалението на цената на телефонните разговори** при голямо разстояние. Използвайки безплатен софтуер (DIALPAD, Skype, ICQ) цената се свежда само до разход към местния Интернет доставчик. Като по този начин се елиминират месечните такси и задължения за минута разговор към PSTN. За PSTN компаниите, употребата на телефония през Интернет също съкращава разходите на големи разстояния през международната телефонна мрежа. Ползата на големите компании от доставчици на услуга за телефония (ITSP) е, че спестяванията им става все по-големи с увеличаване обема на повикванията. Инвестицията за закупуване на Voice Gateway, за да свърже PSTN с Интернет е висока. Но технологично развитие води към системно падане на цените на качествения хардуер. И това ,че инвестицията е еднократна.

• **Мулти функционалност на линията за свръзка на потребителя**. Много хора днес все още използуват модем за да се свързват с

Интернет и голяма част от тях имат само една телефонна линия. Така те нямат възможност да бъдат едновременно и Online и да провеждат разговор по телефона по едно и същото време. Постигнатото при DSL технологията решение е в полза скъпо струващите разговори през PSTN или пък нуждата от две телефонни линии осигурявани от ISDN технологията работеща отново за обществения телеком.Така VoIP решенията задоволяват изискванията на потребителите за многоцелево ползване на наличните линии за свръзка.

2. Общо описание на интернет генерираните рискове

В интернет има няколко основни риска за детето ви. Интернет е огромно пространство, в което се съдържа огромно количество информация, като разбира се не цялата е подходяща за вашето дете. Съществуват порнографски и сайтове за залагания, както и такива който пропагандират анорексия или обезобразяване на тялото.

Съществуват и множество сайтове, които предлагат цигари, алкохол и дори наркотици. В случай, че детето ви има достъп до кредитната ви карта, кой знае какво може да се случи.

Без да го съзнава, детето ви може да предостави важна лична или финансова информация на грешния човек или фирма. Децата имат склонност към участие в онлайн конкурси и игри. Ако искаш да се регистрираш за участие обаче, често се налага да попълваш регистрационни форми, които включват повече или по-малко лична информация. Това е техника, използвана от някои недобросъвестни търговци, които могат да задръстят пощата ви със спам ли да използват предоставената им информация, по начин различен от обявения.

Детето ви може да бъде тормозени от други деца (така нареченият „кибер тормоз"). То може да бъде атакувано чрез електронни писма, стаи за разговор, форуми и дори, чрез интернет страници създадени специално за целта.

В интернет детето ви, както и вие може да се натъкнете на фалшиви интернет страници, замаскирани като електронни магазини, страници на банка или пък такива предлагащи ви съблазнителна бърза печалба. Тези страници са програмирани по такъв начин, че след като въведете в тях банковите си данни или данните за кредитната си карта те биват изпращани (без вашето знание разбира се) на създателя на интернет страницата, който от своя страна може да ги използва както намери за добре- най-често за изпразването на банковата ви сметка.

И едно от най опасните и плашещи неща- детето ви може да е мишена на онлайн хищник, който се опитва за пренесе виртуалното „приятелство” с вашето дете в истинския живот.

Преди да се паникьосате и да забраните на децата си завинаги да използват интернет, вгледайте се в рисковете отблизо. Сега може да видите, че повечето от тях могат да бъдат предотвратени като просто научите децата си за тях. Ако успеете да развиете у децата си критично мислене и отговорно отношение към личните и финансовите ви данни, вие значително намалявате риска. Не можете да ги предпазите само от възможността да се натъкнат на сексуален престъпник в мрежата, но дори тогава те са истински застрашени само ако пренебрегнат правилата за контакти с непознати и споделяне на лична информация, което може да помогне на недоброжелателя да ги открие извън интернет.

3. Преобладаващи, възрастово специфични рискове, произтичащи от интернет

В този раздел ще разгледаме най-често срещаните рискове за вашето дете, в зависимост от неговата възраст и на какво се дължи това.

a) До 7 години

В днешно време могат да се видят дори 4-5 годишни деца, които сърфират из интернет. Тези деца обикновен все още не могат да четат или пишат така, че без да го съзнават могат да отворят неподходящо за тях интернет съдържание, дори ако това е обозначено преди отварянето на страницата. Въпреки, че те не са заплашени от онлайн „сексуални хищници" (защото не могат да пишат и съответно не биха могли да комуникират чрез чат) и не биха могли да предоставят лична или финансова информация, все пак не е препоръчително да ги оставяте да посещават интернет без надзор, докато не се научат да четат и пишат. Преди това те нямат възможността да различат подходящото от не подходящото съдържание преди да са видели картинка или снимка на даден сайт, а тогава вече е прекалено късно.

b) 7-10 години

На тези възраст децата вече могат да четат и пишат, което не означава, че го правят много добре. По тази причина те са заплашени от попадане на неподходящи интернет страници без да го съзнават , дори повече от преди. При неправилното написване на дадена дума в интернет търсачка, като yahoo или google например, те могат да получат списък с интернет сайтове, съдържащи информация много по-различна от търсената. Същото може да се случи и ако директно напишат адреса на дадена страница. Много често има интернет адреси, които се различават само по една буква в адреса си, но имат коренно различно съдържание.

За съжаление на тази възраст риска на децата ви нараства и поради факта, че те вече са способни да попълват онлайн регистрационни

форми, чрез които биха могли да предоставят лична информация, или директно да я споделят с някой , когото са срещнали в чат стаите например.
Риска от онлайн „хищници" при тази възрастова група нараства, но все още не е достигнал максимума си, защото повечето деца под 10 години все още често са придружавани от възрастни когато са навън , а онлайн педофилите знаят това.

c) 11-15 години

Според експертите, на тази възраст е най-вероятно детето ви да стане мишена за сексуален престъпник. Обикновено педофилите се целят в две категории деца. Първата група са несамостоятелни и наивни деца, които лесно вярват на всяка дума на онлайн престъпника. Другата група включва деца с противоположен характер. Там влизат деца, които са агресивни и склонни да поемат рискове в търсене на своята независимост и зрялост.

Педофилите предпочитат деца на тази възраст, защото от една страна те все още не разсъждават като възрастни, а от друга вече имат свободата да посещават приятелите си и места, като лунапарк например, без възрастен придружител. Освен това, децата на тази възраст не са особено предпазливи и са склонни да споделят лична информация, особено ако си мислят, че от другата срана е някой на тяхната възраст.

d) 16-18 години

На тази възраст децата порастват и мисленето им прилича повече на това на възрастен. Поради тази причина риска от сексуални престъпници намалява, но те пък са по освободени по отношение на споделянето на лична информация и предоставянето на банкови данни, до които те вероятно вече имат достъп. Ако детето ви е в тази възрастова група не би било излишно ако внимателно следите банковите си извлечения и движението по кредитната ви карта. Детето ви може да се изкуши да поръчва скъпи продукти по интернет. Другия вариант е да бъде измамено, като попадне на фалшива интернет страница, която е маскирана като банков портал

или електронен магазин и несъзнателно да предостави финансова информация на неподходящите хора или пък да поръча прдук, за който да плати, но той така и да не пристигне.

Друга важна група от рискове включва интернет страници, които пропагандират обезобразяване на тялото, расизъм или анорексия, както и наличието на информация за приготвянето на експлозиви например.

4. Подробно описание на рисковете от интернет и начините за справяне с тях.

а) Педофилия (чат стаи и програми, форуми и т.н.)

Онлайн стаи за разговор - да започнем с това, какво представляват тези стаи. Според американски речник на разговорните думи това е виртуално пространство, където интернет потребителите могат да разговарят онлайн в реално време, посредством клавиатура, а напоследък и чрез слушалки и/или компютърна камера.

За хора които не са посещавали такива места, това може да не изглежда особено обезпокоително, но и тук както в реалния живот контактите с непознати крият редица рискове.

Като за начало трябва да сте наясно, че при контактите си с други потребители в стаите за разговори, детето ви може да попадне на недобронамерен посетител. Интернет пространството, предоставя висока степен на анонимност, като по този начин позволява на зрял мъж например, да се предоставя за връстник на детето ви, целейки да спечели доверието му. Веднъж установил контакт, недоброжелателят (много често педофил) се опитва да предразположи детето, като показва разбиране към проблемите и споделя неговите интереси. Педофилите обикновено се целят в деца, които по време на разговора в чата показват склонност към съгласяване и са по-пасивни при общуването. Това са характеристики на така наречените аусайдери, които са изолирани от връстниците си и нямат много приятели. Както в реалната среда, така и във виртуалното пространство този тип подрастващи са по-уязвими поради отчаяната си нужда от внимание.

След като известно време контактуват само във виртуалното пространство, често се преминава и към общуване чрез електронни писма или SMS-и, а не рядко се стига и до телефонни обаждания. Това помага на недоброжелателят да добие допълнителна смелост, като му показва, че е успял да накара детето да му има доверие и да

се чувства комфортно при общуването си с него. Следващата фаза е детето да бъде подготвено за факта, че новият му „приятел" евентуално не е на такава възраст, на каквато е споделил в началото. Обикновено се започва с въпроси, като „Какво мислиш за по-големите братя?" или „Как би ти харесало да имаш по-възрастен приятел, който да ти помага". По този начин измамникът се опитва да изтъкне позитивните страни от общуването с по-възрастни, като отклонява детето от евентуалните рискове, които то може да носи. Ако детето в крайна сметка се изплаши, нещата спират дотук. Това обикновено не тревожи интернет прелъстителите, защото те най-често обработват едновременно няколко деца, за да увеличат шансовете си за реална среща. Ако набелязаната жертва обаче не се изплаши от факта, че в крайна сметка срещу нея стои възрастен, следва покана за реална среща или искане за размяна на адреси. Когато се стигне до този момент, на малолетните често бива обяснявано, че не бива да казва на родителите или приятелите си, защото те не го/я разбират или не биха искали той/тя да има истински приятели (особено ако детето е уязвимо и има домашни проблеми, за които педофилът вече знае). Нерядко се стига дори до обяснения как да изтрие архива от разговорите им и писмата в интернет. Това намалява възможността на родителите да контролират виртуалните контакти на децата си практически до нула и възможността да разберат, че нещо нередно се случва е минимална.

Най-уязвими за подобен вид рискове са тийнейджърите. Това се дължи на няколко причини. От една страна те са по-склонни да се бунтуват, да търсят самостоятелност и да предприемат рисковани действия с цел доказване на себе си и своята независимост от родителите. От друга страна те имат по-голяма свобода на излизане от по-малките деца и лесно биха могли да осъществят среща с някого, без родителите им да разберат.

Съществува и друг вариант, при който педофилът не иска да се среща лице в лице с жертвата, а се опитва да я убеди да му изпраща лични снимки, изпраща й нецензурни съобщения с открито

сексуално съдържание или се старае да я въвлече във виртуален секс.

Когато говорим за опасностите от стаите за разговор и в частност за педофилията, извършителите на престъпленията са основно мъже. Въпреки това в световната практика вече има документирани случаи на склоняване към проституция или сексуални посегателства върху малолетни или непълнолетни извършвани и от жени. Независимо от пола на извършителя обаче, последствията от престъплението са еднакво нежелани. За това е добре преди да пуснете детето си свободно да се потопи в интернет, да помислите, какво може да бъде направено за да гарантирате неговата безопасност

Преди да позволите на детето си да посещава чат канали, първо трябва да се уверите, че сте направили всичко необходимо за да го защитите. Погрижете се да го научите, че както в истинския живот и тук съществуват опасности.

Трябва ясно да обясните, че не всичко което вижда в интернет е такова каквото изглежда и не всеки, който среща в интернет е този, за които се представя.

Още в самото начало разяснете, че детето ви не бива да дава електронния си адрес, снимка, данни за кредитна карта или каквато и да е друга лична информация на някой, който познава само от интернет, независимо колко дълго е продължили виртуалното им приятелство.

След това трябва да поставите ясни правила за посещаване на чат каналите и интернет като цяло. Би било добре да направите график на точните дни от седмицата и часовете, в които на вашето дете е позволено да влиза в интернет.

Най-подходящо е да изберете такива дни и часове, в които обикновено сте си вкъщи, за да можете да наблюдавате детето си докато е в стаите за разговор. Бъдете нащрек, но не прекалено натрапчиви, защото е важно да се ползвате с доверието на вашето дете. Ако започнете да проверявате детето прекалено често, то може

да почувства, че отнемате от личната му свобода и да започне да крие неща от вас.

Най-добре е да сте някъде наблизо, но не прекалено. Ако постъпите по този начин детето ви ще ви има доверие и ще сподели с вас ако се случи нещо нередно.

Ако не искате да накарате детето ви да се крие от вас, трябва да му обясните, че то няма вина за неприятните неща, които понякога се случват в чат каналите. Ако нещо такова се случи опитайте се да успокоите детето и да оправите проблема вместо да се вбесявате. Ако някои изпраща на детето ви груби или сексуални съобщения, просто блокирайте потребителя, чрез опцията „игнорирай", която всеки чат канал би трябвало да притежава. И запомнете- не се вбесявайте. Ако веднъж накажете детето си за нещо, което не е негова вина то никога повече няма да дойде при вас и да сподели, когато е несигурно или уплашено от нещо, което се е случило в интернет.

Друго нещо, което може да направите, за да гарантирате безопасността на вашето дете е да проверите стаите за разговор, които то посещава. Въпреки, че не можете да бъдете сигурни, че те са безопасни, поне се уверете, че са за деца.

И накрая - ако искате да накарате детето си да гледа сериозно на правилата за интернет безопасност, ясно посочете последствията за нарушаването на всяко правило и винаги ги спазвайте. За да са по ясни нещата може да направите нещо като договор за ползване на интернет, който Вие и вашето дете да поспишете. В него може да включите правата и задълженията както вашите така и на вашето дете. Тук ви предоставяме няколко адреса, на които можете да намерите готови за отпечатване споразумения, като разбира се ако искате винаги може да напишете и свои собствени.

b) Вируси, спайуер, адауер

Компютърни вируси

В компютърния жаргон, **вирус** е саморазмножаваща се програма, която се разпространява като вмъква копия от себе си в друг изпълним код (програми) или документи. Това дава и името на този вид програми, тъй като подобно поведение е сходно с това на биологичен вирус, който се размножава като се вмъква в живи клетки. По аналогия, вмъкването на вирус в програма често се нарича "инфекция". Вирусите са само един от видовете злонамерени програми, но в разговорния език термина често се използва да обозначава и представители на другите видове, като троянски коне и червеи.

Компютърния вирус има способността да се предава и между различните компютри чрез електронната поща или при качването на заразен файл. Вирусите са в състояние да се разпространяват с голяма бързина и да обхващат громен брой компютри. Установено е например, че Mydoom е заразил четвърт милион компютри само за един ден през януари 2004 година. През март 1999, вируса Мелиса (Melissa) принуди майкрософт и редица други големи компании да изключат напълно електронните си пощи, докато се намери начин за справяне с проблема. Друг пример е вируса ILOVEYOU (ОБИЧАМТЕ), който се появи през 2000 година и имаше подобен опустошителен ефект.

Спайуер (spyware)

Спайуер се нарича широка категория от злонамерен софтуер, проектиран да пречи или да завземе частичен контрол над функциите на компютъра, без ваше знание. Докато буквалното значение на думата (от английски spy- шпионин) предполага следене на потребителя, този термин вече се употребява за по-широка група от софтуер, който нарушава нормалното функциониране на компютъра за целите на трето лице.

Казано по друг начин ю, спайуера е тип програма, която наблюдава дейностите, които потребителя извършва на компютъра си и изпраща събраната информация чрез интернет до зададен от

създателя на спайуера адрес. Спайуера може да събира много и различна информация за потребителя. Подобен тип софтуер може да проследява какви уеб страници посещавате и да изпрати информацията на рекламна агенция. Може да проследи какво печатате на клавиатурата и по този начин да събере данни за паролите ви в интенрет или данните за кредитната ви карта. Други версии просто стартират отварянето на прозорци или връзки, които не сте натискали.

Адуер (adware или advertising-supported software-)

Адуер е тип софтуер (обикновено поддържан от рекламодатели), който автоматично пуска, показва на монитора или сваля на компютъра ви рекламни материали, без ваше желание, докато инсталирате или ползвате въпросния софтуер.

Адуера бива интегриран в някоя програма или върви в комплект с нея. Програмистите гледат на него като начин за възвръщане на средствата, изразходвани за създаването на програмата, а в някои случаи прибавянето на адуер към програмата дава възможност тя да бъде предоставяна безплатно на потребителите или на намалена цена.

Въпреки това, той може да бъде инсталиран на компютъра ви без ваше знание и независимо от факта, че не вреди на системата, може да бъде досаден и да загуби голяма част от времето ви в опити да затворите ненужните прозорци и да изтриете свалените от него рекламни материали.

с) Измами с кредитни карти (фишинг, троянски коне, фалшиви интернет страници, спам)

Фишинг

Фишинг (или риболов) е практика, при която недоброжелатели придобиват важна информация, като парола или данни за кредитна карта, като се представят за оторизиран представител който има право на достъп до тези данни.

Човек, който извършва такъв тип измами се нарича «рибар» (phisher). Той изпраща спам съобщения до потенциалните си жертви, които гласят, че следва да потвърдят банковите си данни, като накрая посочва линк, който изглежда че води към истинска интернет страница на банка. В действителност страницата е фалшива и „рибарят" се възползва от придобитата информация за собствени цели.

Друг начин за фишинг е чрез създаване на интернет страници, които имат почти идентичен интерфейс и адрес като страницата на дадена банка. Например www.bla-bla.com, вместо www.bla_bla.com. За човек, който няма много опит е лесно да бъде заблуден и да предостави банковите си данни.

ПОМНЕТЕ !!!
Винаги недоброжелателите печелят, а вие губите.

Как да се предпазите

- Никога не отговаряйте на e-mail, който ви кара да посетите даден интернет сайт или изисква да предоставите лична информация.
- Никога не натискайте върху линкове или прикачени файлове, освен ако не ги очаквате и сте напълно сигурни от кого са.
- Никога не отваряйте файлове с разширение .zip или .rar ако не знаете от кого е файла и какво точно съдържа.
- Използвайте анти - фишинг софтуер програми и файъруол (част от софтуер и/или хардуер, която функционира при наличие на мрежа и спира достъпа от и към вашия компютър на неразрешените програми), които идентифицират интернет страници и електронни писма с фишинг съдържание, като освен това предпазват от шпионящ софтуер (спайуер- голяма група зловреден софтуер, проектиран за да пречи или да взима частичен контрол върху дадени компютърни функции, без знанието на ползвателя), както и от малуер (вид софтуер, проектиран да разрушава компютърната операционна система).
- Често обновявайте, както компютърната си конфигурация, така и софтуера си

- Никога не изпращайте по електронна поща пароли, номера на кредитни карти или друга лична информация.
- Редовно проверявайте банковите си извлечения!

Троянски кон

В компютърния свят **троянският кон**, наричан още **троянец**, е злонамерена програма, за която се твърди, че притежава някаква полезна цел, а всъщност би причинила нещо съвсем различно при изпълнението си, например: превземането на канали в IRC, изтриване на съдържание от твърдия диск, кражба на поверителни данни (пароли, информация за банкови сметки и кредитни карти) и др. Тези програми са получили името си от мита за големия, кух дървен кон, чрез който гърците печелят Троянската война, като се скриват в него и се промъкват в укрепения град Троя.

Троянските коне обикновено се разпространяват под формата на изпълними файлове за Microsoft Windows: .exe, .scr, .bat или .pif. Неопитният потребител, който работи с настройките по подразбиране, при които разширенията на файловете се скриват, не е в състояние да разбере истинския вид на файла, ако е маскиран с т.нар. *двойно разширение*, например 'Readme.txt.exe', потребителят ще види единствено 'Readme.txt', като истинското разширение .exe ще остане скрито. За да е пълна заблудата, троянецът, след стартирането си, наистина би могъл да отвори някакъв текстов документ, Или да имитира инсталационен просес, но всъщност ще работи във фонов режим и тайно ще краде, променя или изтрива информаиция или настройки на компютъра, а дори би могъл да се използва от злонамерени трети лица за извършването на атаки върху други мрежи, най-често *разпределени атаки от тип „отказ от услуга“* (Distributed Denial of Service - DDoS).

За да се защитите от троянските коне, никога не отваряйте приложения към електронните писма, които не сте очаквали да получите, особено ако подателят е неизвестен. Винаги използвайте противовирусна програма за проверка на файловете преди тяхното отваряне. Пазете се от файлове, свалени чрез програми за

споделяне посредством p2p (peer-to-peer) като KaZaA или Gnutella. Това е един от най-известните начини за разпространение на троянските коне.

Никога не влизайте във сайтове, настояващи да ги гледате с IE при разрешен ActiveX Тази покана е еквивалентна на „елате без гащи“. Никога, ама никога не цъкайте на непознат файл, „за да се отвори, та да го видите за какво е.“ Уви, втория съвет го спазват само тези, които са се мъчили да си възстановят изгубените файлове.

Най-често троянския кон е създаден, за да контролира компютъра, на който е бил стартиран. Примери за такива троянски коне са NetBus, SubSeven, Back Orifice и др. Днешните противовирусни програми безпроблемно улавят по-голямата част от съществуващите троянски коне, но има и такива, които са специално проектирани да не се забелязват от противовирусния софтуер или да го обезвреждат.

Принципът на работа на троянския кон е доста прост — след изпълненението си на даден компютър (примерът е за компютри работещи с MS Windows) той създава ключове в т.нар. регистър (registry), откъдето си осигурява начално стартиране, когато се стартира операционната система. След като се зареди в паметта, той действа на принципа на сървър и отваря един или повече порта, чрез които злонамерени личности, използващи клиентска програма, пригодена да работи с дадения вид троянец, биха могли да използват заразения компютър. Клиентите често придобиват пълен контрол над компютъра и могат дори да местят курсора на мишката върху монитора, както и да четат, трият, или качват файлове.

Съществуват троянци, които се ъпдейтват сами до последна версия.

Радикален начин за борба е да се взима интернет през прокси, без гейтуей но на IE да са зададени неверни настройки, така че, да не може да се свърже с Интернет. Към момента няма злонамерена програма, (те са по-напредничави от добронамерените) която да търси на друго място настройките за

връзка с интернет, освен от IE. А някои просто ползват IE за връзка, като го пускат през неговите API, без да се показва прозорец.

Спам

Спам (на английски *spam*) е използване на среда за електронни комуникации за масово изпращане на нежелани съобщения. Най-известната форма на спам е под формата на съобщения с рекламно съдържание по електронната поща. Спамът е използван и с други цели и използвайки други медии, като Usenet, търсачки, уеблогове, ICQ, IRC и SMS.

Спамът разпространяван чрез услугите за моментни съобщения е по известен като *spim*.

Методи за борба

Методите за борба се разделят на две категории:

- Методи, подходящи за прилагане от доставчици (ISP) / оператори на услуги;
- Методи, подходящи за прилагане от крайни потребители;

Няма точно разделение кои методи в коя категория попадат, затова просто ще бъдат изброени:

- **Блокиране на адресите**, от които се изпраща Спам - приложимо както от доставчици, така и от крайни клиенти. Резултатът е, че просто писмата не достигат до вас или в случая с краен клиент биват маркирани като нежелани и евентуално изтрити.
- **Неотваряне на нежелана поща**. Поради широкото разпространение на Internet Explorer, ниската потребителска култура и голямото количество проблеми със сигурността на по-горе споменатото приложение освен загубата на време, за отваряне на писмото / прочитане на съобщение, може компютърът да бъде заразен от вирус, троянски кон и подобен род mallware. Като краен резултат има сериозна възможност за кражба на ценни данни (банкови сметки, пароли). Отварянето на нежелано писмо също така може да даде сигнал с използване на скрити картинки в писмото, когато то е

в HTML формат, че адресът на електронната поща се използва активно. Обикновено адресите, до които се разпраща нежелана поща, се генерират с използване на речници с думи и имена, към които се добавят имена на домейни и поради това на изпращача (спамера) не е ясно дали даден адрес на електронна поща се използва или не, но с използване на скрити картинки на него може да бъде съобщено и да последва повишение на активността на изпращаната нежелана поща към този адрес.

- **Използване на черни списъци** - Обикновено това са обществено достъпни интернет сайтове, съдържащи списъци с известни адреси, от които се изпраща спам.

Тъй като горните методи се заобикалят сравнително лесно (SMTP протокола не разполага с надеждни средства за доказване самоличността на подателя), напоследък най-успешни се оказват методи, които не разчитат само на информацията за подателя.

- **Черни списъци за IP адреси на компютри**, от които се изпраща спам. Тези адреси не се фалшифицират лесно, но е възможно предварително "превзет" компютър - "зомби" да бъде накаран да изпраща писмата от своя адрес.
- **Блокиране на писма, съдържащи определени думи** - най-простия пример е с думата "Виагра". Това би могло да спре цялата нежелана поща по дадена тема. Като противодействие, спамерите обикновено използват странен начин за изписване на думата - например "Viaagraa", или търсят символи с подобен вид - "V1agra".
- **Смислов/синтактичен анализ на писмото** - силно усложнен вариант на горната техника, при който по определени признаци се прави опит да се извлекат характеристики на текста, които да покажат дали това е спам или не.
- **Блокиране на писма по определени, технически характеристики** - най-известните примери са:

- Блокиране на писма от сървъри, които нямат име (само IP адрес)

- Блокиране на писма изпратени с непознати (или известни с "черното" си предназначение) програми.

За съжаление засега няма система, която да дава 100% гаранция. Още по-неприятното е, че ако направим системата за защита твърде "подозрителна", има голям шанс някое важно писмо да отиде при нежеланите...

Най-важният съвет за защита от спам е:

Не давайте никъде ваш или на приятел електронен адрес!

Никъде включва:
- ✓ Сайтове, които изискват регистрация.
- ✓ Електронни картички (за съжаление получателят, освен картичката, ще започне да получава и спам).
- ✓ Безплатни програми или програми с неизвестен автор.
- ✓ Промоции и игри - в или извън Интернет.

Ако някой сайт изисква да Ви изпрати паролата за достъп по Email, можете да си регистрирате пощенска кутия специално за тази цел.

d) **Дайлъри** (Dialers или Diallers)

Дайлърът е компютърна програма, която създава връзка с интернет или друга компютърна мрежа, чрез аналогова телефонна линия. Обикновено дайлъра работи без знанието на потребителя. Дайлърите, с които често може да заразите компютрите си посещавайки порнографски сайтове или сайтове с кракове и серийни номера за софтуерни програми, могат да нанесат вреда само на потребители, които осъществяват връзка с интернет чрез модем.

Програмите наречени дайлъри са необходими, за да може да се свържете с интернет (когато става въпрос за не-широколентова връзка), тъй като те са тези, които избират телефонния номер, чрез които се свързвате с мрежата. Дайлърите които можете не по свое желание да прикачите от мрежата обаче, са проектирани така, че когато няма компютърна активност (т.е компютърът не се използва в момента) те набират определени телефони с добавени импулси,

обикновено в чужбина и генерират огромни телефонни сметки, от които печели собственика на импулсния телефон.

В някои случаи дайлъра ви предупреждава, че ще бъдете свързани с импулсен телефон, като ви се обещава достъп до специално съдържание, до което можете да достигнете само чрез този номер. Например ви се предлага достъп до софтуер и mp3 (обикновено незаконни), като и порнография или хакерска информация и достъп до вирусни програми.

Когато тук говорим за дайлъри (Dialers или Diallers) се има предвид само програмите, които се свързват с импулсни телефони без знанието на потребителя.

Има няколко признака, по които да разберете, че към компютъра ви е закачена нежелана дайлър програма:

- Когато отваряте интернет страница се появява диалогов прозорец.
- На интернет страницата само се загатва (ако изобщо е спомената) цената на услугата
- Инсталирането на програмата упомената в диалоговия прозорец, започва дори когато натиснете бутона за отказ.
- Дайлърът се инсталира като основна връзка, без да иска разрешение или да съобщи за това.
- Дайлърът самостоятелно осъществява телефонни връзки, без намеса от страна на потребителя.
- Преди да набере, дайлъра не показва информация за тарифата на даден номер.
- Високата стойност на услугата не може да бъде установена по време ан осъществената връзка.
- Дайлърът не може да бъде деинсталиран, или поне не без сериозни усилия.

Ето няколко програми, които предпазват или отстраняват нежелани дайлър програми:

Anti-Dialer Toolkit Pro,
MKS_Vir,
Dialer Killer

е) Интернет тормоз (**cyberbullying,** cyber-bullying, online bullying)

Според една от най-популярните дефиниции, интернет тормоз (или кибер тормоз) е използването на електронни информационни или комуникационни механизми като електронна поща, програми за интернет комуникация, мобилни телефони, пейджъри и недобронамерени интернет страници за тормоз на личност или група от хора, чрез личностни нападки или по друг начин, като в някои случаи това може да представлява и интернет престъпление. Кибер тормоза е съзнателно и повтарящо се нанасяне на вреда, осъществявано чрез електронната среда.

Съществуват различи видове интернет тормоз, но всички те имат някои общи характеристики.

Тормозът може да започне в интернет и да остане там, без да се разпростира в истинския живот. В този случаи В този случаи тормозещият и жертвата не се познават лично и никога не са се срещали. Този вид тормоз обикновено започва с т. нар на английски flame (огън, пламвам) или с невинен разговор в интернет стая за разговор (чат стая).

“Flame” е обидно или провокиращо съобщение, публикувано обикновено в интернет форум, с цел да доведе до негативна реакция от страна на участващите в дискусията. Провокаторът, наричан още трол, изчаква някой да отговори на провокацията и го набелязва като жертва. Често участниците във форуми имат профил включващ лични данни, електронен адрес, а нерядко и снимка. Така натрапника има достатъчно информация за да започне тормоз. Той започва за праща на жертвата електронни писма, публикува лични нападки, касаещи характера или външният вид на жертватаis. Този вид тормоз е по-малко мъчителен и обикновено не трае дълго. Извършващия тормоза не познава лично мишената си и ако жертвата спре да реагира на атаките той бързо се отегчава и престава или си намира друга жертва.

Другият, по-опасен и травмиращ тип интернет тормоз е когато тормозещият и жертвата са се срещали лично и дори се познават добре. В този случаи обидите са по-лични и засягат жертвата повече. Този вид тормоз може да е започнал в истинския живот и да е продължил в интернет или да е точно обратното. В най-тежките

случаи, извършващият тормоза може дори да създаде за целта специална интернет страниза, на която да публикува нападки, а понякога дори и снимки на жертвата и нейното семейство и приятели. Има случаи в които жертвите разбират за съществуването на тези страници месеци, дори години след тяхното създаване. Понякога се стига дотам, че на тези страници нападателя търси поддръжници и сформира коалиции срещу жертвата или пък се правят черни списъци на „задръстени" съученици.

За възрастен интернет тормозът може да не звучи много сериозно, тъй като не става въпрос за физическо насилие, но не забравяйте, че детската психика е по-крехка и подобно преживяване може да доведе до загуба на самочувствие, депресия и изолация от приятели и съученици- неща които значително могат да повлияят бъдещия живот на детето. Нещата се влошават още повече ако тормозещият и жертвата учат в едно и също училище или са съседи, защото тогава те неизбежно се срещат често и детето бива обиждано или заплашвано ежедневно, а това го кара да не се чувства сигурно не само на улицата или в училище, но и вкъщи.

За да предпазите детето си от интернет тормоз трябва да започнете като му обясните всички опасности, които може да срещне в мрежата. Обяснете му, че добрите обноски са толкова важни в интернет, колкото и извън него. По този начин ще предотвратите възможността то да стане случайна жертва на *трол* например или като влезе в злобен спор с потенциален натрапник.

Следващото нещо, което ви съветваме да направите е да инсталирате филтриращ софтуер на домашния ви компютър. С помощта на този тип програми може лесно да блокирате нежеланите атаки и да прекратите тормоза. Ако натрапника е упорит и продължава да изпраща електронни писма или съобщения от различни адреси не позволявайте на детето ви да отваря електронни писма от непознати или изберете и-мейл клиент (програма за получаване на електронна поща), която позволява получаването на писма само от хора, които са включени в списъка с контакти.

Въпреки, че не е добра идея да позволявате на детето си да чете писма от натрапника, ако тормозът не пре може да се окаже полезно ако ви ги прочетете. От тях може да получите информация колко далеч са стигнали нещата, а ако съдържат истински заплахи може да ги запазите като доказателство при по-нататъшни правни действия. Ако заплахите ви звучат достоверно уведомете и полицията.

Изключително важно е да разберете дали детето ви и този, който го тормози са се срещали лично и точно колко добре се познават. От това зависят следващите ви действия.

Ако детето ви не се е срещало с натрапника е много важно да не допуснете това да се случи. Трябва да предупредите детето си да не дава каквато и да е лична информация, като телефон, домашен адрес, името на училището, което посещава или каквото и да е друго, което може да помогне то да бъде открито извън интернет. Въпреки, че това се случва рядко, понякога тормозещите са толкова злонамерени или ядосани, че се опитват да се срещнат с жертвата лице в лице и да превърнат интернет тормоза в истинско издевателство.

Ако натрапника и детето ви се познават трябва да убедите детето си да сподели, кой е той. След като знаете това може да опитате да се свържете с родителите му. Често родителите на тормозещият не знаят какво прави детето им в интернет. Ако ги информирате за поведението му в интернет те вероятно ще ви помогнат да разрешите проблема. Обикновено това е достатъчно, но понякога родителите не могат или не искат да повярват, че детето им е способно на подобно нещо, затова може да ви се наложи да ги убедите. В този случаи от полза могат да ви бъдат заплашителни електронни писка, пристигнали от личния му адрес, съобщения от мобилния му телефон или нещо друго, което да го идентифицира като налагащия тормоза.

Както вече споменахме, в най тежките случаи към обикновения интернет тормоз е прибавено и създаването на интернет страници с обиди към жертвата и семейството й. най-неприятното е, че могат да минат месеци и години в които всеки може да види тези страници

преди жертвата да разбере, а дори тогава някои материали биха могли да останат в мрежата практически завинаги. Ако не можете да разрешите проблема директно със създателя на страницата или родителите му, може да се свържете с фирмата, която отговаря за поддръжката на страницата и да помолите тя да бъде отстранена. Обикновено фирмите поддържащи интернет страници, както и доставчиците на интернет подписват етични кодекси така, че не би трябвало да е проблем да премахнат страницата.

И накрая, но не по значение, не забравяйте, че децата ви не винаги ще имат желание да споделят с вас неприятностите си в интернет. Детето ви може да е било жертва на тормоз доста дълго време преди вие да разберете за това. За това вие трябва да сте подготвени и да очаквате, че честата смяна на настроението на вашето дете, депресията му, изолацията му от приятели и връстници, както и друго странно поведение могат да са дължат на кибер тормоз. Може и да не е така, но когато провеждате „домашно разследване" обърнете внимание и на тази възможност.

f) Други често срещани рискове

Има няколко проблема, освен сексуалният, които са важни и широко разпространени по мрежата. Един от тях е проблемът с "ANA"- *Anorexia nervosa (анорексия). Съществуват множество интернет страници, клубове, чат канали и форуми, които са превърнали в култ това сериозно здравословно състояние.* Съдържанието на страниците е написано по такъв начин, че едно невинно дете може да бъде подведено относно това смъртоносно психическо заболяване.

Втори основен проблем е **неонацизма**. Съществуват няколко много влиятелни световни организации, които разпространяват такъв вид информация, чрез огромен брой интернет страници, ftp - сървъри или чат канали. Повечето страници съдържат предимно текстове и поради това има сайтове, които не могат да бъдат разпознати като расистки или Нацистки, дори от възрастни. "Уловката" е в текстовете и историите, намиращи се на страниците,

които обикновено дезинформират младежите относно историята, самата организация , етичните въпроси и т.н., като просто смесват няколко действителни факта с една лъжа

Друг голям проблем, от който е особено важно да бъдат предпазени децата са интернет страниците за така нареченото **обезобразяване или модифициране на тялото**. Тези общности се поддържат от хора, които имат претенциите да са в добро психическо здраве. За съжаление те предлагат на децата много опасни, вредни и вероятно смъртоносни умения. Ето няколко примера извадени от гореспоменатия тип страници: илюстриран наръчник за това как да станеш евнух; собственоръчно ампутиране на долен крайник; предпазване на плътта от възпаление, след премахване на кожата от нея (без разумна, функционална или медицинска причина); премахване или модифициране на тестисите или пениса. Тези сайтове често се крият зад пиърсинг или манията за татуировки, които в днешно време са широко разпространени по целия свят. Има няколко интернет страници, които дори предлагат безплатни дискове с огромно разнообразие от снимки и филми по тази тема.

Последният шокиращ пример, касаещ интернет безопасността е свързан с масово разпространената масова психоза, свързана с **тероризма**. Съществува огромен брой интернет страници, торенти, peer-to-peer мрежи и частни сървъри, които предлагат информация за това как да станеш терорист, как да направиш бомба вкъщи, или филми показващи убийства в детайли, по реалистичен, нецензурен и агресивен начин.

V. Филтриращ софтуер

1. Инструменти за подбор на подходяща за децата информация

Този раздел е фокусиран върху инструменти, които дават възможност на родители, учители, библиотекари и др. да подбират подходяща за децата информация. Въпреки това се появява и друг набор от инструменти, който подпомага разработването на контролните инструменти. Пример за такива инструменти представляват интернет страници и софтуер, които подпомагат интернет провайдерите или трети страни при класифициране не интернет съдържанието, както и софтуер, който може да бъде използван за разпространяването на подобна класификация.

Надяваме се, че този доклад, ще послужи за повишаване на осведомеността относно съществуващите технологии, които могат да се използват с цел предпазване на децата в интернет. Още повече, ние се надяваме, че ще помогне на хората да идентифицират нужди в областта, които за момента не се покриват от технологиите, и ще стимулира усилията за работа в тази насока.

2. Механизми за действие на филтриращия софтуер

Идентифицирането или описването на съдържание от определен тип и предприемането на действие на база специфичността на информацията.

2.1 Действия

До този момент съществуват технологии, които са способни да предприемат шест вида действия, базирани на категоризацията или характеристиките на съдържанието на интернет страниците: предлагане, търсене, информиране, наблюдение, предупреждаване и блокиране.

2.1.1 Предлагане: препоръчва подходящо за деца съдържание.

Голям брой интернет страници, брошури и книги предлагат списъци с интернет страници, подходящи за деца. Като допълнение и някои филтриращи програми предлагат препоръки за подходящи за разглеждане от деца сайтове. Примери за механизма на предлагане са интернет порталите на : *Yahooligans!, American Library Association's "Great Sites"* ("Страхотните сайтове" на Американската библиотечна асоциация, Bonus.com, Microsystems Route 6-16 и списъкът на CyberYES, както и The Internet Kids & Family Yellow Pages (Жълтите страници за интернет децата и семействата им).

2.1.2 Филтриране по време на търсене: подбира съдържание подходящо за деца, като отговаря на конкретно търсене.

Съществуват множество търсачки, които по принцип филтрират резултатите от дадено търсене за неподходящо съдържание. Това се смята за предимство във фирменото досие и маркетинговата стратегия, като се цели да се привлекат повече родители и децата им, които да използват търсачката.
Към примерите за блокиращи търсенето портали са: Google.com, Altavista.com.

2.1.3 Информиране: предоставят информация за съдържанието.

Категоризацията по системата PICS, рецензиите и друго описание на съдържанието могат да помогнат на родителите и възпитателите да насочват децата към подходяща интернет информация. За да бъде полезна обаче, информацията трябва да бъде лесно достъпна. Някои филтриращи програми са програмирани да предоставят информация за съдържанието на интернет страниците в момента, в който потребителят се опита да ги отвори. Информацията може да се появява под формата на графики или банери върху интернет страниците, като част от браузъра или друг софтуер. Например, при TRUSTe се изобразява "trustmark" (сертификат за доверие), под формата на графика, на сайтове, които имат определен тип одобрена поверителна политика. evaluWeb пък показва на банер, който е част от съответната интернет страница, възрастовата група, за която сайтът е подходящ. Системата за

навигация в интернет Alexa предоставя информация за сайта, чрез изскачащо в отделен прозорец, допълнително меню, което може да дава информация за който и да е сайт.

2.1.4 Наблюдение: създава архив за по-късна проверка, който съдържа информация за опитите за отваряне на страници и отвореното съдържание.

Много филтриращи програми включват механизми за наблюдение.Например програмата Cyber Snoop записва данни за интернет активността, докато детето е в интернет. Възрастният «администратор» може да прегледа архива за да установи каки интернет страници е посетило детето, какви електронни писма е изпратило или в какви видове разговори по мрежата е участвало. Друга филтрираща програма- Net Nanny, има опция за записване на всички опити да се отвори съдържание, което е в разрез с политиката на администратора. Други примери за софтуер с функции за наблюдение са: Bess, CYBERsitter, I-Gear, SmartFilter. (За съжаление, всички мониторингови схеми са в разрез с правото на неприкосновен личен живот. Не винаги нарушаването на нечии права е начинът той да бъде защитен.)

2.1.5 Предупреждаване: предоставя информация за съдържанието на страницата и препоръчва да не бъде отваряна.

Механизмът за предупреждение съобщава, че съдържанието на страницата не се препоръчва, преди самото то да се появи на екрана. Този тип инструменти могат да бъдат полезни при предпазване на децата от неволно изтегляне на файлове, чието съдържание може да ги разстрои. Много интернет страници за възрастни съдържат предупреждение, поставено на видно място, гласящо, че съдържанието не е подходящо за лица под 18 години, или използват система за проверка на възрастта.

Инструмент като Microsoft Internet Explorer Content Advisor, които са проектирани да блокират страници, но включват и отмяна на забраната след въвеждането на парола, могат да бъдат използвани и за предупреждаване. Родителите могат да предоставят

на децата си парола, която да им позвлява достъп до информация, които иначе би била блокирана. По този начин децата биват предупредени, че съдържанието на страницата не е подходящо, но все пак могат да я отворят ако желаят.

Проблемът при взаимоотношенията родители-деца, когато става въпрос за безопасността на детето в интернет, се състои в това, че много често децата имат висока компютърна грамотност, докато при родителите им тя напълно липсва.

2.1.6 Блокиране: спира достъпа на деца до дадено съдържание.

Голямо разнообразие от инструменти предпазва децата от достъп до неподходяща информация. Някои, като MS Internet Explorer, филтрират информацията на база на набор от PICS категории, посочени от родителя. Други, като Bess блокират интернет страници, които съдържат думи, които се смятат за неподходящи или са включени в списъка "лошо за деца". Други ,като AME например, блокират всички страници, които не се появяват в списъка "одобрено за деца".

Други примери за блокиращ софтуер са: Bonus.com, Cyber Patrol, CYBERsitter, Cyber Snoop, evaluWEB, I-Gear, Net Nanny, PlanetView

2.2 Локализация

Механизмите, които прилагат действията, описани по-горе, могат да се разположат на различни места в компютърната система, включително и личния компютър на потребителя, в локалната мрежа, в локалния или отдалечен прокси сървър, при интернет доставчика или като част от търсача или уеб сайт.

2.2.1 Персоналният компютър

Разполагането на механизмите в персоналния компютър може да улесни тяхното конфигуриране и преконфигуриране от родителите, учителите или други администратори. От друга страна, това може да улесни преконфигурирането на тези механизми от децата, противно на желанията на родителите им и вероятно без

знанието на родителите. Някои от продуктите базирани в персоналния компютър са разработени, които да предотвратяват механизми за злонамереното им изменение. Много от продуктите, базирани в персоналния компютър, изискват актуализация; някои могат да се адаптират сами, когато компютърът се включи към интернет.

Примери на инструменти, които могат да работят в персоналния компютър включват: Cyber Patrol, CYBERsitter, Cyber Snoop, NetNanny, SurfControl, Net Shepherd, Firefox разширения на браузърите.

2.2.2 Защитни стени в локалните мрежи или локални proxy сървъри (сървъри посредници)

Разполагането на механизмите в локалните мрежи или използването на локални proxy сървъри може да бъде полезно решение в ситуации, когато се работи в мрежа от PC, такива като училища или библиотеки. Централизираната конфигурация е по-лесна за системния администратор и по-трудна за индивидите за злонамерено вмешателство.

Примери на инструменти, които могат да работят в локални мрежи или proxy сървъри включват: CyberPatrol, Bess, Cyber Snoop, I-Gear, NetNanny, SafeSurf Internet Filtering Solution, SmartFilter, SurfControl.

2.2.3 Доставчици на интернет

Интернет доставчиците не могат ефективно да контролират огромното количество материали, създавани от индивиди и организации. Някои интернет доставчици предлагат услуги, специално предназначени за деца. Доставчиците могат да предоставят филтриран интернет достъп или ограничен достъп до чатове, новини или други видове услуги.

Примери на инструменти, които могат да се използват от интернет доставчиците включват: AME, I-Gear, netFilter, SurfControl.

2.2.4 Търсачки

Някои търсачки връщат по подразбиране само показалците към съдържание, което е подходящо за деца и младежи. Например, Google и AltaVista са програмирани да не показват съдържание за възрастни. Те трябва изрично да се конфигурират, за да могат да го правят.

2.2.5 Уебсайт

Множество уебсайтове дават списъци на съдържание, което е подходящо за деца. В допълнение, някои уебсайтове съдържат етикети, графики, или други описания на съдържания, които може да бъдат полезни на родителите в насочването на техните деца към подходящо съдъжание. Асоциацията за Атестиране на съдържанието в интернет е международна нестопанска организицаия на интернет лидерите, които работят за развитието на безопасен интернет. Базов елемент на организацията е описателен справочник, който често е наричан въпросник на Асоциацията за атестиране на съдържанието в интернет. Доставчиците на съдържание проверяват кои от елементите на въпросника присъстват или отсъстват в техните уебсайтове. Това от своя страна генерира малък файл, съдържащ етикети, които след това се свързват със съдържанието на един или повече домейна. Потребителите, особено родителите на малки деца, могат да използват филтриращ софтуер, за да разрешат или забранят достъпа до определени уебсайтове на базата на информацията, декларирана на етикета. Ключов момент е, че не Асоциацията за атестиране на съдържанието в интернет характеризира съдържанието, а тези, които го предоставят правят това, като използват системата за етикетиране на асоциацията. Справочникът на Асоциацията се състои от няколко въпроса:

- Присъствие или отсъствие на голи тела
- Присъствие или отсъствие на сексуално съдържание content
- Описание или рисунки на насилие
- Използван език
- Присъствие или отсъствие на съдържание, генерирано от потребителя и дали това е контролирано
- Описание или друго потенциално вредно съдържание такова като хазарт, наркотици и алкохол

2.3 Възможност за настройки

Продуктите за филтриране в интернет дават голям набор от опции за настройки, включително: механизми за блокиране и позволяване на списъци; определяне на ключови думи или фрази за превключване; определяне на категории от съдържание, които да бъдат позволени или блокирани, предупредителни съобщения, влизане с регистрация или други действия. Продуктите, позволяващи настройки, обикновено са насочени към разнообразни нужди на потребителите, и ако не са внимателно програмирани, могат да бъдат твърде сложни за конфигуриране.

2.4 Класификация

Независимо какви действия са предприети, механизмите трябва да етикетират или да определят съдъжанието от определен тип. За всяка система, която етикетира или класифицира съдържание, е важно да се разбере кой извършва класификацията, и какви критерии се използват за това.

2.4.1 Кой/как

Класификацията може да се извършва от:

Доставчиците на съдържание. Асоциацията за атестиране на съдържанието в интернет и SafeSurf са примери на платформиза спецификация (PICS) на съдържанието в интернет, които са програмирани за използване от доставчиците на съдържание.

Експерти на трета страна. Много компании за филтриране използват екипи от информационни специалисти, родители и учители да подпомогнат класифицирането на съдържанието. Например, AME, Bess, Bonus.com, Cyber Patrol, SurfControl.

Местни администратори. Родител, учител или друг местен „администратор" може лично да решава какво съдържание да бъде достъпно за децата под негово наблюдение. Cyber Snoop и Click & Browse Jr. са примери на продукти, които включват списъци с разрешени сайтове, генерирани от местни администратори. Разбира

се, в случая трябва да се приложи механизъм за проверка на грешката „контролиране на контрольора".

Уебмастери и провайдери на пространство. Една от привилегиите на отвореното информационно общество е правото да се изразява мнение за собственото съдържание и да го споделя с другите, които също имат правото да оценяват вашето съдържание. Това е линията, където трябва да различим не само незаконно съдържание, а друга категория – неморално съдържание. Трябвада отбележим, че не винаги неморалното съдържание е незаконно. Разбира се нравствеността зависи от кулутрата и безопасността в интернет е глобален въпрос, но основните морални ценности са неизменни.

Проучване или гласуване. Един начин да се класифицират обекти е чрез проучване или гласуване. Тази техника се използва от редица организации за класиране на ресторанти и филми. Напоследък Net Shepherd започнаха да използват този подход с тяхната световна служба за класиране на мнението. Net Shepherd е установила "Оценяваща общност" от хора, които оценяват и класифицират съдържанието и получават точки, които могат да се заменят за награди.

Автоматизирани инструменти. Това са автоматизирани инструменти за подпомагане на класифицирането на съдъжанието онлайн. Някои от тези инструменти, например evaluWeb, се използват за динамично класифициране на съдържанието, при запитване от потребителя. Други, такива като инструментите наети от N2H2, се използват за подпомагане на хора, които класифицират, при намиране на подозрителни сайтове. Друг софтуер, който използва автоматизирани инструменти за класифициране на съдържанието включва: CYBERsitter, netFilter, Net Nanny.

2.4.2 Класификационна схема

Класификационната схема може да е програмирана да открива съдържание, което е „добро за деца" или съдържание, което е „вредно за деца" или едновременно и двете. Съдържанието може да се класифицира на базата на подходящо за възрастта, ил на

базата на специфични характеристики или елементи на съдържанието, или на базата на това, кой е създал съдържанието, различавайки правителствени или неправителствени източници.

2.4.3 Обхват

Съдържанието по интернет се предоставя посредством множество протоколи HTTP (хипертекст трансфер протокол), FTP, SMTP, RSS/RDF, чат, телнет и т.н. Някои продукти и услуги са фокусирани на един или малък брой от тези протоколи, докато други предоставят по-обширни решения, като контролират всичко, което детето прави онлайн. В допълнение, някои продукти и услуги контролират само входящите комуникации, докато други контролират и входящите и изходящи комуникации. Инструментите, които контролират изходящите комуникации могат да бъдат конфигурирани да предпазват децата от предоставяне на лична информация, която може се използва в тяхна вреда, такива като домашен адрес или телефонен номер.

3. Пропуски

Значителен прогрес е постигнат в набора от инструменти за родители, учители и библиотекари, но почти във всички видове инструменти могат да се направят подобрения, а някои от тях все още не са широко достъпни. Ние подчертахме няколко вида инструменти, които може би се нуждаят от по-натъшно развитие.

3.1 Система(и) за самооценяване с широко покритие

Докато някои системи за самооценка, базирани на платформи за определяне на съдържанието в интернет, и особено Асоциацията за атестиране на съдържанието в интернет, са привлекли значително медийно покрити по света, никоя от системите за самооценка не са получили дори приблизително световно отразяване. Alexa Internet съобщава, че през август 1997 те са „претърсили" набор от 88,647 уеб страници (това са били най-търсените страници от техните потребители) и са открили, че 2363

имат етикети на ICRA labels, а 483 имат етикети на SafeSurf. Година по-късно ICRA съобщава, че над 80,000 сайта са били оценени с въпросника на ICRA, и че много от тези сайтове съдържат огромен брой страници. Обаче, не е ясно какъв процент от най-популярните сайтове или от най-агресивните са се самооценили, или дали този процент нараства.

Трябва също да се отбележи, че има стратегически действия, такива като задължително етикетиране, което може да доведе до разширяване обхвата на системите за самоетикетиране. Тези стратегии се използват от някои търсачки и индексиращи служби, които изискват етикетиране на ICRA, за да стартират процедурите.

3.2 Повече изследване на „предупредителните" действия

Въпреки че много от блокиращите инструменти могат да бъдат използвани като предупредителни инструменти, просто като казват на децата парола за пренасочване, никой не е програмирал техния интерфейс така, че да направи тази функция атрактивна, нито пък насърчава активно родителите да разгледат тази възможност. Тази опция може да е полезен инструмент за защита на децата от случайно разтоварване на съдържание, което да ги разстрои.

VI. Кой може да ви помогне?

1. Държавни органи

Държавната агенция за закрила на детето

В България, държавния орган отговорен за защита на децата, както в интернет, така и извън него е **Държавната агенция за закрила на детето**, където може да разчитате на екип от професионалисти- педагози, психолози, лекари и адвокати, които разработват програми за предпазване а децата и могат да ви помогнат за защита на техните права. Повечето от правата на децата в България са гарантирани от приетия на 31 май 2000 година, Закон за закрила на детето.

Сигнали към агенцията можете да подадете чрез интернет адрес: http://www.stopech.sacp.government.bg/?sid=child_eng&pid=911000000

или на телефон **02 933 90 50**

Дирекция "Социално подпомагане"

Във всяка община има Отдел за закрила на детето. Ако не знаеш къде се намира най-близката за теб община, виж „Връзки" – там са посочени адресите и телефоните на отделите за закрила на детето в различните градове.

В отделите работят **социални работници** заедно с други специалисти, които помагат за разрешаването на проблемите на децата.

Министерство на вътрешните работи

Министерството може да осигури на детето ви полицейска закрила в рамките на 48 часа, когато:

- Е обект на престъпление;
- Има непосредствена заплаха за живота и здравето му;
- Има опасност да бъде въвлечено в извършването на престъпление.

2. Неправителствени организации

В България вече съществуват множество неправителствени организации, работещи за закрила на детето. Тук можете да намерите контактите и сферата на дейност на някои от тях.

Българска асоциация за защита на детето - http://www.bgacp.com/

На страницата на организацията можете да намерите и важни връзки към редица други организации работещи в същата сфера.

Детство без сълзи- http://www.detstvobezsalzi.orgl

"Детство без сълзи" е сдружение с нестопанска цел за обществено полезна дейност. Дейността на сдружението е насочена към защита правата на деца пострадали от насилие във всички негови форми - домашно, физическо, психическо, сексуално; закрила на деца станали жертва на трафик; борба с детската порнография и детската проституция; издирване на изчезнали деца; социална рехабилитация на такива деца и социална превенция на насилието.

Целите на сдружението са:

- Подпомагане на деца, жертви на насилие
- Насърчаване на обществеността начало, превантивната и подпомагащата дейности по въпросите за насилието упражнявано върху деца;
- Подпомагане на децата жертви от престъпления и техните родители за реинтеграция в социалния живот;
- Запознаване на българската и международната общественост със състоянието и проблемите на горните процеси в страната;

Адрес: ул. „Солунска”4, ет 2, ап. 3
Тел.: 980 87 84
е-мейл: office@detstvobezsalzi.org

Асоциация Деца в мрежата- http://kidsweb.mobikom.com

Асоциация Деца в мрежата е създадена с цел превръщането на ИНТЕРНЕТ в безопасно за децата място за образование и развлечение..

Тел..: 088 233 024
Е-мейл: kids_on_the_web@mail.com

VII. Полезни интернет адреси

http://www.onlinechildprotection.org/bg/ - интернет страница, насочена изцяло към проблемите за безопасността на децата в интернет

Http://www.bnap.org/ - Българска национална асоциация на потребителите

Http://www.bnap.org/f/ - Форум на Българска национална асоциация на потребителите

http://www.sacp.government.bg/ – Държавна агенция за закрила на детето

Интернет сайтове на български, с информация за интернет безопасността, както и игри и забавна информация подходяща за деца:
http://www.az-deteto.com
http://www.dechica.com
http://kidsbg.com

http://deca.start.bg-/ - интернет портал съдържащ връзки към голям брой страници подходящи за деца

http://potrebitel.strat.bg/ - интернет портал съдържащ връзки към страници с полезна за потребителите информация

Международни страници съдържащи информация за интернет безопасността и материали подходящи за деца:
http://www.safekids.com
http://www.safeteens.com

http://www.netsmartz.org

http://www.kidsmart.org.uk- информация за родители, учители и деца

http://www.ftc.gov/bcp/conline/edcams/kidzprivacy - тук можете да намерите раздели с информация полезна както за вас така и за вашите деца

http://familyinternet.about.com – интернет сайт подходящ за цялото семейство

http://www.cyberangels.org – тук можете да намерите допълнителна информация за това как да научите децата си да се предпазват в мрежата.

http://www.netalert.net.au – популяризира необходимостта от безопасен интернет за децата

http://www.teenangels.org – сайт представящ дейността на група тийнейджъри, които образоват връстниците си за интернет безопасността

http://www.wiredkids.org – разнообразна информация за интернет безопасността, както и множество онлайн и офлайн проекти насочени както към децата, така и към възрастните

http://www.BeSafeOnline.org- предоставя съвети по интернет безопасност за деца, родители и учители, както и насърчава отговорно поведение в мрежата

http://www.getnetwise.org – портал за интернет безопасност

http://www.blogsafety.com/forum.jspa?forumID=1100000006 – форум, където родители, тийнейджъри, обучители и експерти обсъждат безопасното общуване в интернет.

http://www.google.com/Top/Computers/Internet/Proxying_and_Filtering/Content_Filtering/Software/Client - тук можете да намерите допълнителна информация за програмите филтриращи интернет съдържанието

http://www.saferinternet.org – Европейския портал за интернет безопасност

БНАП
София, 1000
Ул. “11 Август” №10
Тел. 02/9890106
Факс. 02/9890107
E-mail: bnap@bnap.org

www.bnap.org
www.onlinechildprotection.org

При изготвянето на пособието са използвани материали от Уикипедия- свободната енциклопедия:
http://bg.wikipedia.org/