СОФИЙСКИ ФОРУМ ЗА СИГУРНОСТ
SOFIA SECURITY FORUM

Erasmus+

ЦЕНТЪР ЗА РАЗВИТИЕ НА ЧОВЕШКИТЕ РЕСУРСИ

Сигурността@ на младите в интернет. Предизвикателствата пред киберсигурността

Редактор Йордан Божилов

София, 2015

София, 2015

© Редактор: Йордан Божилов

© Издателство: Елестра ЕООД

СЪДЪРЖАНИЕ

УВОД 5

О Б Р Ъ Щ Е Н И Е 7

ДОКЛАД ОТ ПРОУЧВАНЕ НА НАГЛАСИ И ПОЗНАНИЯ НА МЛАДИТЕ ХОРА ЗА БЕЗОПАСНОСТ В ИНТЕРНЕТ В РАМКИТЕ НА ПРОЕКТ: "СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ. ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД КИБЕРСИГУРНОСТТА." 9

ПРОУЧВАНЕ ЗА СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ 21

ПРЕПОРЪКИ ЗА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В КИБЕРПРОСТРАНСТВОТО 33

СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ
ЗАЩО МЛАДИТЕ СА УЯЗВИМИ В МРЕЖАТА? 39

ЗАПЛАХИ И РИСКОВЕ В ИНТЕРНЕТ 55

ОПАЗВАНЕ НА ЦЕННА ИНФОРМАЦИЯ И БЕЗОПАСНО ОПЕРИРАНЕ СЪС СРЕДСТВА 57

СИГУРНОСТ В КИБЕРПРОСТРАНСТВОТО 59

КОМПРОМЕТИРАНЕ НА ИНФОРМАЦИОННАТА БЕЗОПАСНОСТ ЧРЕЗ МЕТОДИТЕ НА СОЦИАЛНИЯ ИНЖЕНЕРИНГ 62

УВОД

Йордан Божилов
Председател на СОФИЙСКИ ФОРУМ ЗА СИГУРНОСТ

В днешния динамичен и изпълнен с рискове свят въпросите на сигурността излизат на преден план. Много са аспектите на сигурността, като сигурността на интернет е само един от тях и, за съжаление, често подценяван въпрос, въпреки че животът ни все повече се обвързва с виртуалното пространство. Ние сме постоянно он-лайн, като чрез интернет търсим информация, комуникираме, осъществяваме финансови и други операции и т.н. Доколко обаче сме запознати с рисковете, които ни заплашват и имаме ли изградена култура на поведение в интернет е сериозен въпрос. За съжаление все повече хора стават жертва на различните рискове, които ни дебнат в интернет, а сред най-уязвимите са младите хора.

Софийски форум за сигурност започна проект, чиято цел да способства за повишаване на сигурността на младите хора в интернет и да подпомогне държавните органи в разработването на политики в тази област. Проектът получи подкрепата на Центъра за развитие на човешките ресурси и се подпомага и финансира по програма Еразъм +.

Бе направен анализ на рисковете и заплахите в интернет, защо младите хора са уязвими и каква е международната практика за преодоляване на рисковете в интернет.

В хода на проекта беше проведен тридневен форум с участието на младежи на възраст между 15 и 30 години, представители на министерства и ведомства, неправителствения сектор, академичните сред и бизнеса. Нашето убеждение е, че именно чрез подобно сътрудничество и взаимодействие могат да се провеждат наистина работещи политики в областта на защитата на младите в интернет.

Форумът беше разделен на три части. През първия ден специалисти в областта на сигурността изнесоха презентации, чиято цел бе да запознаят аудиторията с рисковете в интернет, да покажат защо младите хора са уязвими и да представят различни държавни политики.

През втория ден участниците бяха разделени в три работни групи по интереси. Целта на работните групи бе да се задълбочат познанията на участниците в определени области. Първата работна група се фокусира върху "Предизвикателствата пред киберсигурността". Участниците дискутираха какви са рисковите фактори и широк кръг въпроси, свързани с интернет. Втората група работи по въпросите, свързани с "Развитието на онлайн сектора и ИКТ". В тази група бе развърната своеобразна лаборатория за компютърна вирусология и младите хора задълбочиха техническите си познания. Третата група разгледа психологическите аспекти на рисковете в интернет. С участниците в тази група бе проведен психологически тест за личностно развитие.

В третия ден на форума участниците сами търсиха решения на проблемите на сигурността в интернет. Те трябваше да използват опита и знанията, придобити от първите два дни на форума, и сами да формулират предложения и мерки. Бе организирана симулация на заседание на правителството по проблемите на сигурността в интернет. Всеки имаше предварително зададена роля на член на кабинета. В резултат на обсъжданията са изготвени предложения, които са приложение към обръщението, прието от конференцията.

Съществена част от проекта бе провеждането на изследване за нагласите и познанията на младите хора за безопасна работа в интернет. Надяваме се, че това изследване ще подпомогне държавните органи да набележат правилните политики. При проучването на нагласите и познанията на младите хора в интернет активно се включиха различни министерства и организации, като част

от въпросите в анкетите бяха формулирани от самите държавни структури.

Не е възможно да се прави политика без да има достатъчно добро познаване на обекта на политики. Впрочем, младите хора не трябва да бъдат само обект на политики, но и техен субект. Те трябва активно да се включат в подготовката на решения, които ще се отнасят до тях. Младите хора по време на форума имаха възможност да правят предложения, да участват в ролеви игри и да се обучават по въпросите на сигурността във виртуалното пространство.

В хода на проекта бе организиран конкурс за есе, като младите хора трябваше да покажат познания по темата или да споделят свои впечатления или реални ситуации, но и да демонстрират добри познания по български език, добро логическо мислене и възможност да подготвят кратък и съдържателен материал. Най-добрите есета в двете възрастови групи бяха наградени с парични и предметни награди.

Младите хора, взели участие в проекта, имат възможност, по тяхно искане, да получат Youthpass certificate.

За да се разпространят познанията по безопасен интернет бе разработена специална фейсбук-страница, която постоянно се попълва и осъвременява.

Младите хора, участвали във форума, приеха декларация до държавните органи, в която са изложени техните виждания как да се повиши сигурността в интернет. Направени са и конкретни предложения за действия и политики.

Проектът получи широка медийна подкрепа. Изготвени са няколко материала, участници в проекта дадоха интервюта за телевизии и радиа по темата.

В настоящото издание ще намерите материалите, изготвени в рамките на проекта, както и презентациите на специалистите по въпросите на сигурността в интернет, изнесени по време на тридневния форум на 10-12 ноември 2015. Надяваме се, че това ще бъде малък принос за по-сигурен и безопасен интернет за младите хора.

До
Президента на Република България Росен Плевнелиев
Председателя на Народното събрание Цецка Цачева
Министър-председателя на Република България Бойко Борисов

О Б Р Ъ Щ Е Н И Е

/прието от участниците в младежки форум по проблемите на безопасността в интернет/

В периода 10-12 ноември 2015 година в София се проведе тридневен форум по въпросите на сигурността на младите в интернет и предизвикателствата пред киберсигурността, организиран от Софийски форум за сигурност по програма Еразъм + и с подкрепата на Центъра за развитие на човешките ресурси. Във форума участие взеха младежи на възраст между 15-30 години, представители на различни министерства и ведомства, специалисти в областта на киберсигурността, представители на IT бизнеса в България.

Участниците в конференцията се обединиха около мнението, че рисковете и заплахите за младите хора във виртуалното пространство са многобройни, постоянно се увеличават и стават все по-комплексни.

За младите хора интернет се превръща все повече в потребност, като чрез мрежата те черпят познания, споделят информация, комуникират и т.н. Интернет създава сериозен потенциал за развитие, но същевременно крие и сериозни опасности, особено ако младите хора не ги познават и нямат знанията как да се предпазят. За съжаление все повече се увеличава броят на младежите, които са станали жертва на престъпления, започнали или извършени чрез интернет. В същото време, младите хора не са обучавани и не знаят към кой държавен орган да се обърнат, когато установят неправомерни дейности в интернет. Отслабена е връзката между родители и деца, когато става въпрос за споделяне на проблеми, свързани с интернет.

За да се повиши сигурността на младите в интернет, участниците в конференцията предлагат да бъдат предприети следните мерки:

1. Да се предприемат действия за обучение на младите хора за работа в интернет. Важно е създаването на култура за работа в тази среда. Най-удачно би било да се включат в училищното образование определени модули, съобразени с възрастта на учениците.

2. Да се приеме Национална стратегия за киберсигурност, като специално внимание в нея да бъде отделено на младите хора като една от най-застрашените групи от кибер-рискове.

3. Да се работи с родителите с цел да се повиши родителския контрол върху ползването на интернет от младите хора, като за целта е подходящо обсъждане на тези въпроси на родителски срещи в училище.

4. Необходима е координация между държавните органи, бизнеса, неправителствения сектор и академичните среди за противодействие на рисковете в интернет и за подпомагане на младите хора да се справят с тях.

София 12 .11.2015

ПРЕДЛОЖЕНИЯ ЗА МЕРКИ И ПОЛИТИКИ /МЛАДЕЖКО ПРАВИТЕЛСТВО 1/

1. Организиране на срещи, дискусии и образователни мероприятия, в които свободно да участват родители и ученици с цел подобряване на комуникациите родител-дете.

2. Създаване на кампании, групи в интернет, събития и много развлечения по темата за сигурността.

3. Въвеждане на нов предмет „Сигурността ми в интернет" в учебния план.

4. Използване уменията и способностите на киберпрестъпници чрез замяна наказанията им с цел подпомагането на органите на МВР, МО и ДАНС.

5. Стрес-тестове на информационните системи на държавните администрации и ведомства.

6. Отпускане на средства за финансиране на Националния Център за безопасен интернет разширяване на неговата дейност.

7. Взаимодействие между държавните институции и националните медии за повишена информираност на младите хора по повод тяхната киберсигурност.

8. Реформа в НК във връзка с криминализирането на зловредни кибер-атаки.

9. Съвместна работа на МО, МТИТС, МП, МЗ, ММС, МОН, ДАНС, НПО по създаването на работна група по киберсигурност.

ПРЕДЛОЖЕНИЯ ЗА МЕРКИ И ПОЛИТИКИ /МЛАДЕЖКО ПРАВИТЕЛСТВО 2/

1. Провеждане на политики за информираност чрез:

- сайтове
- рекламни клипове
- късометражни филми от държавни училища (финансиране: публично-частно)

2. Въвеждане на политики за образование, като:

- ролеви игри (МВР, МО, МОН и Общини, ММС и др.)
- промяна в учебните планове
- създаване на работни групи по въпросите на сигурността в интернет то различни специалисти (педагози, IT специалисти, психолози, представители на МВР)
- обучение на родители, учители, директори, деца по безопасност в интернет

3. Провеждане на политики за превенция

- промяна на законодателството
- работа с интернет доставчиците (ограничителни пакети)
- онлайн антивирусна програма, поддържана от правителството, в полза на социално слаби семейства

ДОКЛАД ОТ ПРОУЧВАНЕ НА НАГЛАСИ И ПОЗНАНИЯ НА МЛАДИТЕ ХОРА ЗА БЕЗОПАСНОСТ В ИНТЕРНЕТ В РАМКИТЕ НА ПРОЕКТ: "СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ. ПРЕДИЗВИКАТЕЛСТВАТА ПРЕД КИБЕРСИГУРНОСТТА."

За провеждане на политики в една или друга област е необходимо познание на ситуацията и идентифициране на основните рискове. С цел да се подпомогне изграждането на държавна политика в областта на киберсигурността, бе направено проучване на познанията и нагласите на младите хора в областта на сигурността в интернет.

За разработване на теоретичен модел-подход бе извършен анализ на наличната литература по въпросите на сигурността в интернет, като специално внимание бе обърнато на рисковете за младите хора във възрастовата група 15-30 години. Бяха идентифицирани основните рискове и заплахи, което позволи формулиране на въпроси, които да идентифицират как младите хора възприемат тези рискове.

Общият брой въпроси в анкетата бе 40, като част от тях бяха насочени към личността на респондента, като възраст, пол, занятие, местоживеене. Друга група въпроси бяха насочени към навици при работа в интернет, група въпроси беше насочена към оценка на знанията специфични средства, основно софтуерни, за работа в интернет и за сигурността във виртуалното пространство. Чрез анкетата се цели и проучване на специфично поведение.

Бяха формулирани въпроси, свързани с основни правила и навици за безопасна работа в интернет, които се базират на препоръки на международни експерти в тази област. Специална група въпроси бяха свързани с ролята на държавата в областта на безопасния интернет и ролята на образованието в създаване на култура на поведение в интернет.

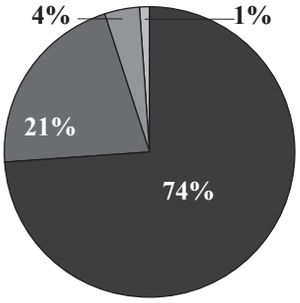
Част от въпросите бяха формулирани по такъв начин, че да служат за целите на обучението на младите за работа в интернет. По този начин, отговаряйки на въпроси на анкетата, младите хора могат да разберат за отделни прийоми и техники за осигуряване на тяхната безопасност.

Анкетата бе разработена в два варианта – хартиен и онлайн, което позволи включване на повече респонденти от различни градове. Анкетата бе абсолютно анонимна. Като цяло респондентите с интерес и положително посрещнаха предоставената им анкета. Попълването не породи затруднения поради това, че въпросите бяха формулирани ясно и с отчитане на възрастовата група на респондентите. Респондентите се отнасяха към попълването с необходимата сериозност и внимание. Считаме, че постигнатите резултати са представителни в рамките на формулираните въпроси и дават достатъчно материал за по-нататъшни анализи и работа в направление на осигуряване на сигурността на младите хора в интернет.

В обследването се включиха млади хора на възраст между 15 и 30 години, като анкетите в хартиен ваирант бяха изпратени в училища и университети, а електронната форма бе достъпна чрез страницаната на Софийски форум за сигурност и чрез фейсбук страницата на проекта „Сигурност на младите в интернет“.

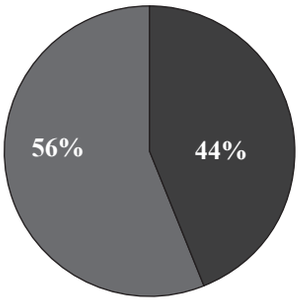
1. Вие сте на възраст между:

- 15-20 г.
- 25-30 г.
- 21-25 г.
- над 30 г.



2. Вие сте:

- мъж
- жена

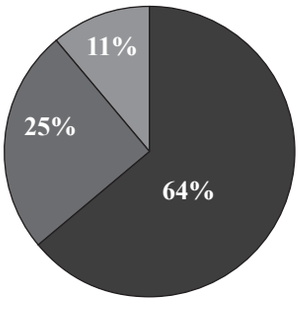


56% = 231
44% = 290

Респондентите бяха разпределени приблизително поравно като процентно отношение между половете.

3. Вие:

- учите
- работите
- нито едно от двете

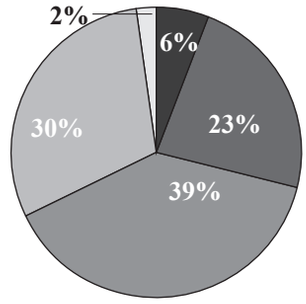


64% = 485
25% = 33
11% = 5

По-голямата част от респондентите са учащи в средните училища или университети. Сред студентите, попълнили анкетата се очертава голяма част, които освен обучението осъществяват и трудова дейност.

4. Вие прекарвате в интернет дневно

- по-малко от 1 час
- 4-6 часа
- между 1 и 2 часа
- над 6 часа
- между 2 и 4 часа

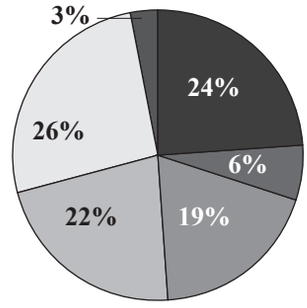


39% = 191
30% = 147
23% = 114
6% = 27
2% = 12

Анкетното проучване показа, че младите хора прекарват голяма част от времето си пред компютъра. Бе установено, че младежите в ученическа възраст използват интернет средно над 4 часа дневно, което е повече от досегашните изследвания, включително такива, провеждани на европейско ниво. Прави впечатление фактът, че времето, прекарвано в интернет, намалява с оглед на това дали лицата учат и/или работят. При всички положения интернет заема много сериозно място в ежедневието на младите хора.

5. Интернет за Вас е свързан основно с:

- търсене на информация
- работа
- комуникация с други хора
- учене
- забавление
- друго

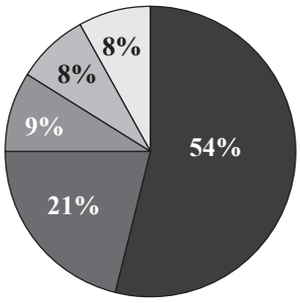


26% = 417
24% = 397
22% = 353
19% = 310
6% = 101
3% = 45

Освен че интернет заема голяма част от времето на младежите, той се свързва с комуникацията, търсене на информация, забавление и т.н. Иначе казано, всички основни дейности в нашия живот вече се свързват с използването на интернет.

6. Запознати ли сте с рисковете и опасностите в интернет?

- не
- по-скоро не
- по-скоро да
- да
- не считам, че съществуват рискове в интернет

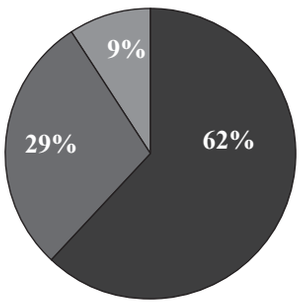


54% = 309
21% = 162
9% = 29
8% = 12
8% = 9

Както бе отбелязано по-горе, младите хора прекарват в интернет голяма част от времето си и осъществяват най-различна дейност. В същото време 75% от тях не знаят или не са напълно наясно какви рискове ги дебнат във виртуалното пространство.

7. Провеждано ли е с Вас обучение за сигурност при работа в интернет?

- не
- да
- обучавал съм се самостоятелно чрез специализирана литература

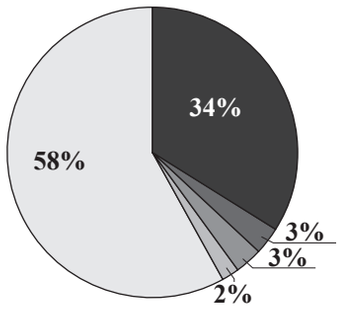


62% = 324
29% = 149
9% = 48

Резултатът от отговорите на въпрос 6 до голяма степен е свързан и се припокрива с отговорите на въпрос 7. Почти същият процент от младите хора отговорят, че не е провеждано обучение с тях.

8. Ако с Вас е провеждано обучение по сигурност при работа в интернет то е било:

- в училище
- в университета
- посещавал съм курс самостоятелно
- от работодателя
- не съм обучаван

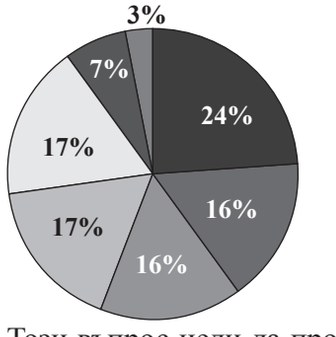


58% = 281
34% = 165
3% = 16
3% = 13
2% = 8

Част от младите хора отговарят, че е провеждано с тях обучение в училище. По всяка вероятност това се дължи на активността на отделни училищни директори или преподаватели, или дейността на неправителствени организации. Категорично може да се каже, че обучението по безопасност в интернет не е резултат на целенасочена политика и системност.

9. Според Вас рисковете в интернет са свързани основно с:

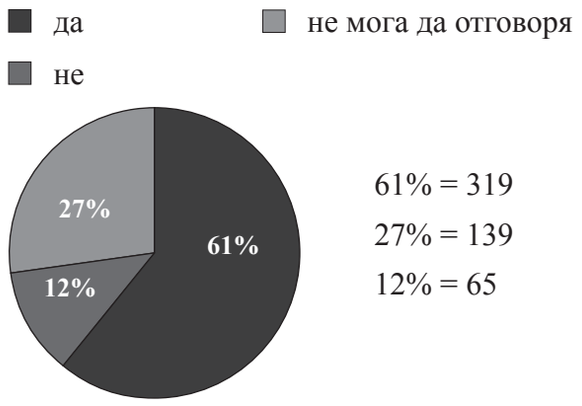
- кражба на информация
- злепоставяне на отделни хора чрез изнасяне на невярна информация
- финансови злоупотреби
- сексуални престъпления
- изпращане на вируси
- тероризъм
- друго



24% = 421
17% = 311
17% = 296
16% = 292
16% = 291
7% = 120

Този въпрос цели да проучи какви рискове разпознават младите хора в интернет. На практика отговорите са разпределни поравно между тъй наречените „традиционни рискове“ в интернет. Интересното е, че младите хора почти не разпознават опасността от тероризъм и кибер-тероризъм, което е ново явление, но представлява изключителна опасност. Същото може да се каже и за въпроса за радикализация чрез интернет и привличане на младежи за терористична дейност чрез интернет. Изследвания показват, че над 90% от младите хора, рекрутирани от Ислямска държава са били привлечени чрез интернет.

10. Знаете ли как да се предпазите от рисковете в интернет?



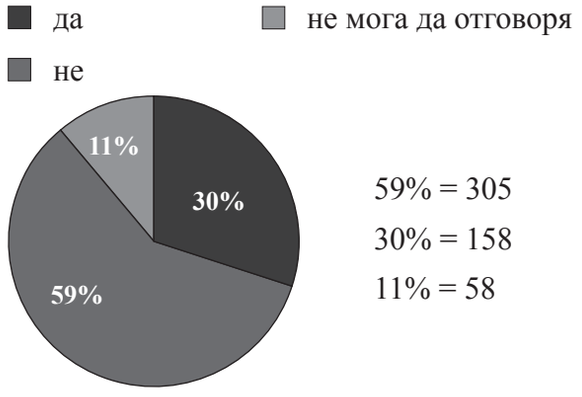
Младите хора показват доста висока степен на увереност за справяне с рисковете, което според нас се дължи на непознаване на рисковете и заплахите и това се доказва от отговорите на редица въпроси по-долу.

11. Били ли сте изложени някога на риск в интернет като кражба на парола или лични данни, обида от други лица или по друг начин?



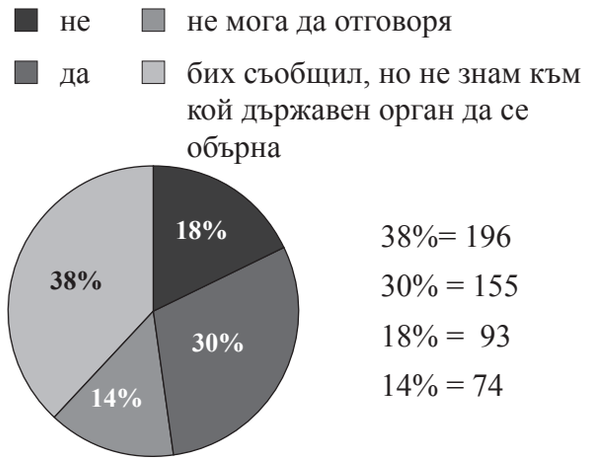
Отговорите на този въпрос трябва да заострят общественото внимание и да бъдат сигнална лампа за държавните органи. 75% от младежите са били вече обект на риск в интернет. Ако това се съпостави с отговорите на горните въпроси може да се направи извода, че българските млади хора са изключително уязвими.

12. Знаете ли към кой орган в държавата следва да се обърнете, ако считате че в интернет се извършва неправомерна дейност или се нарушават Вашите или на Ваши познати правата и интересите?



Група въпроси в анкетата бе свързана с това, доколко държавните органи, имащи отношение към киберсигурността, са разпознаваеми за младежите. Горният въпрос показва, че 60% не знаят кой орган е компетентен при рискове в интернет.

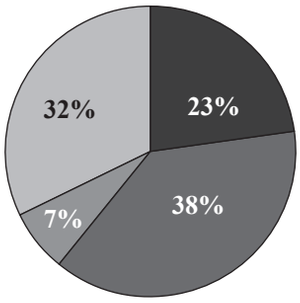
13. Ще съобщите ли на държавен орган, ако сенатъкнетенасайт,който пропагандира сексуално насилие, тероризъм или друга неправомерна дейност?



Интересно, е че младите хора имат нагласата да комуникират с компетентните държавни органи, когато става въпрос за рискове и заплахи в интернет. На този фон прави впечатление, че те не знаят към кого да се обърнат. Това е проблем на държавата, нейните органи и на образованието.

14. Ще споделите ли с Вашите родители, ако с Вас се свърже непознато лице чрез социалните мрежи и Ви предложи среща?

- не
- да
- не мога да отговоря
- не, но ще споделя с приятели

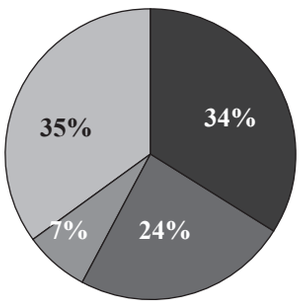


38% = 196
32% = 164
23% = 116
7% = 38

Повече от половината от младите хора не споделят определена информация с родителите си. Това трябва да заостри вниманието на обществото, тъй като връзката между родители и младежи е изключително важна за предпазване на млажежите от рисковете в киберпространството.

15. Споделяте ли в интернет:

- лична информация
- информация за свои навици
- служебна информация
- не споделям нито едно от изброените

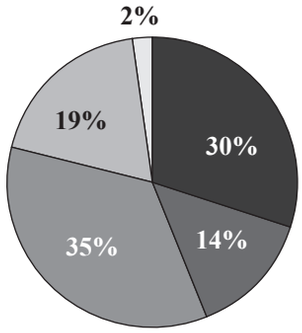


35% = 222
34% = 218
24% = 153
7% = 47

Отговорите на този въпрос показват, че има склонност към споделяне на определена информация, която може да осигури достъп на недоброномерени лица в интернет. Необходимо е да се информират младежите, че определен вид информация не следва да се споделя, за да бъдат те предпазени от рисковете. Това е въпрос на „култура“ на поведение в интернет.

16. Случвало ли Ви се е в интернет:

- непознат да Ви предлага среща и запознанство
- да Ви откраднат профил или парола
- да се натъкнете на лъжлива или подвеждаща информация
- непознати да Ви правят непристойни предложения
- да Ви предлагат да станете член на радикална или терористична организация

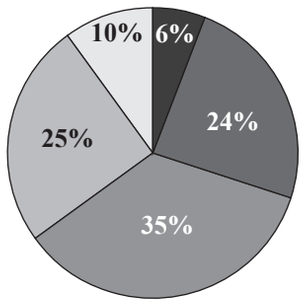


35% = 361
30% = 304
19% = 188
14% = 143
2% = 24

Въпрос 16 до голяма степен демонстрира вече установето по-горе, а именно че младите хора стават обект на различни рискове в кибер-пространството.

17. Чувствате ли сигурни при работа в интернет?

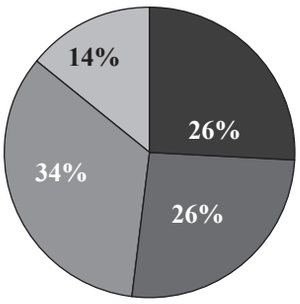
- не
- по-скоро не
- по-скоро да
- да
- не мога да отговоря



35% = 184
25% = 129
24% = 125
10% = 50
6% = 30

18. Вашите родители/настойници знаят ли какви сайтове посещавате и с кого общувате в интернет?

- не
- споделям само малка част
- споделям по-голяма част
- не мога да отговоря

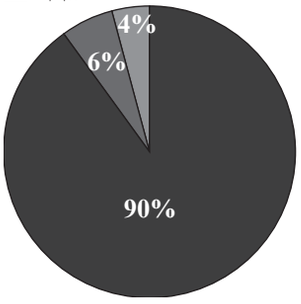


34% = 177
26% = 138
26% = 135
14% = 71

Този въпрос бе контролен въпрос за връзката между младежи и родители и той отново демонстрира, че тази връзка отслабва.

19. Качвате ли в социалните мрежи лични снимки с неподходящо съдържание?

- не
- вече не качвам
- да

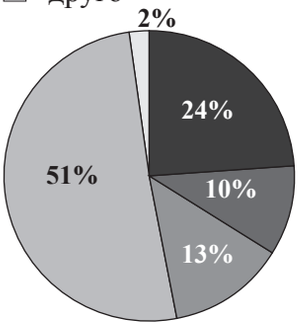


90% = 462
6% = 32
4% = 21

Въпреки, че съществуват младежи, които качват неподходящи снимки в интернет, огромната част от анкетираните отговоряят отрицателно. Един от начините да се повиши сигурността в интернет е именно като не се качва лична информация или снимки и материали с неподходящо съдържание.

20. Ако искате да намерите информация по интересуващ Ви въпрос, Вие преди всичко:

- ще попитате Ваши близки или приятели
- ще потърсите книга в библиотеката
- ще попитате учител/преподавател
- ще потърсите информация в интернет
- друго

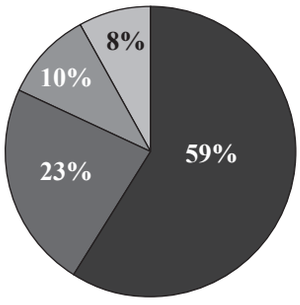


51% = 447
24% = 213
13% = 110
10% = 84
2% = 22

Интернет се превръща в основен източник на информация. Все по-малко младежите се обръщат към книги или към други хора. Това показва още веднъж, че трябва да се провежда целенасочено обучение с младежите, за да могат те по-добре да се ориентират във виртуалното пространство.

21. Използвате ли настройките за поверителност в социалните мрежи?

- да
- само ако се сетя за тях
- не
- не знам какво е това

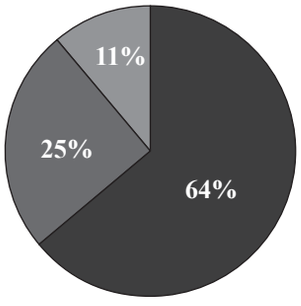


59% = 370
23% = 83
10% = 52
8% = 15

По-голямата част от младежите демонстрират добра култура на поведение, що се касае до технически аспекти на сигурността в интернет.

22. Ако се натъкнете на интересна и сензационна тема в социалните мрежи:

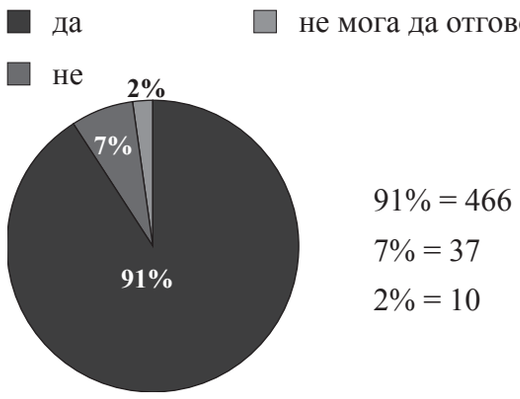
- ще я разгледам
- няма да я отварям, ако не ми е известен източникът
- не мога да отговоря



64% = 305
25% = 156
11% = 54

Известно е, че голяма част от вирусите се разпространяват като прикачени към интересни и сензационни материали. Потребителят, отваряйки подобна тема, даже не знае, че е станал обект на атака. На тази база, отговорите на горния въпрос трябва да ни покажат, че младежите не знаят за подобни опасности.

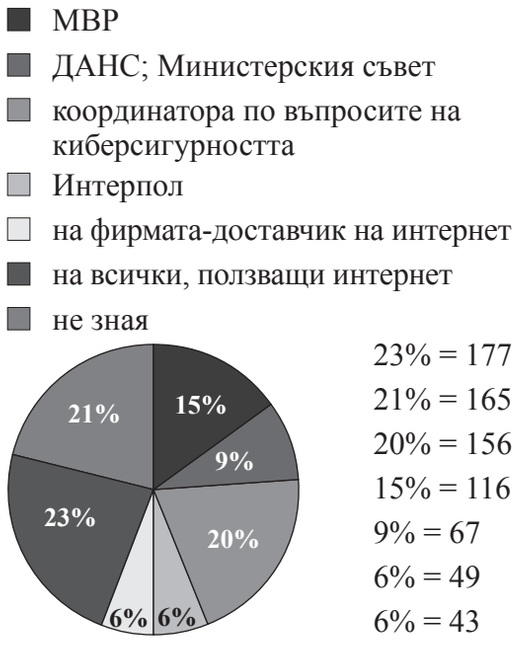
23. Имате ли инсталирана антивирусна програма ?



91% = 466
7% = 37
2% = 10

Отговорите на въпрос 23 показват добро познаване от страна на младите хора на това, че има начин за предпазване от рисковете и това са антивирусните програми.

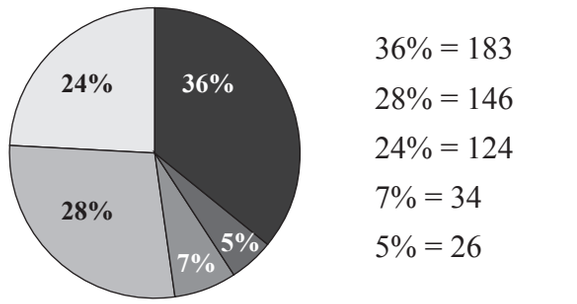
24. Сигурността в интернет е отговорност на:



23% = 177
21% = 165
20% = 156
15% = 116
9% = 67
6% = 49
6% = 43

Отговорите на горния въпрос още веднъж показват, че младите хора не разпознават държавните органи, ангажирани с въпросите на сигурността в интернет. Сигурността в интернет е ангажимент на всички, ползващи мрежата. Специално място имат държавните органи, които трябва да неутрализират рисковете, но младите хора не знаят кои са те. Почти 20% посочват като орган "координатора по въпросите на киберсигурността", какъвто не съществува в системата на държавното управление.

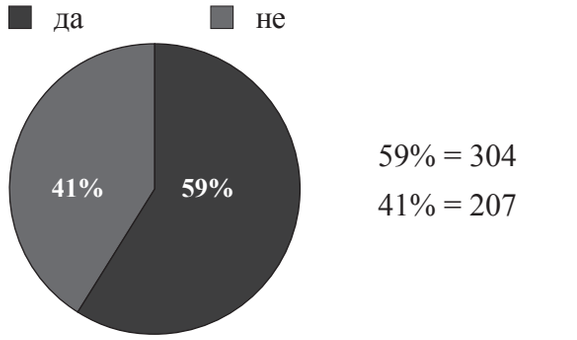
25. Ако намерите на улицата флаш-памет Вие ще я:



36% = 183
28% = 146
24% = 124
7% = 34
5% = 26

Почти 30% от младите хора биха проверили намерена флаш-памет за нейното съдържание. Известен е случай на проникване в секретни мрежи именно чрез този начин. Тези отговори показват, че младежите не са информирани за рисковете.

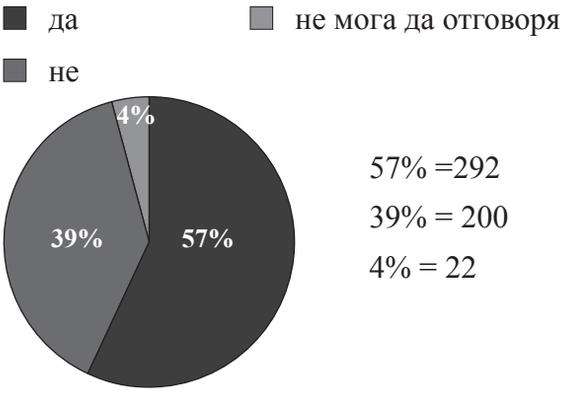
26. Обновявате ли редовно операционната система и софтуера, които използвате?



59% = 304
41% = 207

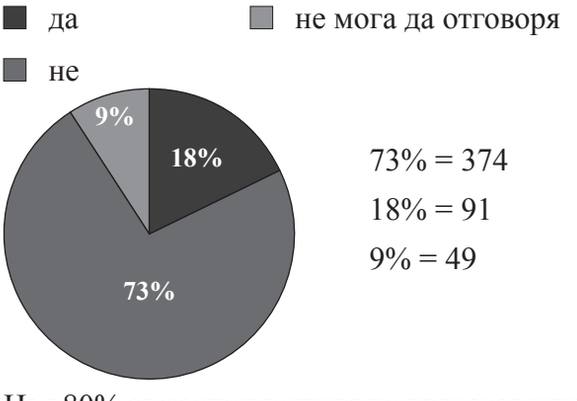
По-голяма част от младежите демонстрират добра "култура" на работа в интернет, но все още има и такива младежи, които са изложени на риск поради неосъвременяване на софтуера, който ползват.

27. Използвате ли различни (отделни) имейли за лична и служебна комуникация?



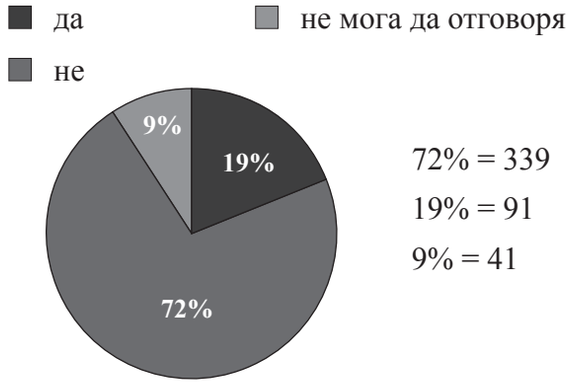
Много от рисковете са свързани именно с неразделянето на ползването на итернет за лични и за служебни цели. Голям е процентът на лицата, които ползват едни и същи имейли. Все пак следва да отчетем, че по-голямата част от респондентите са млади хора и не работят.

28. Проверявате ли сигурността на сайтовете, които използвате (напр. със SiteAdvisor или WhoIs.net)?



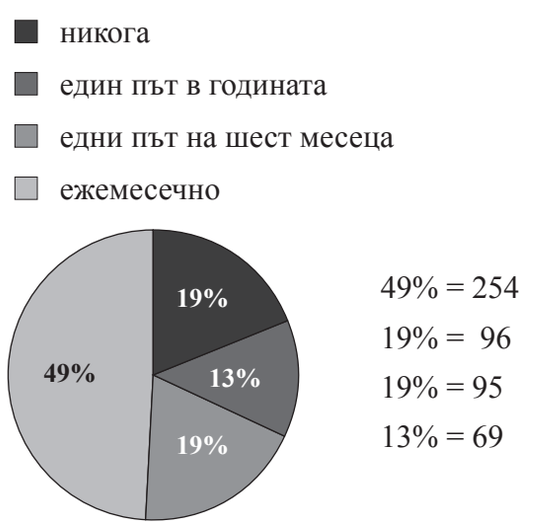
Над 80% от респондентите не познават или не използват възможностите за проверка на сайтове. Голяма част от киберпрестъпленията са резултат от това, че потребителите се насочват към фалшиви сайтовете, чиято цел е да изтеглят необходимата информация и да навредят на потребителите, основно във финансово отношение. Изводът, който трябва да направим от отговорите на този въпрос е, че е необходимо целенасочено обучение и запознаване на младите хора с възможностите да минимизират рисковете за себе си.

29. Проверявате ли получените прикачени файлове преди да ги използвате (напр.virustotal.com)?



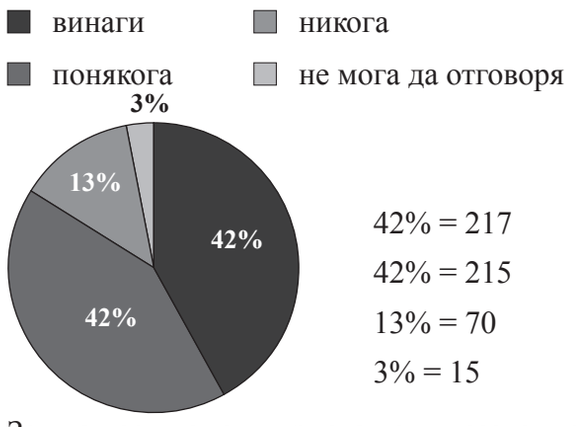
Този въпрос е още една демонстрация на написаното по-горе относно непознаването на възможности за предпазване от риск. От друга страна това може да бъде и резултат от неглижиране или от прекалена самоувереност у младежите, че няма да станат обект на риск. При всички положения, обучение е необходимо.

30. Колко често изчиствате историята за Вашето сърфиране и кеш паметта на браузъра?



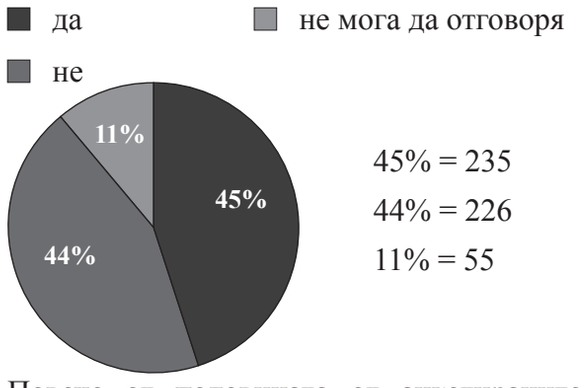
По-голямата част от респондентите „изчистват“ историята на браузванията, с което не позволяват да се определят техните интереси, или сайтове, които се посещават. Това е добър начин за предпазване от рискове.

31. Излизате ли от Вашия профил (изход/ LogOff), след като спрете да използвате услуги като електронно банкиране, Facebook, Gmail, Twitter?



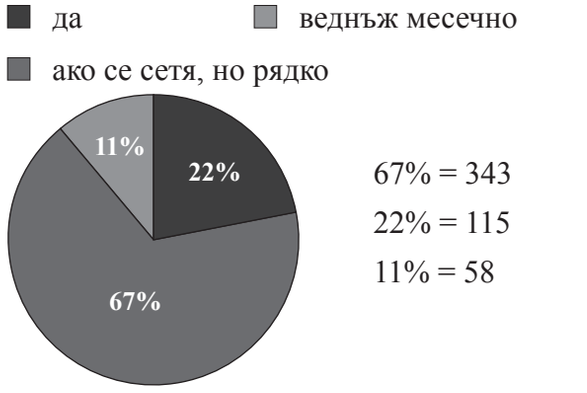
За да се намали риска от незаконно проникване е необходимо излизане от профилите. Все още голяма част от младите хора пренебрегват или не знаят за това.

32. Използвате ли еднакви пароли за достъп до различни приложения и електронни услуги?



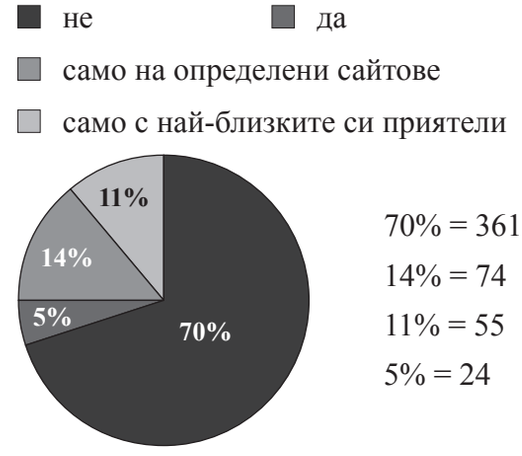
Повече от половината от анкетираните младежи не използват различни пароли, поради което могат по-лесно да станат обект на атака, като по този начин бъде застрашена важна информация.

33. Сменяте ли често паролите си?



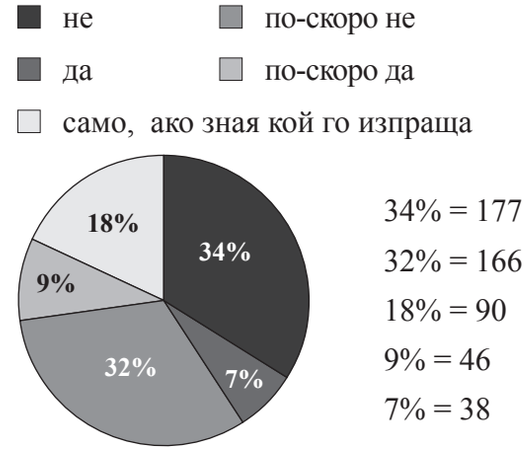
Почти 90% от отговорилите на този въпрос не изпълняват една от най-важните препоръки на специалистите, а именно за честа смяна на пароли, което е една от гаранциите за предпазване в интернет.

34. Разкривате ли личните си пароли с приятели и познати?



По-голята част от отговорилите показват добра култура на поведение в интернет по отношение на неразкриване на пароли.

35. Ще отворите ли файл, ако не сте сигурен за съдържанието му?



Отговорите на този въпрос са разпределени между различните възможности. Това показва, че като цяло младежите не са наясно и нямат ясно изграден начин на поведение.

36. Споделяте ли лична информация в интернет като име, парола, адрес, домашен телефон, училището, в което учите, семейна информация и т.н.?



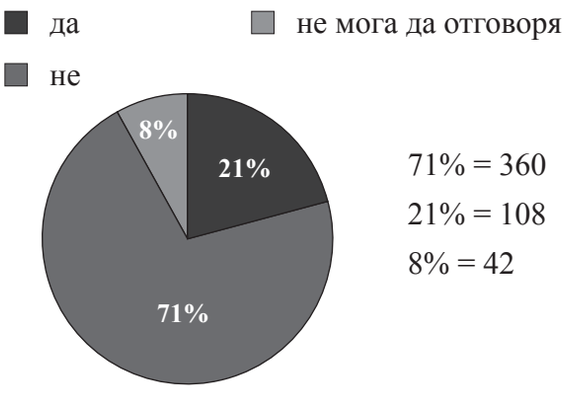
Над 60% споделят лична информация. Като правило лична информация не следва да се споделя в интернет. Въпреки това много от услугите, които ползваме в интернет, изискват споделяне на подобна информация. Ето защо е важно да се информират младите хора, кога и при какви обстоятелства може да бъде споделена лична информация.

37. Бихте ли приели да излезете на среща с непознат, с когото сте установили връзка чрез социалните мрежи



Отговорите на въпрос 37 трябва да заострят вниманието на обществото и най-вече на родителите. Почти 30% биха излезли на среща с непознат, ако "вдъхва доверие". Много от лицата с престъпни намерения в интернет създават фалшиви профили, така че целенасочено да заблудят младия човек, да му бъде "вдъхнато доверие", като възможност да извърши престъпление спрямо него. Необходимо е да се информират младежите за подобни опасности.

38. Съхранявате ли на Вашия компютър лични данни, пароли, ПИН-кодове и друга ценна информация?



Отговорите на въпрос 38 показват добра култура на поведение у повечето младежи.

39. Ако установите злоупотреба в интернет, Вие ще се обърнете към:



Отново отговорите на въпрос 39 демонстрират, че младите хора не знаят към кой държавен орган да се обърнат при риск в интернет.

Въпреки, че държавните органи, отговорни за сигурността в интернет, са неразпознаваеми за младите хора, младежите биха приели едно по-строго контролиране на интернет с цел повишаване на сигурността. Това показва, че въпросите на сигурността са високо в ценностите на младежите и те биха допуснали определена степен на контрол. Това проличава от отговорите на въпрос 40 по-долу.

40. Считате ли, че държавните органи трябва да контролират по-строго дейността на потребителите в интернет?



На базата на проучванията на отговорите може да се заключи, че интернет има важна социално-комуникативна и познавателна функция за младите хора. Те не само прекарват значително време в интернет, но и получават голяма част от знанията и познанията за човека и обществото.

Младите хора са запознати със съществуването на рискове в интернет и посочват като рискове широк спектър проблеми. Въпреки че са запознати с определени рискове, по-голямата част от младите хора не знаят как да се предпазят от тях. До голяма степен това е свързано с факта, че те не са били обучавани. Само една малка част от младежите отговарят положително на въпроса дали с тях е било провеждано обучение. По-скоро обучението се дължи на инициативи на отделни директори или учители или на дейността на неправителствени организации, но ясно показва липса на устойчивост и целенасоченост на този процес.

Липсата на адекватно обучение до голя степен обосновава факта, че повече от 60% от участвалите в допитването отговарят, че те или техен познат е бил изложен на риск в интернет. Необходимо е въвеждане на целенасочено обучение по въпросите на интернет. Това от само себе си не би могло да реши изцяло въпросите на сигурността на младите в интернет, но ще им даде познание за рисковете и как могат да се предпазят от тях.

В областта на сигурността в интернет, като се отчитат и характера на рисковете за младите хора, особено важна е връзката родители-младежи. На базата на проучването може да се направи извод, че тази връзка по отношение на това, доколко родителите знаят какво прави тяхното дете в мрежата, не е стабилна. По-голямата част от младите хора не споделят какво правят в интернет или споделят само малка част със своите родители.

Интересен е фактът, че младите хора виждат наличието на голям брой разнообразни рискове, но проблемът на тероризма, включително кибертероризма е посочен само от малък брой респонденти. Това още веднъж показва необходимостта от информираност на младежите. Различни групи по света използват интернет за набиране на терористи или за радикализиране на младите хора. Кибертероризмът е сред основните заплахи за съвременните държави и организации, като вече се говори и за кибер-войни.

Независимо от това, дали е провеждано обучение или не, повечето от младите хора демонстрират достатъчно висока култура на работа във виртуалната среда. Те имат понятие от най-общите мерки за сигурност, като използване на различни пароли и тяхната промяна, осъвременяване на софтуер, несподеляне на лична информация. Наясно са, че не следва да се качват снимки или материали с неподходящо съдържание.

В същото време, те са склонни да извършат сериозни грешки при работа в интернет. На въпрос дали намерена флаш-памет първо ще бъде проверена за съдържанието в нея, почти една трета отговарят положително. Впрочем, това е класически пример за заразяване на компютри с вируси. Подхвърлена флаш-памет да се подключи към компютър, което да активира вирусите. Ако младите хора бяха обучени, то те щяха да знаят рисковете от подобно поведение.

Интернет става все по-важна среда за запознанства на хора. Повечето млади хора са установявали подобни запознанства. В това по принцип няма проблем. Въпросът е дали зад дадения профил в интернет се крие същото лице, за което се представя. Много от младите хора са се натъквали на невярна и подвеждаща информация в интернет. Въпреки това, поти една трета от отговорилите на въпрос дали ще излязат на среща с човек, с когото са се запознали в интернет, казват че ще го направят ако човекът им "вдъхва доверие". Може би това обяснява и факта, че голя част от младите хора стават жертва на престъпление именно в следствие на подобни запознанства.

Проучването установи, че по-голямата част от младежите не са наясно кои са държавните органи, отговорни за въпросите на сигурността в интернет и не знаят към кого да се обърнат при необходимост. Това не е проблем на младите хора, а е по-скоро проблем на национално ниво. България все още няма стратегия за киберсигурност, съответно няма ясно разпределение на отговорностите и компетенциите на органите в тази област. Сигурността на младите в интернет следва да бъде част от общата стратегия за киберсигурност.

Повече от половината от младите хора считат, че е необходимо да има контрол върху интернет доколкото това би позволило да се осигури по-голяма сигурност.

С оглед на бъдещи дейности и политики могат да се направят няколко извода.

1. Необходимо е да се предприемат действия за обучение на младите хора за работа в интернет. Важно е създаването на култура на работа в тази среда. Най-удачно би било да се включат в училищното образование определени модули, съобразени с възрастта на учениците.

2. Да се приеме стратегия за кибер-сигурността на младите хора като част от общата стратегия за киберсигурност.

3. Да се работи с родителите с цел да се повиши родителския контрол върху ползването на интернет от младите хора.

4. Необходима е координация между държавни органи, бизнеса, неправителствения сектор и академичните среди за противодействие на рисковете в интернет.

ПРОУЧВАНЕ ЗА СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ

Мартин Чорбаджийски, Клаудия Чочулова

Настоящото проучване има за цел да обърне внимание на три ключови аспекта: какви са най-често срещаните рискове и заплахи за сигурността на младите в интернет, защо младите хора са особено застрашени в интернет и какви са практиките в някои европейски държави за повишаване на сигурността на младите хора във виртуалното пространство. Изследването е извършено от екип на Софийски форум за сигурност в рамките на проекта *„Сигурност@ на младите в интернет, предизвикателствата на киберсигурността“*, който се осъществява по Програма Еразъм+ , финансирана от ЕК и със съдействието на Центъра за развитие на човешките ресурси. Докладът се позовава не само на опита на отделни европейски държави, но и на различните инициативи, осъществявани на ниво ЕС. Направен и кратък обзор на практиките е и политиките в Република България, като се правят съответните изводи. В рамките на целия проект ще се изготвят препоръки за повишаване сигурността на младите в интернет.

РИСКОВЕ И ЗАПЛАХИ ЗА МЛАДИТЕ ХОРА В ИНТЕРНЕТ

Държавната комисия по сигурността на информацията използва следните определения за риск и заплаха, които ще приемем и ние за настоящото изследване. Заплахата е опасност, възможност за поява на нещо неприятно, лошо. Закана да се причини някому нещо неприятно, зло. При риска няма определено предварително време за настъпването му. Дори да бъде установен достатъчно рано, той си остава принципно невъзможен за неутрализиране[1]. Редица проучвания и проекти в областта на киберсигурността и сигурността обръщат внимание на следните рискове и заплахи за младите хора в интернет като най-сериозни и/или най-често срещани:

- *Порнография, сексуални престъпления и насилие*

Все повече млади хора биват излагани на този риск. Интернет все по-често се използва от потенциални и реални извършители на сексуални престъпления за подготовка на сексуални злоупотреби с деца, по-специално чрез сприятеляване с цел сексуална злоупотреба и детска порнография. Младите хора могат да станат жертва на т.нар. сексуални хищници, които в днешно време се насочват към социалните мрежи и примамват младежи, демонстрирайки привиден интерес към техните хобита, любими изпълнители, предавания и пр[2]. Така например педофили лесно могат да се доберат до лична информация- адрес, имена, профили, след което изпращат изображения и видео, които имат сексуално съдържание.

Порнографията и особено детската порнография е друг съществен риск, който може да има дълготрайно въздействие върху психиката на детето или тийнейджъра. Освен прякото негативно въздействие върху психиката и развитието на младите хора, сайтове с порнографско съдържание често крият зловреден софтуер, който атакува компютрите при разглеждане на тези сайтове.

Онлайн насилието също е вече широко разпространено и също може да има дълготрайни неприятни последици за младите хора, особено поради опасността от повтаряне на видяното

[1] „Рискове за интересите на Република България в областта на защитата на класифицираната информация, Държавна комисия по сигурността на информацията, с.3”, http://www.dksi.bg/NR/rdonlyres/5DB28C7E-7B2B-4DBE-894D-759B7329D913/0/Riskove_za_za6itata_na_KI.pdf (Прегледан на 08.09.2015г.)

[2] Kam, K., 4 Dangers of the Internet, page 3 - http://www.webmd.com/parenting/features/4-dangers-internet (Прегледан на 08.09.2015г.)

насилие.

- *Кибертормоз*

Кибертормозът е съвкупно понятие за действия, които могат да навредят на даден индивид в интернет и включват заплахи, злоупотреби, следене или друго агресивно поведение, което е продължително във времето. Кибертормозът може да включва обидни реплики, публикуване на снимки в интернет без разрешението на притежателя им, споделяне на видеоклипове, които могат по някакъв начин да накърнят достойнството и доброто име. Противодействието срещу тази заплаха е особено трудно, тъй като извършителят остава неизвестен, а често използва идентичността на своя жертва и извършва кибертормоз от нейно име (Kam, K., 4 Dangers of the Internet). Кибертормозът може да има дълбоки последици върху психическото състояние на детето или тийнейджъра.

- *Радикализация чрез интернет*

Разпространението на радикални идеи или призиви към радикални действия, насочени срещу отделни хора или групи е все по-често явление. Свидетели сме на разпространение на радикални идеологии, насочени срещу малцинствени или религиозни социални групи. Интернет позволява и бързата организация на неограничен брой хора за извършване на радикални противозаконни действия.

Появата на т. нар. Ислямска държава и засилването на други терористични групировки даде тласък на този вид заплаха и доведе до стартирането на интернет кампании за привличането на бойци и симпатизанти. Това става чрез различни мултимедийни материали или обещания за заплащане и просперитет. Използвайки интернет терористите се насочват най-често към деца и юноши от проблемни семейства, т.нар социални аутсайдери, маргинализирани младежи или имигранти и бежанци. Тази заплаха включва и десният радикализъм - дискриминация на мюсюлмани и други малцинства, което се превръща във все по-голям проблем.

Наред с радикалния ислямизъм наблюдаваме и ръст на неговото отрицания - антиислямския радикализъм, набиращ сила в много европейски държави.

- *Фишинг*

Това е широко използван похват от компютърни престъпници за получаване на важна информация. Те просто създават съобщения или интернет сайт, които "претендират", че са добронамерени, като приканват да се въведе важна лична информация. При фишинга измамници разпращат електронна поща, която претендира, че идва от почтена компания и се опитва да убеди получателя да даде важна лична или финансова информация. Електронното съобщение обикновено моли да се изпрати в отговор или да се въведете на уебсайт, към който има връзка. Тези данни, например потребителски имена, пароли и номера на кредитни карти, после се използват от измамниците, за да се получат пари или услуги от името на пострадалия[3].

- *Кражба на информация и използване на зловреден софтуер*

Кражбата на информация е сериозна заплаха, тъй като може да доведе до кражба на идентичността в интернет, в който случай крадецът се представя за своята жертва и по този начин безнаказано извършва престъпления /в реалното и във виртуалното пространство/. Ако не се вземат своевременни мерки (като например докладване за откраднат профил до компетентните органи или администратори на съответния уебсайт), престъпленията могат да се припишат на жертвата. Младежите често не обръщат внимание на последиците от споделянето на лична информация в киберпространството и пренебрегват декларациите за поверителност при използването на онлайн услуги. В съчетание с неприлагането на настройките за поверителност,

[3] „Фишинг", http://www.cybercrime.bg/bg/internet (Прегледан на 24.09.2015г.)

споделената от тях лична информация е лесна плячка за различни видове зловреден софтуер, като тя може да бъде директно откраднатa или да бъде изтеглена без знанието на нейния собствени/автор за това. Тази информация може да се използва за проникване в устройствата за достъп до интернет (компютър, лаптоп, телефон и др.) и така злонамерени лица да се доберат до още по-голямо количество информация като лични снимки, пароли за уебсайтове, кодове на кредитни и дебитни карти (особено ако детето/тийнейджъра и родителя използват едно и също устройство).

- *Кражба на самоличност*

Извършва се, когато някой използва личните Ви данни като име и фамилия, ЕГН, осигуровки, номера на кредитни/дебитни карти или друга идентифицираща Ви информация без Вашето знание и съгласие, за да извърши измама или други престъпления[4]. В много случаи кражбата на самоличност се установява изключително късно, когато са направени непоправими щети на личността или имуществото.

- *Игри, съдържащи насилие*

Сред младите все по-популярни стават видео игрите, които съдържат насилие. Същевременно те крият риска от приемането на виртуалната реалност за действителна и пренасянето на виртуалния свят в реалния. Това може да доведе както до проблеми в общуването и социална изолация, така и до опити за пресъздаване на виртуалните изживявания. Специалисти все повече отчитат, че игрите, съдържащи насилие, играят важна роля в радикализирането на младежите и приобщаването им към различни терористични и криминални групировки.

- *Онлайн финансови измами и други финансови рискове*

Все по-голям е броят на пазаруване и разплащане за различни услуги чрез интернет. Въпреки че големите компании обръщат сериозно внимание върху сигурността, не са изключени ситуации, при които хората попадат на неистински търговци. Рискът се крие в извършването на самата транзакция и постигането на различен от очаквания резултат - заплатеният продукт или не се получава, получава се в занижено качество или количество или лицето се оказва обвързан с нежелан абонамент, за който плаща повече. Примерите в това отношение могат да бъдат многобройни.

Сред другите финансови рискове следва да се отбележи незаконният хазарт, което може да се отрази негативно на семейния бюджет, може и да се пренесе в реалния живот като превърне младия човек в редовен посетител на казина или да доведе до неговата задлъжнялост в резултат на онлайн играта. Собствениците на хазартни сайтове физически се намират в офшорни зони; в резултат на това операторите могат да променят, преместват или напълно да отстраняват сайтовете си в рамките на няколко минути. Тази възможност позволява недобросъвестните оператори да вземат номера на кредитни карти, както и пари, депозирани в сметките на играчите, след което да закрият дейността си[5].

- *Хакерство сред младите*

Все по-популярна сред младите хора се превръща „професията“ хакер. Деца и юноши намират забавление и удоволствие, но най-вече усещане за предизвикателство при проникването в сайтове, кражбата на кодове, данни и пр. По този начин те се превръщат в част от проблема и излагат на риск свои връстници. В повечето случай това е невинна игра и не се получава сериозно увреждане на личността или собствеността, но има случаи на сериозни негативни последици.

- *Плагиатство*

Плагиатството е представянето на нечии мисли, идеи за свои собствени. Съществува целенасочено плагиатство, но в някои от случаите то е следствие от липсата на знания за правилата

[4] „При кражба на лични данни“ - http://www.cybercrime.bg/bg/internet/f04ff8/ (Прегледан на 24.09.2015г.)

[5] Незаконен хазарт - http://www.cybercrime.bg/bg/internet/3ad1da/

по използването и цитирането на чуждия труд. Последствията от плагиатството могат да бъдат изключване от образователни институции, съд или глоба. За да се предотвратят неблагоприятните последствия, младите хора трябва да бъдат запознати с правилата за използване на чуждия труд при техни разработки. Наблюденията показват, че това е изключително силно разпространено явление сред студентите, като повечето от тях не осъзнават или нямат информация, че неправомерното използване на чужд интелектуален продукт е престъпление.

- *Рискове при запознанства в интернет*

Рискът тук произтича от неспазването на определени правила, като например да не се споделя незабавно личната информация, уверение, че насрещната страна е такава, за каквото се представя (идентичността на другата страна, много престъпници скриват реалната си възраст, пол и намерения, възползвайки се от доверието на младите хора), срещата да се проведе на публично място, където има много хора и др.

- *Пренебрегване на правилата за онлайн комуникация*

Младите хора често не взимат необходимите мерки, за да гарантира своята сигурност при онлайн комуникация. Рискът е свързан с липсата на предпазливост, а донякъде и липса на култура за защита при онлайн комуникация. Това може да доведе до злоупотреба с лична информация, кражба на снимки, видео, нежелани контакти, попадане на неподходящо съдържание и др.

Изброените по-горе рискове са само една малка част от рисковете и заплахите в интернет. Интернет може да създаде рискове или чрез него традиционните рискове да се задълбочат. Ние считаме, че е необходимо да се засили общественото внимание към тези опасности. Те са многобройни и разнопосочни и същевременно се развиват бързо, еволюират и възникват все по-изобретателни методи, чрез които се застрашава сигурността на младите в интернет. Нека да не забравяме, че интернет създава изключителни възможности за получаване и обмен на информация, за извършване на различни дейности, които ни обогатяват или правят живота ни по-лесен, но в същото време той крие и рискове, които ние трябва да познаваме за да се защитим. Това се отнася най-вече до младите хора.

ЗАЩО МЛАДИТЕ СА УЯЗВИМИ

Опасностите, които интернет пространството крие могат да засегнат всички. Защо тогава младите са особено уязвими към тях?

Никога преди младите хора не са имали достъп до толкова много информация и до толкова различен набор от дейности на едно място. Може да кажем дори, че те „живеят“ в интернет. Независимо дали говорим за деца или тийнейджъри интернет е важна част от техния живот, а като такава много от представите им за света и живота могат да се оформят именно там. В интернет те общуват, споделят информация, запознават се с нови хора, градят социален имидж. От друга страна това, което се случва в интернет се отразява на живота им и преживяванията онлайн могат да имат ефект върху житейското им развитие. Младите хора са по-склонни към нови контакти, към нови запознанства, по-доверчиви са, а често не са запознати с рисковете, които интернет крие или с това как да гарантират своята безопасност онлайн.

Влошената семейна среда е един от факторите за уязвимостта на младите в интернет. Ако те не се разбират добре със своите родители, не споделят с тях своите преживявания и се стремят да ги държат напълно настрана от своя „живот“ онлайн, това повишава вероятността младите хора да бъдат изложени на рискове. В такива случаи самите те са по-склонни към рисково поведение, тъй като чувстват родителите далеч от себе си и отказват да чуят съветите им.

Социалната изолация е друг фактор, който допринася към уязвимостта на младите. Ако те не чувстват, че „принадлежат“ в училище, сред своите приятели и семейство, ако редовно са обект на нападки от свои връстници и търпят лошо отношение, те търсят утеха в интернет, където могат да общуват с напълно непознати хора, които не знаят нищо за тях. Тук отново стават по-склонни към рисково поведение и е по-вероятно да пренебрегнат правилата за сигурност[6,7].

Нека да вземем за пример тийнейджърите. Те са индивиди, които започват да изграждат свой личен живот и дълготрайни социални контакти, но имат стремеж да водят този живот независимо от своите родители. Всъщност това е процес, при който те търсят своето място в обществото и своята идентичност. В много случаи се сблъскват с обществени нагласи, които не им импонират. Получават се конфликти между установените принципи в обществото, от една страна, и желанието, амбициите на младежите, от друга. Голяма част от хората, които се радикализират го правят именно на тази основа – те се чувстват неразбрани, не намират място в обществото, не споделят неговите норми и смятат, че то ги потиска. Лица с престъпни намерения, използващи интернет, се възползват от това и атакуват именно тази част от съзнанието на младите хора, като се представят за приятели, разбиращи и симпатизиращи на намеренията и целите им, насърчаващи ги да не слушат родителите си. Постепенно, стъпка по стъпка, те печелят доверие, което улеснява извършването на избраното от тях престъпление.

Друга причина се състои в емоционалната уязвимост. Много деца и юноши се чувстват несигурни, особено когато са поставени в условията да заемат по-ниско социално положение сред своите връстници. Те често изпитват проблеми у дома, което поражда у тях нуждата да търсят тръпка, ново усещане, риск, какъвто може да е случаят при срещата с непознат от интернет. Около 30% от децата в ЕС имат контакти, с които са се запознали онлайн, а 23% от тях се запознават с пет или повече души. Девет процента от тези деца са се срещали на живо със свои онлайн познати[8] (Smahel, D. Helsper, E. J., Barbovschi, M. & Dedkova, L., 2012). От друга страна същият риск се отнася и за т.нар. „лидери” на социалните групи или „популярните“, за които статистиката показва, че рискуват запознанства на живо поради голямата си увереност[9]. Към списъка с причини следва да добавим и начина, по който в интернет се използва интересът на младите към игри, гатанки, предизвикателства и задачи. В много сайтове с игри често може да се открие зловреден софтуер, а една от тактиките на престъпниците включва привличане на вниманието чрез сложни задачи и загадки. В заключение по този аспект следва да отбележим, че причините за уязвимостта се крият както в самия живот, който младите водят, така и в степента им на запознатост със заплахите, които киберпространството крие.

ЕВРОПЕЙСКАТА ПРАКТИКА

Посочването на рисковете и причините за уязвимостта на младите в интернет логично води към следващия въпрос, а именно какви са добрите практики в справянето с тези проблеми. В Европа Държавите членки на ЕС са възприели различни подходи и прилагат многобройни решения, ето и някои от тях:

---

[6] „What can make young people vulnerable online”- http://parentinfo.org/article/what-can-make-young-people-vulnerable-online (Прегледан на 25.09.2015г.)

[7] „Vulnerable young people, social media and e-safety” - http://www.saferinternet.org.uk/content/childnet/safterinternetcentre/downloads/Research_Highlights/UKCCIS_RH_19_MPP.pdf (Прегледан на 25.9.2015г.)

[8] Smahel, D. Helsper, E. J., Barbovschi, M. & Dedkova, L., 2012 , „Meeting Online Strangers among European Children” - http://www.cyberpsychology.eu/team/storage/Smahel-2012-Bergen.pdf

[9] Ibid

В Латвия впечатление прави проектът Net-Safe[10], който препоръчва обучението на младите хора по безопасност в интернет да се съчетае с атрактивни за тях дейности. В сайта на проекта посетителите могат да свирят на пиано, да решават забавни и същевременно образователни тестове. Сред една от интересните и иновативни идеи е създаването на форум, в който младите могат взаимно да се образоват по въпросите на интернет безопасността, да споделят полезни идеи и информация, а също така и неприятни преживявания, от които техни връстници да се учат[11].

Доклад за рисковете и безопасността на младите в интернет във Франция показва, че ролята на родителите в страната е голяма и те са първият източник, към който младите хора се обръщат за помощ и съвети в интернет[12]. Словакия представлява интересен пример, тъй като един от основните рискове се крие в социалните мрежи, риск илюстриран от факта, че 81% от словашките тийнейджъри използват Фейсбук всеки ден. В социалните мрежи младите хора споделят твърде много лична информация и за тази цел е създаден интернет порталът Bezpečný /Безопасен/[13], фокусиран и върху елиминирането на заплахи за онлайн сигурността. Сайтът е посветен на деца и родители и съдържа различни практически съвети относно начина за справяне и избягване на проблеми в интернет. В съответствие с авторите на този уебсайт, публикуването на истинско име или фамилия, домашен / училищен адрес и публикуването на снимки може да доведе до физически нападения и тормоз. Обръща се внимание на „статусите" в социалните мрежи, описващи чувствата и дейностите на младите потребители като например приготвяне на багаж за почивка, чакане на летище, пристигане на определеното за почивка място. В резултат на това, са описани много случаи на домашни обири след споделянето на такава информация онлайн. Словашкият опит посочва още, че родителите трябва да са основният източник на информация, а незаинтересоваността им към проблема на онлайн безопасността сама по себе си представлява риск за техните деца.

От тази гледна точка почти всички проучвания и проекти в ЕС на тема безопасност и сигурност в интернет препоръчват родители и деца взаимно да разговарят по тази тема, а родителите да упражняват контрол в различна степен върху заниманията на децата онлайн. Препоръчват се също така съвместни обучения между родители и деца, които от ранна възраст да повишат своята култура на сигурност и така да се установи връзка на доверие между родител и дете по отношение на сърфирането в интернет. Редица проучвания, съфинансирани от институциите на ЕС, сочат, че според родителите някои от най-добрите практики в повишаване на интернет безопасността са обученията на децата и юношите в училище, по-достъпна и разбираема информация, която да запознае самите родители с рисковете, обучения и курсове за самите родители, които да бъдат организирани от правителствата, местните власти или НПО-та.

В Обединеното кралство се обръща сериозно внимание на мнението на младите хора по отношение на сигурността в интернет, което има принос към политиките, които се развиват в тази област и специфичните проблеми, които могат да възникнат. Акцентира се върху ролята, която училищата и университетите имат в запознаването на деца и юноши с въпросите за сигурността в интернет и е създаден специален сайт с практични съвети за организации различни от училища и университети, които работят с млади хора (вж. http://www.onlinecompass.org.uk/).

В Германия филтрирането на определено онлайн съдържание е нещо, зад което застават мнозинството родители. Много немски мобилни оператори са създали софтуер, посветен на

[10] „Net Safe Project" - http://www.canee.net/latvia/net_safe_project

[11] http://www.ebaltics.com/00704598

[12] Catherine Blaya and Seraphin Alava, Risks and safety for children on the internet: the FR report, page 56 http://eprints.lse.ac.uk/46442/1/FranceReportEnglish.pdf (Прегледан на 04.09.2015г.)

[13] Bezpečný Internet. (2015). Sociálne siete. Nebezpečenstvá sociálnych sietí. http://www.bezpecnyinternet.sk/ (Прегледан на 05.09.2015г.)

родителския контрол и същевременно са подписали различни кодекси, свързани със защитата при сърфиране от мобилни устройства[14].

Голямо е значението, което се отдава на различните инструменти за докладване, чрез които може да се реагира на неподходящо за деца съдържание. Такива инструменти трябва да бъдат максимално опростени, за да могат да се използват както от родители, така и от деца. Подчертава се и уникалната позиция, в която IT компаниите и интернет доставчиците се намират за развиване на интернет сигурността и помощта която могат да окажат на своите клиенти. Някои IT компании разполагат със специален софтуер за родители, който да ги запознае с опасностите в интернет или да им помогне при наблюдение на онлайн дейността на децата им.

Обект на фокус са и процедури, чрез които съществуващите закони по отношение на киберпрестъпленията се прилагат, като ЕС се фокусира върху сътрудничество на ниво държави членки и на глобално равнище, тъй като киберпрестъпленията често пресичат границите. В държави като Франция, Холандия, Великобритания и Швеция например вредите, нанесени на деца посредством онлайн контакти, са обект на наказателно преследване.

Европейският съюз взема мерки за подобряване на сигурността в интернет като насърчава саморегулацията и съвместната регулация на интернет пространството и неговата безопасност чрез публично-частно партньорство с IT компании, интернет доставчици и социални мрежи, които доброволно се ангажират с тази задача[15]. Тежестта на превантивните мерки срещу кибертормоза нараства все повече, тъй като голяма част от него се извършва от деца или тийнейджъри и затова е важно в училищата да се работи по този проблем и да се насърчава отделянето на повече време за децата днес, за да не се превърнат в престъпници утре.

Политиките на правителствено ниво трябва да дадат основната насока за развитието на сигурността на младите в интернет. Някои държави членки възприемат цялостни национални стратегии за сигурността на децата в интернет (Великобритания) , други залагат на институцията на омбудсмана за защита правата на децата (Унгария и Полша) или са създадени специални органи, които се занимават с предпазването на младите в интернет и сътрудничат тясно с органите на реда, медиите, мобилните оператори и интернет доставчиците.

В много европейски училища програмата за обучение по онлайн сигурност е съобразена с възрастта на учениците. Във Великобритания много деца се канят на форуми, посветени на онлайн рисковете и политиките за противодействие, за да дадат своето мнение, т.е. на тях се гледа като на активна заинтересована страна. Младите хора, успешно преминали обучения за безопасност в интернет се привличат за работа със свои връстници, които все още не са запознати с тези въпроси.

В ЕС голяма роля играят неправителствените организации, които често участват във формирането на правителствените политики и спомагат за засилването на международното сътрудничество по интернет безопасността.

Много полезен е опитът на мрежата InHope[16], обединение на различни неправителствени организации, които държат отворени горещи телефонни линии, чиято крайна цел е премахването на сексуалния тормоз над деца в интернет и сайтове с такова съдържание. Мрежата действа както на ниво ЕС, така и в глобален мащаб. Друга подобен източник е т.нар. мрежа Insafe[17], организатор

[14] Global Resource and Information Directory. (September, 3, 2014). Germany. Country Profile, para. 6- http://www.fosigrid.org/europe/germany (Прегледан на 02.09.2015г.)

[15] Safer Social Networking Principles for the EU, February 10, 2009- https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf (Прегледан на 10.09.2015г.)

[16] http://inhope.org/gns/home.aspx (Прегледан на 10.09.2015г.)

[17] http://www.saferinternet.org/ (Прегледан на 10.09.2015г.)

на Деня за безопасен интернет, който се провежда всеки февруари и се състои в различни дейности, промотиращи безопасността на младите хора в интернет. В мрежата Insafe си сътрудничат НПО-та, образователни институции, органи на реда, бизнес организации и родители. Европейският парламент е наясно с опасностите, които онлайн средата крие за децата и на интернет страницата InHope се акцентира върху подчертания от европейските депутати факт, че над 80% от жертвите в киберпространството са деца по-малки от 10 години. Ето защо ЕП положи усилия за приемане на резолюция относно безопасността на децата в киберпространството в началото на тази година. Сред конкретните стъпки, препоръчани в съответствие с инициативата на Европейския парламент[18] е снабдяването на Европол и националните правоприлагащи органи с необходимите средства, човешки ресурси, разследващи правомощия и технически възможности за сериозно и ефективно съдебно преследване, разследване и изправяне пред съд на извършителите на киберпрестъпления, разработване на нови високотехнологични способности, които да помогнат при анализирането на огромни количества изображения, свързани например с малтретирането на деца, включително материали, скрити в т.нар. „тъмна мрежа“ (Dark web), призоваване страните от ЕС, които все още не са транспонирали Директивата от 2011 г. относно борбата със сексуалното малтретиране и сексуалната експлоатация на деца и детската порнография в националните си закони да го направят.

Европейската стратегия за интернет сигурност препоръчва засилване на интернет сигурността на ниво местна власт и създаване на местни е-правителства, като се прилага принципът на продължителното обучение на служителите, тъй като поради бързите технологични промени, методите за измама се подобряват[19].

БЪЛГАРИЯ И ВЪПРОСЪТ ЗА СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ

В България все още не съществува стратегия, насочена към преодоляване на рисковете за сигурността на младите хора в интернет. Компетенциите в тази сфера са разпределени между различни държавни органи, но това е още една предпоставка да се размива отговорността.

Органите, които основно се занимават с въпросите на безопасността на децата в интернет е Държавната агенция за закрила на детето, Министерството на транспорта, информационните технологии и съобщенията, а също така и ГДБОП - МВР. Нека не забравяме, че основата в борбата с престъпленията, включително и тези, свързани с интернет, е превенцията. Добра практика в това отношение е сайтът cybercrime.bg, който освен всичко друго съдържа и полезни съвети към родители за безопасната работа на децата им в интернет. Тези съвети включват използването на интернет семейно, т.е. комуникация между дете и родител относно посетените сайтове, опасностите, които крият сайтовете за запознанства и др[20]. Дейност по въпроса за сигурността на младите в интернет извършва и неправителствения сектор, като сайта safe.teacher.bg, Фондация „Партньори - България“, а в страната също се провежда международният Ден за безопасен интернет[21]. Трябва да се отбележи дейността на Националният център за безопасен интернет, който обединява държавния сектор, бизнеса и неправителствени организации в опит да превърне интернет в едно по-безопасно място и да се предотвратяват киберпрестъпления. Друг пример от кампанията на Микрософт България „НетАларма“, в рамките на която ученици от гимназиите в

[18] „European Parliament calls for crackdown on online child sexual abuse” - http://www.inhope.org/tns/news-and-events/news/15-03-12/European_Parliament_calls_for_crackdown_on_online_child_sexual_abuse.aspx (Прегледан на 12.09.2015г.)

[19] European Internet Security Strategy, page 14 - http://cor.europa.eu/en/documentation/studies/Documents/european-internet-security-strategy-2013.pdf (Прегледан на 04.09.2015г.)

[20] „Съвети към родителите” - http://www.cybercrime.bg/bg/exploitation/aee587/ (Прегледан на 24.09.2015г.)

[21] http://www.saferinternetday.org/web/bulgaria/home (Прегледан на 24.09.2015г.)

цялата страна съставиха първия „Манифест за безопасен интернет“. Кампанията е осъществена със сътрудничеството на членовете на Детския съвет към Държавната агенция за закрила на детето и младежката асоциация “Български детски и младежки парламент”. Чрез своя Манифест, учениците не само споделят какво е важно за тях в Интернет, но и дават идеи за това какви етични и професионални норми е необходимо да се спазват от страна на потребителите[22].

По данни на Националния статистически институт около 83% от българските граждани на възраст между 16 и 24 години редовно използват интернет. Ако прибавим към тази цифра децата под 16 години, тогава цифрата може да скочи до 90%, както стана ясно на провелата се кръгла маса по въпросите на защитата на децата в интернет пространството, организирана от Министерството на транспорта, информационните технологии и съобщенията. От друга страна проучване, извършено за Европейската комисия от мрежата European Schoolnet и Университетът в Лиеж показва, че българските осмокласници са сред най-неуверените в ЕС по отношение на своята онлайн безопасност. Процентът на увереността обаче бележи растеж в 11 клас, като стига средното за ЕС ниво[23]. Основните рискове за младите хора в България са опасността от скъсване с реалността и пристрастяване към видеоигрите, манипулация следствие на онлайн запознанства, експлоатация на детски труд. Като мерки за противодействие на тези рискове се организират най-вече срещи с ученици, обучителни курсове за родители и различни рекламни кампании, целящи повишаване културата на сигурност в интернет.

Банковият сектор в България също е ангажиран със сигурността в интернет и в частност по отношение на електронното банкиране. На сайтовете на банките могат да се открият детайлни правила за сигурността при извършване на финансови операции онлайн, което е от особено значение за младите хора, които се запознават с онлайн услугите на банките. Сред най-важните препоръки са работа единствено с личен компютър, редовно обновяване на софтуера, проверка на страницата за интернет банкиране, която трябва да започва с http**s** (което означава, че сайта притежава специален сертификат за сигурност (SSL certificate или новият TLS certificate), гарантиращ, че връзката със страницата е кодирана, тази препоръка важи и за работа с всякакви други сайтове), въвеждане на допълнителни потребителски идентификатори под формата на кодове, чрез които извършената транзакция да се потвърждава с безплатен SMS, съхранение на такива кодове и друга чувствителна информация на физически носител, а не на компютъра или друго устройство с достъп до интернет.

Всички посочени по-горе мерки или добри практики в България са реализирани по-скоро като инициатива на отделни министерства или организации /основно неправителствени/. Прави впечатление липсата на единно виждане и политика в областта на защита на младите хора в интернет, която да обхване както обучението на самите млади хора, така и предоставяне на повече информация на всички лица и институции, отговорни за тяхното израстване. Естествено, трябва да има и ясна визия за ролята и мястото на държавата н този процес, защото интернет се само че дублира, но понякога и замества реалността, в която досега изцяло живеехме.

ИЗВОДИ

Младите действително остават най-уязвимата група в интернет. Те са склонни да възприемат нови неща много по-бързо от останалата част от населението, а същевременно са уверени в способността си да се справят с потенциални рискове. От друга страна интернет предоставя

[22] Ученици от цялата страна съставиха първия „Манифест за безопасен интернет” - https://www.microsoft.com/bulgaria/press/news_15122010.mspx (Прегледан на 25.09.2015г.)

[23] Survey of Schools, ICT in Education, p.104-105 - https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/KK-31-13-401-EN-N.pdf (Прегледан на 03.05.2015г.)

неограничени възможности за комуникация и информация, но паралелно с тази неограниченост съществуват рискове и заплахи, които се развиват много бързо (появяват се нови, старите се усъвършенстват), а техни жертви най-често стават именно децата и юношите. За да се преодолее тази уязвимост е необходим комплексен подход при формиране на политиките.

Семейството и образователните институции са най-близко до младежта и затова следва да имат водеща роля при запознаването им с опасностите в интернет. Това разбира се не би било достатъчно без усилията на държавата, която да даде насоките за гарантиране на киберсигурността и гражданския сектор, който да допринесе за развитието на тези насоки чрез своя иновационен капацитет. Банките, интернет доставчиците и IT компаниите са последната част от уравнението, която не може да се изключи. Чрез специфичната дейност, която извършват техният принос в повишаване на безопасността в интернет е безценен. Трябва да се даде възможност на младите да участват активно в този процес чрез участие в проекти и проучвания, които се фокусират върху киберсигурността и чрез възможността да споделят опит и идеи със свои връстници. В сравнение с повечето държави членки от ЕС България не работи достатъчно активно по сигурността на младите в интернет. Европейските държави залагат на публично – частното партньорство и отдават сериозно значение на комуникацията и взаимодействието между всички заинтересовани, отделят специално внимание на киберсигурността чрез създаването на стратегии, органи, организирането на продължителни обучения и изготвянето на специални препоръки.

Не бива да се забравяме и ролята на училището. Това е мястото, което следва да подготви младите хора за предизвикателствата на живота. Именно тук те трябва да се запознаят с рисковете в интернет. Отделянето на часове, посветени на безопасността в интернет в рамките на програмата по Информатика/Информационни технологии е от съществено значение за повишаване сигурността в интернет.

В България като цяло проблемите, свързани със сигурността в интернет се подценяват. Затова говори и фактът, че в България няма единен орган, който да се занимава с политиките и мерките в областта на киберсигурността. Все още няма и разработена стратегия за киберсигурност, въпреки че няколко поредни правителства си поставят нейното приемане като приоритет.

Отделни министерства и държавни органи са изградили способности за превенция на рисковете във виртуалното пространство, но това е по-скоро в резултат на реализацията на секторните политики, за които те са отговорни, но не и цялостна визия. Както редица европейски държави и България следва да създаде свой национален орган в областта на киберсигурността, който да гледа глобално на тези въпроси, необходимо е осъвременяване на законодателството и предприемане на конкретни практически стъпки в тази насока.

Като особено уязвима група, каквато са младите, държавните институция трябва да имат един по-широк поглед при информирането за рисковете и представянето на мерките, които младите трябва да предприемат за тяхната лична безопасност в интернет. Отделните инициативи на фирми и неправителствени организации са полезни, но сигурността на младите в интернет трябва да се превърне в устойчива държавна политика, а тъй като младежта е бъдещето на всяка една държава това ще е полезно и за цялото общество.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ

- Банка ДСК - препоръки за сигурност в интернет- https://dskbank.bg/Page/default.aspx?xml_id=/bg-BG/Individuals/dskdirectpersonal/.security/
- Фондация "Партньори-България" - Безопасно използване на интернет- http://partnersbg.org/2013/03/safe-internet/

- „Българските деца на възраст между 9 и 16 години използват интернет през мобилни устройства в ниво над средното за Европейския съюз.“- http://www.focus-news.net/news/2015/06/24/2083295/balgarskite-detsa-na-vazrast-mezhdu-9-i-16-godini-izpolzvat-internet-prez-mobilni-ustroystva-v-nivo-nad-srednoto-za-evropeyskiya-sayuz.html
- „Горнооряховски младежи преминаха обучение за справяне с формите на насилие онлайн и офлайн.“- http://www.helpline.bg/
- Децата не си дават ясна сметка за опасностите, които крие за тях И'нет
- http://computerworld.bg/25281_decata_ne_si_davat_yasna_smetka_za_opasnostite_koito_krie_za_tyah_inet
- „Децата рядко търсят помощ при проблеми онлайн“- http://www.safenet.bg/index.php?id=1391&art_id=16103
- Държавна комисия по сигурността на информацията, Рискове за интересите на Република България в областта на защитата на класифицираната информация.
- http://www.dksi.bg/NR/rdonlyres/5DB28C7E-7B2B-4DBE-894D-759B7329D913/0/Riskove_za_za6itata_na_KI.pdf
- Кръгла маса по въпросите на защитата на децата в интернет пространството, 18 май 2015 г.- https://www.mtitc.government.bg/page.php?category=700&id=8279
- Национален център за безопасен интернет.
- http://www.safenet.bg
- Обединена българска банка- правила за сигурност.
- https://ebb.ubb.bg/help/security_BG.html
- Помощ за вашата безопасност онлайн – Societe Genrale Експресбанк
- http://www.sgeb.bg/bg/byrzi-vryzki/sigurnost-v-internet.html
- Правила за сигурност и безопасност в Интернет- http://sacp.government.bg/deinosti/deca-info-obshtestvo/pravila-bezopasnost-internet/
- Сигурност на младите в интернет- http://safe.teacher.bg/html/etusivu.htm
- УниКредит Булбанк - препоръки за сигурност при работа с интернет банкиране
- http://www.unicreditbulbank.bg/weblayout/groups/bulbankwebsite/documents/bbproductdocument/bg_online_recommendations.pdf
- „5-те най-големи киберзаплахи за 2014-та“- http://www.security.bg/topnews/5-te-naj-golemi-kiberzaplahi-za-2014-ta
- Bezpečný Internet. (2015). Sociálne siete. Nebezpečenstvá sociálnych sietí.- http://www.bezpecnyinternet.sk/
- Gregussová, M., Drobný, M. (2013). Deti v sieti. Ako chrániť seba a naše deti na internete. - http://www.zodpovedne.sk/index.php/component/jdownloads/finish/1-knihy-a-prirucky/9-kniha-deti-v-sieti-2013-14?Itemid=0
- Anti-bullying- http://www.safenetwork.org.uk/help_and_advice/Pages/AntiBullying.aspx
- Children using internet from age of three, study finds http://www.telegraph.co.uk/technology/internet/10029180/Children-using-internet-from-age-of-three-study-finds.html
- Cyber Safety, An Interactive Guide to Staying Safe on the Internet
- http://www.opencolleges.edu.au/informed/cyber-safety/
- E-safety policy- http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/

esafety-policy

- EU Kids Online, Towards a Better Internet for Children- http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20III/Reports/EUKidsOnlinereportfortheCEOCoalition.pdf
- European Internet Security Strategy, European Union, April 2013.
- Global Resource and Information Directory. (September, 3, 2014). Germany. Country Profile- http://www.fosigrid.org/europe/germany
- InHope Annual Report- http://inhope.org/Libraries/Annual_reports/Inhope_Annual_Report_2013.sflb.ashx
- InHope. (March, 12, 2015). European Parliament calls for crackdown on online child sexual abuse - http://www.inhope.org/tns/news-and-events/news/15-03-12/European_Parliament_calls_for_crackdown_on_online_child_sexual_abuse.aspx
- Results of an Expert Survey on Matters of sSafer Internet and Youth Protection in Europe, Youth Protection Roundtable http://uploadi.safe.si/editor/1224568678YPRT_Survey_2007.pdf
- Risks and safety for children on the internet: the FR report- http://eprints.lse.ac.uk/46442/1/FranceReportEnglish.pdf
- Safer Social Networking Principles for the EU, February 10, 2009- https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf
- Smahel, D. Helsper, E. J., Barbovschi, M. & Dedkova, L. (2012) Meeting Online Strangers among European Children. Proceedings of the 15th European Conference on Developmental Psychology. Bologna, Italy, 419-422.
- Survey of Schools, ICT in Education- https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/KK-31-13-401-EN-N.pdf
- The Protection of Children Online http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf
- The Internet and Today's Youth: Protecting our Future- https://blogs.mcafee.com/executive-perspectives/the-internet-and-todays-youth-protecting-our-future/
- Vulnerable young people, social media and e-safety - http://www.saferinternet.org.uk/content/childnet/safterinternetcentre/downloads/Research_Highlights/UKCCIS_RH_19_MPP.pdf
- Wagener, V. (May, 13, 2015). Dangers that lurk on the Internet http://www.dw.com/en/dangers-that-lurk-on-the-internet/a-18448820
- What can make young people vulnerable online? - http://parentinfo.org/article/what-can-make-young-people-vulnerable-online
- „ 4 Dangers of the Internet"-http://www.webmd.com/parenting/features/4-dangers-internet
- https://en.wikipedia.org/wiki/Internet_safety
- https://www.microsoft.com/bulgaria/press/news_15122010.mspx
- http://www.ofcom.org.uk/
- http://www.saferinternetday.org/web/bulgaria/home
- http://www.saferinternetday.org/web/guest;jsessionid=166DDAEEBB283440677EA1AF49C1C604

ПРЕПОРЪКИ ЗА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ В КИБЕРПРОСТРАНСТВОТО

Наталия Николова

Комисия за защита на личните данни

Всеки ден милиони граждани по света използват глобалната мрежа. Банкирането от вкъщи, пазаруването онлайн и използването на социални мрежи е нормално ежедневие за много от нас. Изграждането на информа-ционната инфраструктура обхваща основните обществени сектори като икономика, енергетика, комуникации, но и такива дейности като услугите, които са от първостепенно значение за оцеляването на човека - доставка на храна, вода, здравеопазване и транспорт.

Всеобхватното приложение на информа-ционните технологии създава сложни взаимосвързани и взаимозависими мрежи. Потреблението на онлайн услуги нараства непрекъснато и те започват да придобиват съществено значение в съвременния свят.

Проблеми и предизвикателства

Новото поколение технологии поставят за отговор множество въпроси и основни предизвикателства:

- Запознати ли са потребителите със заплахите в мрежите?
- Как се използват личните данни от потребителите, от доставчиците на услуги и какви са параметрите за настройка?
- Кой от правна гледна точка е администратор и кой обработващ лични данни, както и кой каква отговорност носи?
- Как трябва да се организира отчетността на действията?
- Каква е границата между публичност и неприкосновеност?
- Каква е ролята на надзорните органи и какви са възможностите за съвместни действия и прилагане на общ подход на международно ниво?

Препоръки и възможни решения към администраторите на лични данни

С оглед на изложените по-горе проблеми и предизвикателства, решения могат да се търсят в следните посоки:

1. Необходимост от еднакво разбиране по отношение на това кой е администратор и кой обработващ данни при предоставяне на облачни услуги с оглед уточняване на техните права и задължения.

2. Повишаване на отчетността на обработ-ващите данни спрямо администраторите и задълженията за въвеждане от тяхна страна на технически и организационни мерки за защита. Това може да коригира наблюдавания дисбаланс при обработването в облак, при който клиентът (особено ако е малко или средно предприятие) може да изпита затруднения при упражняването на пълен контрол съгласно законодателството в областта на защитата на данни по отношение на начина, по който доставчикът извършва поисканите услуги.

3. Разпределението на отговорностите между администратор и обработващ да се уреди в договор, който да съдържа клаузи за защита на личните данни, и в който ясно да са разписани:

- задълженията на страните;
- правата на лицата (в т.ч. правна защита), както и гарантиране правото на достъп на физическите лица до техни данни, включително каква информация се обработва за тях и за какви цели;
- възможност за упражняване на контрол от страна на компетентния надзорен орган върху компанията, която предлага облачни услуги (администратор или обработващ);
- процедура, гарантираща „правото да бъдеш забравен“;
- срокове за задържане на данните;
- обвързването на подизпълнителите с клаузите по основния договор между администратор и обработващ;
- ясни правила по отношение съхраняването и процеса по заличаване на данните (не само изтриване на данните, но и заличаване от сървъра);
- процедура за уведомяване при наруша-ване сигурността на данните, както и за уведомяване на компетентния надзорен орган и засегнатите лица;
- описание на наличието на сървъри за поддържане на резервни копия на данните и тяхното местоположение, като към тези устройства следва да се прилагат идентични технически и организационни мерки за защита.

4. По отношение на изпълнителните правомощия, надзорният орган следва да може да проверява, както документацията и политиката по неприкосновеността, така и лог-файловете.

5. Необходимо е да се обърне специално внимание на проблемите, свързани с обра-ботването на бази данни и услуги, съдържащи така наречените „чувствителни данни“. Следва да се предвидят специални предпазни мерки, така че съобщаването, обработването и съхранението на данни извън националната територия да не изложи на неприемливи рискове сигурността и неприкосновеността на личния живот на гражданите, националната сигурност и икономика.

6. Да се работи в посока въвеждане на единни стандарти в областта на неприкосновеността на международно ниво и уеднаквяване на нивото на защита на личните данни между отделните страни. Това може да стане чрез разработването на международен правен инструмент.

7. Да се търсят възможности за по-задълбочено сътрудничество между отделните органи за защита на данните на оперативно ниво.

8. Компаниите да разработват ясна и разбираема политика по неприкосновеността и да се извършва оценка на риска.

9. Да се изисква категорично и информирано съгласие от субектите на данни във връзка с използването на техни лични данни, вкл. за целите на профилирането.

10. Да се използват подходящи техники за анонимизиране и псевдонимизиране на данните.

11. Да се гарантира по-голяма прозрачност и контрол върху процедурите по събиране и обработване на лични данни. Лицата трябва да получават информация относно вида на събираните данни, тяхното обработване, целите за които се събират и дали данните ще се предоставят на трети страни.

12. По-добро справяне с предизвикателства-та пред неприкосновеността чрез прилагане на механизма „неприкосновеност при проектиране“.

13. Прилагане на принципа на самоочетност на администраторите (accountability).

14. Повишаване на осведомеността на обществото.

Насоките за подобряване и развитието на защитата на данните трябва да обхващат обучение

на всички нива, дискусии, засилване на взаимодействието между специалистите (най-вече между юристи и информатици) и осъществяване на добро взаимодействие между всички заинтересовани страни на национално и наднационално равнище.

Препоръки за деца при работа в интернет

1. Не давай лична информация като име, парола, адрес, домашен телефон, месторабота и служебен телефон на родителите си или училището, в което учиш.

2. Не изпращай свои снимки или снимки на твои близки, без преди това да си обсъдил решението си със своите родители.

3. Винаги преди да качиш своя снимка и/или да публикуваш своя мобилен номер, помисли добре дали искаш и ще е добре ли за теб тази информация да стане достъпна за един неограничен кръг от хора.

4. Не приемай среща с някого, с когото си се запознал в интернет, без знанието на твоите родители. Ако те одобрят срещата, нека тя да е на публично и оживено място и задължително да е в присъствие на твои близки или приятели.

5. Не отговаряй на съобщения, които са обидни, заплашващи, неприлични или те карат да се чувстваш неудобно. Информирай родителите си или друг твой близък възрастен човек за такива съобщения и за техния източник.

6. Не отваряй приложения на електронна поща, получени от непознат подател. Те могат да съдържат вирус или програма, която да увреди твоя компютър или да черпи неограничено информация от него.

7. Внимавай, когато някой ти предлага нещо безплатно или те кани да се включиш в дейност, обещаваща лесна, бърза и голяма печалба. В тези случаи, най-вероятно, ще станеш жертва на измама.

8. Бъди внимателен и наблюдателен при попълване на регистрационните форми при извършване на регистрация в интернет сайтове.

9. При регистрации винаги проверявай има ли данни на сайта относно администратора/модераторите, които го поддържат, както и възможност за обратна връзка с тях – адрес за контакт.

10. Чети „Условията за ползване" на сайта, преди да се съгласиш с тях! Там трябва да бъде предоставена информация относно необходимостта и целта на събирането на лични данни на потребителя. В случай че такава информация не е предоставена и не ти е предоставена възможност да се обърнеш към администратора/модераторите на съответния сайт или в тях се съдържа информация, която те притеснява, то тогава сигнализирай на горещите линии, като подадеш оплакване. Трябва да знаеш, че всеки администратор/модератор, който поддържа конкретен сайт, е длъжен да даде информация относно това за какво са му необходими твоите лични данни, за какво ще ги ползва, за какъв срок, какво ще се случи с тях, когато те вече няма да са му необходими за тази цел, за която си му ги предоставил (например регистрация), както и на кого и поради какви причини той ще може да ги даде.

11. Не чети и не разглеждай сайтове, които съдържат материали с вредно или незаконно съдържание. Единственото нещо, което те биха могли да ти донесат са вреди, неприятности и проблеми. Няма нищо грешно и лошо в това, че от чисто любопитство, случайно или по съвет от „приятел" в нета си достъпил сайт с вредно или незаконно съдържание. Не се притеснявай да споделиш това с родител или друг твой близък възрастен човек. Именно той ще ти даде най-добрия съвет как да постъпиш в тази ситуация.

Какво означава „Сайт с вредно съдържание"? Това са интернет страници, чието

съдържание оказва или би могло да доведе да травмиращо психично въздействие или да подтикне техните ползватели към поведение, водещо до психични и/или физически травми.

Какво означава „Сайт с незаконно съдържание”? Това са интернет страници, на които е публикуван или качен материал, за който в закон е предвидена забрана и се носи съответната отговорност.

12. Използвай на максимум възможностите, които предоставя конкретният сайт за социални контакти за защита на твоя профил и информацията, която си качил на него.

13. Внимавай, когато разговаряш в чат, дискусионни форуми, социални мрежи и т.н. Помни, че хората онлайн често могат да се представят за такива, каквито не са. Важно е да знаеш, че възможността, която предоставя мрежата на теб да останеш анонимен или да се представиш за друг, се предоставя и на всички други участници в нета!

14. Нещата, които правиш в Интернет, не трябва да вредят на други хора или да противоречат на законите. Бъди вежлив и уважавай правата и достойнството на другите участници в интернет.

15. Консултирай се с родителите си, преди да свалиш или инсталираш нова програма на компютъра си. Не прави нищо, което може да увреди компютъра ти или чрез дадено действие от твоя страна да се разкрият данни за теб и семейството ти.

16. Споделяй с родителите си или с друг възрастен твой близък за начините, чрез които се забавляваш, информираш и научаваш нови неща от Интернет.

17. Бъди разумен и изобретателен при избора си на пароли. Помни: Паролите трябва да се променят периодично. Колкото по-дълго време използваш една и съща парола, толкова по-голям е рискът тя да бъде разкрита.

18. Използвай антивирусен софтуер. Обновявай го редовно и не забравяй да сканираш компютъра периодично.

19. В случай, че попаднеш на информация или други неща в Мрежата, които не ти харесват или те плашат по някакъв начин и нямаш възможност да го споделиш с родител или с друг възрастен твой близък, то тогава ти можеш да подадеш сигнал на адрес: http://web112.net/, http://www.safenet.bg/ или http://www.cybercrime.bg/bg.

Препоръки за родители

Посъветвайте вашето дете:

1. Да не дава лична информация като име, парола, адрес, домашен телефон, училището, в което учи, месторабота или служебен телефон на родителите си, както и друга лична информация за себе си, приятелите си, за вас, за братя, сестри или други роднини и близки без вашето или тяхно изрично разрешение.

2. Да не приема среща с някого, с когото се е запознал чрез социалните мрежи, сайтовете за запознанства, форумите, чат програмите или по друг начин чрез интернет, без вашето знание и съгласие. Трябва да знае, че един човек може да има няколко регистрирани профила и винаги може да се представи за някой друг. За това е необходимо отделяне на специално внимание към тази категория сайтове с оглед на сигурността на детето.

3. Да не отваря и да не отговаря на електронни съобщения/писма, получени от непознат подател, тъй като те могат да съдържат вирус или друга програма, която да увреди софтуера или хардуера на компютъра, както и да позволи безпрепятствен достъп до съдържащата се в него информация.

4. Да не отговаря на съобщения, които са обидни, заплашващи, неприлични или го карат да се

чувства неудобно и във всички тези случаи да ви информира за такива съобщения.

5. Да не изпраща свои снимки или снимки на свои близки, без преди това да е обсъдил решението си с вас. Обърнете му внимание, че публикуването на негови снимки или качването на видео в социалните мрежи и сайтовете за запознанства прави достъпни тези материали за огромен кръг от хора. Включването на уеб камера в реално време при разговор с непознат в чат програмите води до същия ефект. Лесният достъп до публикувани снимки или видеоматериали може да даде възможност на хора, които искат да му навредят, да ги използват по начин, който да го злепостави.

6. Да не се доверява на хора, с които се познава от и общува във виртуалния свят, да не споделя с тях свои или на близките си лични данни, които могат да бъдат от различно естество, но в своята съвкупност да доведат до идентификация на детето или на неговите родители, братя, сестри, приятели и др. Изострете му вниманието върху, това да не предоставя и да не публикува собственото си име или това на близки и приятели, адрес, данни за училището, в което учат, телефон /стационарен или мобилен/. Предоставянето или публикуването на името и адреса на дома и/или училището, в което учи, в интернет ще даде възможност на всеки, които има за цел да го открие в реалния свят, да го идентифицира и да стигне до него. Опасността, която крие предоставянето на телефонният номер, било стационарен или мобилен, може да доведе до телефонен тормоз от страна на злонамерени хора, както и да бъде използван от тях за злепоставящи действия и публикации в нета и извън него.

7. Да се консултира с вас винаги преди да свали или инсталира нова програма или друг софтуер на компютъра.

8. Да внимава и да се съобразява с правилото - нещата, които прави в Интернет, да не вредят на други хора или да противоречат на законите.

9. Да внимава, когато създава нови познанства и провежда разговори в чата - хората онлайн често се представят за такива, каквито не са.

10. Да споделя с вас начините, чрез които се забавлява, игрите, които харесва, и новите неща, които научава от Интернет.

11. Да пази паролите си, да не ги споделя с никого и да ги променя периодично.

12. В случай, че попадне на информация, която го плаши или го притесни по един или друг повод, да сподели това с вас или да подаде сигнал на горещата линия за безопасен интернет: http://web112.net/, http://www.safenet.bg/ или http://www.cybercrime.bg/bg, чрез предвидения за тази цел паник бутон.

Какво може да направите, за да се погрижите за безопасността на детето в интернет

1. Поемете лична отговорност за безопас-ността на детето си в Интернет.

2. Наложете правила за безопасно ползване на Интернет и следете за тяхното стриктно спазване.

3. Поставете компютъра в обща стая/помещение. Поставянето на компютъра в общо помещение ще ви даде възможност да станете „страничен" и „недосаждащ" свидетел на посещаваните интернет страници от детето, както и на всички извършени от него посещения, действия, дискусии и т.н. поне за периода от време, през който сте заедно.

4. Провеждайте периодични разговори с детето за опасностите, които крие интернет, и начините, по които то може да се защити. Обяснете му колко е важно да пази личните си данни и тези на своите близки, роднини и приятели и да не ги предоставя на „онлайн приятели", като

говорите с него свободно относно злоупотребите, за които могат да бъдат използвани те.

5. Създайте потребителски профил на детето си на компютъра в къщи. Децата трябва да имат собствени акаунти на компютъра. Това е много ефикасен начин за контрол на дейностите им в интернет. И още нещо: администратор на домашния компютър трябва задължително да бъде възрастен човек. Акаунта на детето задължително трябва да бъде без или с ограничени администраторски права.

6. Инсталирайте програма за родителски контрол - програмата за родителски контрол ще ви предостави възможност да ограничете достъпа на вашето дете до сайтове с неподходящо за него съдържание, да наложите времеви рестрикции за ползване на компютъра, да блокирате ползването на определени програми и т.н.

7. Прекарвайте повече време със своите деца, като:играете на предпочитаните от тях компютърни игри или разглеждате интересните за тях интернет страници - така ще разберете за навиците им, и за тяхното поведение в мрежата, за желанията и интересите им.

8. Сърфирайте заедно в Интернет и едновременно с това ги учите на безопасно и етично поведение в мрежата.

9. Станете приятел с детето си във виртуалния свят - направете регистрация в ползваните/ достъпваните от него електронни дискусионни групи, социалните мрежи, чат програми, които представляват форум за обмен на знания, информация, видеоклипчета, снимки, дискусии, създаване на нови запознанства и др. Това ще ви даде възможност да имате пряк поглед върху поведението на детето ви в мрежата.

СИГУРНОСТТА НА МЛАДИТЕ В ИНТЕРНЕТ
ЗАЩО МЛАДИТЕ СА УЯЗВИМИ В МРЕЖАТА?

докторант Атанас Людмилов Генчев

Факултет по педагогика на Софийски университет „Св. Св. Климент Охридски”

1. АКТУАЛНОСТ НА ПРОБЛЕМА ДНЕС.

Проблемът е особено актуален днес макар и интернет да съществува вече повече от четири десетилетия, поради две основни причини бурното развитие на информационните и комуникационни технологии и широкото им приложение вече в почти всички области на човешка дейност. Отдавна мина времето, когато мрежата се създава и използва с едничката цел за пренос на данни и комуникация между научни звена в затворена и защитена среда от малък брой хора и то научни работници. В нашето съвремие влизането в мрежата вече е нещо, толкова повсеместно и обичайно, колкото например „седенките” в селата преди повече от век. По данни[1] от националната статистика вече повече от половината 56,7 % от населението на страната имат постоянен достъп до интернет или това са 1 480 722 млн. души. В тези данни разбира се не се включват хората, които въобще са ползвали мрежата в живота си, което ще увеличи значително процентите. Широкото използване от всички и достъпността на всяка технология добавя и допълнителни рискове за злоупотреби с нея. Нека си припомним само един не много отдавнашен лозунг „Мирният атом - във всеки дом”[2], който в нашият случай и съвремие звучи „интернет във всеки дом.” В подкрепа на последното е съобщението на Европейската комисия за стратегията 2020, където сред основните инициативи на общоевропейско ниво на това десетилетие е „Програма в областта на цифровите технологии за Европа“ с цел „да бъдат постигнати устойчиви икономически и социални ползи от единен цифров пазар, който се основава на бърз и високоскоростен интернет и оперативно съвместими приложения, широколентов достъп до интернет за всички до 2013 г., достъп до по-високоскоростен интернет (от най-малко 30 Mbps) до 2020 г. и ползването на поне 50 % от европейските домакинства на интернет връзка от над 100 Mbps.” [1, с.17] Разбира се трудно е да се каже, че интернет действително не е вече във всеки дом въпросът тук е дали е достатъчно сигурен, колкото в началото на неговото създаване. Широкото използване от различни хора води и до все по-големите заплахи, които постепенно от реалният свят биват адаптирани и прехвърляни във виртуалното пространство, така вече почти всички опасности си имат и подобаващ виртуален вариант. Въпросът тук е ние успяваме ли успешно да се борим и неутрализираме тези заплахи както го правим в реалния живот или пренебрегваме виртуалното пространство. Фактът, че се създават антивирусни програми и друг защитен софтуер предпазващи от вируси, зловреден и шпионски софтуер, а също постепенно се създадоха и редица институции и специализирани звена за киберсигурност, говори за силата на заплахите и рисковете, които крие мрежата. Ако трябва отново да се върнем към стратегията 2020 и там ще открием загрижеността относно сигурността ни в мрежата „да насърчат използването на модерни, достъпни онлайн услуги (като например електронно правителство, електронен здравен портал, „интелигентен дом“, цифрови умения, сигурност).”[1, с.17] Ето защо необходимостта от обучение за сигурност в интернет е голяма особено сред най-уязвимите групи от населението, сред които са децата. Те от своя страна

[1] НСИ - http://www.nsi.bg/bg/content/2808/%D0%B4%D0%BE%D1%81%D1%82%D1%8A%D0%BF-%D0%BD%D0%B0-%D0%B4%D0%BE%D0%BC%D0%B0%D0%BA%D0%B8%D0%BD%D1%81%D1%82%D0%B2%D0%B0%D1%82%D0%B0-%D0-%B4%D0%BE-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82

[2] по вестник Работническо дело 1974 година по повод откриването на 1 блок на АЕЦ "Козлодуй" [12]

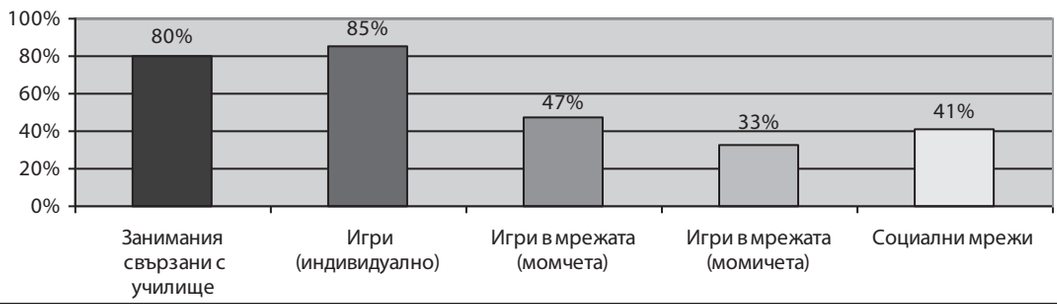
станаха може би и най-много прекарващите именно във виртуалната среда групи от населението, което допълнително усложнява нещата. Така например според статистика децата и юношите (9-16 години) в нашата страна по средно използване на интернет се нареждат на второ място след тези от Швеция[3]. Целите на използване на интернет, обаче се различава, според възрастта така както следва:

❖ „Децата между 5 и 8 години най-често използват интернет, за да пишат домашни, да търсят информация, да играят и да общуват с приятели."[9, с.5]

До последните 10-тина години, като че ли господстваше тезата, че в този възрастов диапазон интернет почти не се използва, или поне не чак толкова повсеместно и съответно на сигурността в интернет не се обръщаше особено внимание. Нещата обаче се променят, колкото по достъпни станаха технологиите (от гледна точка на цени, пазар, устройства, интерфейс) и колкото съдържанието в мрежата се увеличи и разнообрази, толкова повече се разшири и използването на интернет, но не само по брой хора от един и същи възрастов диапазон, а и се разпростря в различните възрасти, както по посока спадане на възрастта на използване, така и увеличаване на възрастта. Най-вече поради по-голямата възприемчивост и адаптивност на децата спадането на възрастта, от която започва да се ползва интернет се развива много по-бързо, от колкото в другия полюс на човешкия живот. За съжаление нашата статистика не отчита тази тенденция, в НСИ правят основната си статистика във възрастовия диапазон 16-74 години и изпускат голямата част от детския възрастов диапазон. Въпреки това тези тенденции се забелязват чрез отделни частни проучвания и по косвени пътища, чрез пряко наблюдение, чрез притежаваните от семействата устройства с възможности за интернет връзка (най-вече таблетите и телефоните). Ето защо трябва да се обръща повече внимание на киберсигурноста още в този възрастов диапазон.

❖ Децата на възраст 9-12 години вече разнообразяват целите на използване на интернет като добавят и игри и ползване на социалните мрежи. Игрите в мрежата и социалните мрежи повишават риска от опасностите намиращи се във виртуалното пространство, не че търсенето на учебни материали и информация е по-малко застрашаващо, (като се има в предвид, че вирусите и различните шпионски и зловредни програми биват закачвани и на подобни места, но поне липсват сериозните рискове криещи се зад чата, зад непознатите в социалните мрежи, форуми, онлайн игрите и залаганията, които са със съществено по-тежки последици при попадането им за децата).

Диаграма №1: Цели на използване на интернет на децата във възрастовия диапазон 9 - 12 години[4]

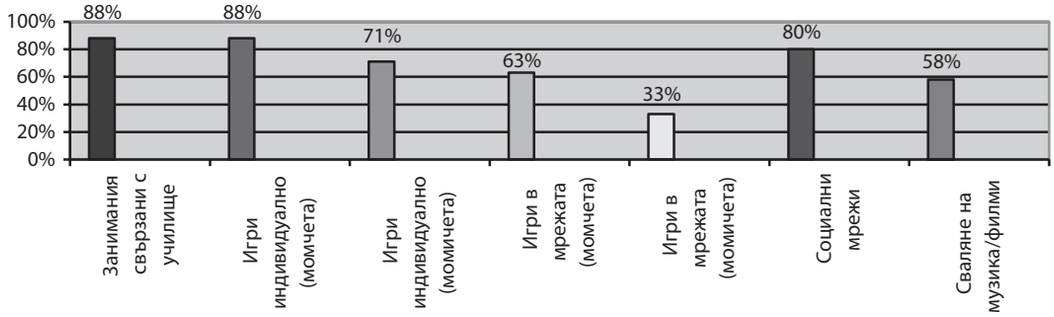


[3] по данни от европейското изследване EU Kids Online
http://www.safenet.bg/images/sampledata/Materiali/Mladite_hora_mezhdu_virtualnoto_i_realnoto.pdf

[4] по данни от европейското изследване EU Kids Online
http://www.safenet.bg/images/sampledata/Materiali/Mladite_hora_mezhdu_virtualnoto_i_realnoto.pdf

❖ Децата на възраст 13-16 години още повече разнообразяват целите на използване на интернет като добавят нови, но и препреоритезират старите. Така например използването на интернет с цел общуване през него се увеличава почти двойно, скачат и другите две цели „игри" и „занимания свързани с училище", но ръста при тях е много по-малък. Според проучване[5] в нашата страна 90 % от тийнеджърите ползват интернет.

Диаграма №2: Цели на използване на интернет на децата във възрастовия диапазон 13 - 16 години[6]



Според друго едно проучване „средно 2000 деца в Европа годишно стават жертва на насилие в интернет."[2] на фона на това в българските училища едва „от 5-и клас има редовни часове по информационни технологии, но по темата за безопасност са предвидени само 2 часа годишно, в които се говори главно за компютърната безопасност, т.е. за вирусите." [2]

Ето защо и опасностите и рисковете за киберсигурноста също се увеличават, тъй като децата, а също и тиинйджърите навлизат в силно уязвими и все по-предпочитани виртуални територии от престъпността като социалните мрежи, чатовете. Като добавим и новопоявилата се тяхна (на тийнеджърите) цел на използване „сваляне на музика/филми", от където са още по-уязвими те, както по направлението относно съдържанието им, така и по направлението на проблемите свързани с авторските права и други, така картината става още по-усложнена.

Всичко казано по-горе показва актуалността на проблема в нашето съвремие, че с широкото навлизане на новата реалност, навлизат както множеството от възможностите и удобствата й, така обаче и рисковете от злоупотреби и престъпност. С опасностите, „капаните", които стоят пред децата ще се запознаем в по-следващата точка, сега нека се запознаем с възрастта, от която е най-необходимо да започне едно такова обучение по киберсигурност.

2. КАКВА ДА БЪДЕ ВЪЗРАСТТА И ПРОГРАМАТА ЗА ОБУЧЕНИЕ?

Един от най-важните въпроси е може би този за възрастта, от която трябва да започва едно обучение по киберсигурност на децата. Важен е поне поради две основни причини едната е да не остане необхванатата възраст на деца използващи вече новите технологии и интернет и втората е да се види какво трябва да бъде подходящото съдържание, методика на обучение, което както се разбира ще бъде различно за различните възрастови диапазони. И така от първата ни точка стана ясно, че използването на интернет става от все по-малка възраст, което довежда до обръщане на

[5] Онлайн тормозът наръчник за учители
http://bul.tabby.eu/10481079109010771075108311031085107 7-10851072-10731088108610961091108810721090107 2.html

[6] по данни от европейското изследване EU Kids Online
http://www.safenet.bg/images/sampledata/Materiali/Mladite_hora_mezhdu_virtualnoto_i_realnoto.pdf

вниманието на един особено важен фактор, развитието на човешката психика и интелект. По този въпрос може да се каже следното: недоразвитието на психическите структури във възрастовите периоди преди 16-18 години е научен факт. Според една от теориите на възрастовата психология „Формалното мислене се развива през юношеския период. Противоположно на детето, юношата е индивид, който разсъждава без да се свързва с настоящето и изгражда теории, чувствайки се добре във всички области… Характерно за юношеството е рефлективното мислене и се заражда хипотетико-дедуктивно мислене.” [10, с.82] или казано с други думи след възрастта от 16 г. се счита, че интелекта и повечето психически структури са изграден в голямата си част и степен. Това означава, че децата са особено уязвими във виртуалното пространство поради това, че не могат сами и в достатъчна степен да преценяват рисковете на виртуалното пространство, те трудно отделят личното от публичното пространство, а любопитството, което е водещата по принцип опознавателна сила ги прави в този случаи и особено непредпазливи. Тоест според логиката на възрастовата психология, с която в голяма степен се съобразява и педагогиката, колкото са по-малки децата, толкова са и по-уязвими, тъй като са и по-недоразвити, а от там и по-неподготвени. От всичко казано до тук може да се отговори на въпроса от каква възраст да започнат обученията за киберсигурност на децата по следния начин: от възрастта, от която започнат да използват интернет, тоест това трябва да бъде един паралелен процес, а не догонващ, запознавайки се едно дете с технологиите, с които си играе или му помагат, то трябва да се запознава по подходящ начин и с опасностите, които могат да носят след себе си тези технологии. След като според вече цитираните данни в точка първа стана ясно, че децата започват да използват интернет на 5-8 години значи и тогава трябва да има часове, занятия и игри, които да информират и създават навици у тях. Понеже за този възрастов период те се намират в предучилищна детска градина или в първи, втори клас значи именно тогава трябва да се въведе и обучението на децата по киберсигурност. Подобно на обучението им за безопасността в реалността при пресичане на улици и кръстовища и въобще за правилата за движение по пътищата.

По отношение на методологията за обучение тя освен, че трябва да бъде съобразена с възрастта на децата трябва да бъдат засегнати и най-важните, най-актуалните проблеми, опасности свързани с ползването на интернет, както и техните възможни решения и препоръки за тяхното ограничаване и избягване.

Трябва да бъде достатъчно актуална за добро или за лошо тази човешка сфера на дейност – информационните и комуникационни технологии е бързо развиваща се в порядъка на месеци, дори може би не можем да кажем година, което ако не бъде съобразено с учебните програми би било много голяма грешка.

Ето защо проучването на актуалното състояние за вирусите, зловредния софтуер, измамите (и като цяло опасностите) и възможностите за осигуряване на киберсигурноста е необходимо условие за успеха на програмата. Необходимо е и проучване на интересите и целите на използване на интернет от децата и тийнеджърите, което също да бъде непрекъснато актуализирано с цел да не остава непозната територия от една страна и от друга да не се получат разминавания.

Важно е да се спомене, и че една подобна учебна програма трябва да бъде изготвена съвместно от педагози, психолози, IT специалисти, експерти по киберсигурност. В малките класове и в предучилищна възраст може да бъде добавена подобна учебна програма като отделни часове в предмета труд и творчество например, докато в горните класове тя ще си влезне в предмета информационни технологии и информатика.

Основни теми в една програма за обучение във връзка с киберсигурноста, може да послужи и съдържанието на настоящият доклад и особено точките свързани с опасностите, „капаните” в интернет, ролята на учителите и препоръките, съобразени според възрастовите особености

на децата и тийнеджърите. Но това е само началото, базата, на която може да се стъпи при обсъждането на една цялостна методика.

3. ОПАСНОСТТА И "КАПАНИТЕ" В ИНТЕРНЕТ ДЕБНАТ ДЕЦАТА И ТИЙНЕДЖЪРИТЕ НЕПРЕКЪСНАТО.

Поради множеството възможности, които предлага интернет като слушане на музика, гледане на филми, игрите, споделяне на различно мултимедийно съдържание, виртуални среди, блоговете, сайтове за запознанства, форумите, интернет библиотеките, удобството от улеснен и независим от време и място начин за комуникиране между хората, взаимодействието в различни процеси, а не само пасивността на потребител той (интернета) притежава особена притегателна сила за младите хора и особено за децата и тийнеджърите.

Много често обаче тази привлекателна страна на интернет и виртуалното пространство се възприема като единствена, но не бива да се пренебрегва факта, че те имат и тъмна страна, която за съжаление е невидима особено за децата и тийнеджърите. В тази тъмна страна се крият редица опасности, „капани" за живота, здравето и нравственото развитие на децата и тиинйджърите.

Основните, от които са:

- ❖ нарушаване на социалната перцепция[7] и сензитивноста в следствие на дългото и постоянно общуване през мрежата, чрез социалните мрежи;
- ❖ нарушаване на социалната интеграция на децата и юношите отново поради дългото и постоянно общуване и стоене в мрежата.

Тези две опасности са по-скоро функционални в смисъл от прекомерната употреба на технологията, отколкото от съдържанието, което самата технология предлага. Споменаваме ги тук, тъй като не малка част от капаните, в които попадат децата и юношите в интернет от съдържателна гледна точка са силно повлияни от тези две опасности. Например поради нарушената си социална перцепция и сензитивност децата и тийнеджърите трудно могат да разпознават скритите сигнали, които може да им подаде непознатият човек, с когото си пишат за истинските му намерения. И още един пример поради нарушената си социална интеграция, поради ограниченото си общуване в реалния свят детето или тиинейджерът това общуване го замества с търсене на множество контакти във виртуалното пространство, където заедно с това намалява и бдителността и започва да търси повече и повече „приятели", които подобно на първия пример не винаги са им известни истинските намерения свързани с това общуване. В тази връзка също децата и тийнеджърите могат да се подмамят към различни нетрадиционни и дори забранени от закона групи и организации.

Други опасности в интернет по-голямата част, от които в основата им лежи съдържанието са:

❖ Онлайн-тормозът[8], който се определя като - „използване на информационните и комуникационни технологии за преднамерено въвличане в повтарящи се или широко разпространени прояви на насилие и нанасяне на емоционална вреда, насочени към други хора. Възможно е жертвата на това поведение да не знае кой е извършителят, макар че при половината от случаите това е известно. Не всички форми на онлайн-тормоз са еднакво тревожни и опасни. Общуването с човек, който не стои пред вас и не е на другия край на телефонната линия, улеснява изразяването на идеи и мисли, тъй като липсват угризения и чувство на разкаяние в резултат

[7] Социалната перцепция „се отнася до процеса на възприемане на социалната реалност, до това как, защо, по какъв начин възприемаме социалните обекти." [6, с. 291]

[8] „Терминът „онлайн-тормоз" за първи път е използван и дефиниран от Бил Билси, канадски педагог с много съществен принос към системата на образованието." [9, с. 5]

на пълното разбиране на отрицателното въздействие на думите и действията. Това се дължи на факта, че човекът, който проявява определен тип поведение, не вижда своята жертва и самият той също остава скрит и в крайна сметка увеличава риска и опасността от дадения тип поведение.” [4]

Онлайн-тормозът се поделя и на различни видове, сред основните са:

- ❖ **flaming** - агресивни нападки в интернет, при които се използва обиден и вулгарен език;
- ❖ **harassment** - обидни послания и индиректни заплахи;
- ❖ **denigration** - изпращане или разпространяване на унизителни слухове за определен човек с цел да се увреди доброто му име;
- ❖ **exclusion** - изключване от виртуална група;
- ❖ **impersonation** - извършителят се представя за друго лице, като по този начин го поставя в опасност или опетнява името му;
- ❖ **outing** - разкриване на тайни и друга лична информация;
- ❖ **trickery** - подмамване на някого в интернет с цел получаване на информация, която после бива разпространена;
- ❖ **cyberstalking** - онлайн-преследване - обсебващо и продължително шпиониране и контролиране на чужди действия в интернет;
- ❖ **онлайн-заплахите** представляват или директно отправени заплахи или „притеснителен материал” - общи твърдения, които създават впечатлението, че авторът е емоционално нестабилен и вероятно обмисля да нарани някого, дори себе си или да извърши самоубийство.”[4]

❖ Следваща опасност е прекомерната лична[9] и дори компрометираща информация, която се качва в различните социални мрежи и платформи. Децата и особено тийнеджърите с цел да се изпъкнат, покажат или похвалят пред своите близки, приятели и познати качват различни техни снимки, клипове и друга лична информация, която обаче може да се окаже доста рискова, както към момента на качването й (например да се използва за подигравки от съученици и приятели, от непознати с престъпни цели, за създаване на фалшиви профили и т.н.), така и след години когато те дори най-малко очакват, все пак интернет е една огромна база от данни, която съхранява много често неща дори когато са премахнати от нас (например при качени компрометиращи снимки в социалната мрежа като тийнеджър, които към онзи момент не са били от голямо негативно значение, то след 4-5 години, когато същият този тийнейджър е пораснал и си търси работа едни такива снимки биха му попречили доста, „…по - добрия виртуален имидж може да е пагубно в даден момент за вашата кариера… вероятността работодател да се натъкне на любопитни факти за свой служител или кандидат за работа става все по – голяма, особено ако компанията знае как да търси.”[5, с. 6]

❖ Следваща опасност са зловредни приложения и измами, тук може да се включат, както шпионският софтуер, така и този, с който източват информацията от компютрите и другите устройства от мейлите и акаунтите в различните сайтове. Освен източващи има и достатъчно софтуер, който блокира или унищожава информацията, това може да доведе до изгубване на важна информация особено когато децата и тийнеджърите ползват споделено компютър или устройство, което техните родители ползват и служебно. Друга група зловредни програми са свързани с измамите източване на кредитни карти и банкови сметки, продажба на некачествени или нереално скъпи продукти и други подобни.

[9] „Още при първия контакт с непознат в интернет над половината от децата (58%) споделят истинското си име, а 36% показват своя снимка или видео в реално време, сочат данни от специално проучване на НЦИОМ.”[2]

❖ Следваща опасност са подлъгващите[10] незаконни кампании и организации в интернет. Те не се различават почти по нищо друго от реалните техни варианти единственото е, че се реализират и набират хората посредством мрежата. Тук се причисляват многото и различни кампании свързани с лъжливо представяне на лични проблеми на хора, които набират средства, кампании за омраза на етническа, религиозна и друг тип основа. От организациите такива са различните видове секти, терористични, религиозни и други подобни, които се опитват да примамят като свои членове именно деца и/или тийнеджъри, тъй като са най-лесно податливи на пропаганда, маниполации и вярвания.

❖ Трафика на хора като следваща опасност. Това е една опасност подобна на предните две, която е сред тези които и в реалността се развиват, но превзе и територията на виртуалното пространство. Опасност, която е причина хиляди деца да изчезват или да бъдат въвлечени в престъпни схеми.

Част от описаните по-горе опасности са представени като „капани" в Наръчник за учители. Младите хора между виртуалното и реалното. Разработване и прилагане на казуси в учебна среда, които изглеждат по следният начин:

➢ **Ти не можеш да ме видиш**: идеята за невидимостта и за възможността да останеш анонимен премахва всички притеснения от евентуално разпознаване, което би могло да доведе до неодобрение или наказание.

➢ **Аз не мога да те видя**: липсата на осезаема обратна връзка относно последствията от действията в интернет върху другите или върху самия извършител служи като пречка пред изпитването на истинско съчувствие и признаването на факта, че извършените действия причиняват вреда и носят лоши последствия.

➢ **Кой съм аз?** (изследване на самоличността): профилите на тийнейджърите в социалните мрежи се превръщат в публично място за изследване на тяхната изграждаща се индивидуалност. Това може да доведе до разкриване на неподходяща информация.

➢ **Готин/а ли съм?** (сексуално съзряване): тийнейджърите изследват и изпробват в мрежата своето полово съзряване, при това в култура, която насърчава предизвикателната сексуалност. Възможно е те да се стремят да подражават на провокативните образи, които ги заливат от рекламната и развлекателната индустрия.

➢ **Всички го правят** (социални норми в интернет): съчетаването на фактори, които водят до липса на задръжки в интернет, и тенденцията тийнейджърите да проявяват стадно чувство може да доведе до възникване на социални норми в интернет, които подкрепят безотговорното поведение.

➢ **Ако мога да го направя, сигурно не е проблем**: само защото нещо може лесно да бъде направено, то не е лошо и не представлява проблем.

➢ **Търся любов**: тийнейджърите, които „търсят любов" в интернет, понякога правят неща, с които привличат неподходящи прояви на внимание.

➢ **Колко далеч мога да стигна** (рисково поведение): подрастващите изпробват границите, защото по този начин се научават колко устойчиви са те и кое е позволено. Рисковото поведение в интернет понякога може да се окаже по-безопасен начин за поемане на определени рискове, в сравнение с алтернативите в реалния свят".[9, с.12]

4. РОЛЯ НА РОДИТЕЛЯ.

[10] „На 1/5 им се е случвало някои от хората, с които са се срещнали, да са излъгали за истинската си възраст. А всяко 10-о хлапе е било обект на лоши намерения."[2]

Нека отново започнем с малко статистика, според която „близо 60 % от възрастните признават, че не са запознати с всички опасности, които дебнат децата им онлайн.”[3] Това е един много висок процент, който може да се каже, че показва както липсата на ангажираност по проблема така и неговото игнориране като съществена и непосредствена заплаха за техните деца. В тази връзка родителите, като че ли са по-склонни да обръщат внимание на своите деца например за това до колко късно и къде да ходят, с кого се запознават и излизат „физически”, отколкото когато те го правят „виртуално”. Седейки техните деца в къщи пред компютъра, таблета или телефона те си създават усещане за една доста фалшива сигурност и успокоение, че всичко е наред и под контрол. Невидимата, отложена доста често заплаха, каквато е тази във виртуалното пространство се пренебрегва от родителите и едва, когато попадне някой от тях на проблемна ситуация, тогава разбира за сериозността на проблема, който е игнорирал.

Според проучване[11] проведено в град Варна участниците в него споделят, че „нямат информация за най-актуалните социални мрежи и видео-чатове, които са особено популярни сред младежите”.[3] Много често, обаче не липсата на информация, особено в нашето съвремие, в което ние буквално сме потопени непрекъснато в нея, а ориентацията при търсенето и успешното й използване са причини за грешките, които допускаме. Ето защо е необходимо да се фокусира вниманието на родителите по отношение на новите опасности и реални рискове, които крие новата виртуална среда. Точно това, че тя е нова за родителите (поне що се касае до българските условия на технологично развитие) е друга причина за пренебрегването на опасностите, които крие, т.е. когато самите родители не са се сблъсквали с виртуалните опасности, няма как те да ги оценят като високо рискови както тези, които например сами са изпитали на гърба си, когато са били деца.

Според същото проучване проведено в град Варна „като най-голяма заплаха родителите определят насилието в интернет пространството.”[3] След цялата тази информация основното, на което трябва да се обърне внимание е какво да се направи, за да се засили ролята на родителя по отношение на предпазването на децата от киберопасностите? Три са основните насоки – информиране, подпомагане и сътрудничество.

Информиране за опасностите в интернет пространството, техните основни индикатори за разпознаването им както чисто технически (при наблюдаването на интерфейса на използваните от децата им устройства и съдържанието на посетените сайтове) така и чисто поведенчески (с открояването на поведенческите характеристики даващи индикации за наличие на проблем). В тази насока трябва да се включи и популяризирането на идеята за наличието на интернет опасностите и рисковете, създаване на навици с използване на начините на тяхното преодоляване или ограничаване и отново информиране за организациите, които могат да съдействат при възникването на проблеми.

Следващата насока е подпомагане тясно свързана с информирането, тъй като след като бъдат информирани родителите е необходимо и да бъдат подкрепяни за в бъдеще и постоянно с необходимата литература и специализиран софтуер за родителски контрол, техническа подкрепа и консултиране, от IT специалисти, за да бъдат с актуална информация и по този начин да бъдат полезни на своите деца. По възможност тази помощ, подкрепа да е безплатна поне за социално слаби семейства, които трудно биха могли сами със собствени средства да осигурят например минимално изискуемото за сигурността в интернет – антивирусните програми. Често тези семейства едва подсигуряват на децата си самите компютри и интернета притиснати от технологичните и образователни изисквания и не са в състояние да отделят средства и за

[11] Проект "Безопасен интернет", финансиран от дирекция "Превенции". Той „е онлайн базирана информационна кампания с включени към нея две интерактивни обучения насочени към родители на деца между 5 и 12 години.” [3] Проекта се реализира от сдружение Beehive Co-working Space-Varna. [3]

допълнителен софтуер. Само като пример един едногодишен абонаментен лиценз на антивирусна програма е около 50 лева. Тук може да се помисли и за включването им във вид на помощ като част от социалното подпомагане или мярка по закрилата на детето при рискови ситуации. Всичко това е въпрос на експертна оценка, разбира се.

Последната насока, която обаче свързва първите две сътрудничеството е особено важна. Без добрата координация и сътрудничество между деца, родители, учители, институции по киберсигурност трудно биха се постигнали добри резултати. Понякога дори само недобрата комуникация между тези основни субекти довежда до задълбочаване на възникналите проблеми и открива пътя към рисковото поведение на децата в мрежата, а не само. Когато имаме засилен контрол на децата от това какво се случва в мрежата от страна на учителите в училището и слаб такъв от страна на родителите в дома, тогава не можем да бъдем уверени, че е подсигурена сигурността на децата. Същото се случва, и когато няма достатъчна заинтересованост при сигнали и търсене на съдействие от страна на институциите оторизирани с функциите по киберсигурност и закрила на детето. От тук можем да изведем 9 задължения на родителите по отношение киберсигурноста на своите деца:

- да се информират и самообучават за новите предизвикателства във виртуалното пространство;
- да осъществяват контрол върху посещаваните от своите деца сайтове и страници в мрежата;
- да се интересуват от запознанствата на децата с виртуалните им приятели;
- да информират и напомнят периодично своите деца за опасностите и рисковете които се крият в мрежата, за количеството и качеството на споделяната информация във виртуалното пространство;
- да се интересуват от вълнуващите ги събития, модни тенденции, групи, музика, религиозни и политически идеологии и това как ги споделят с останалите в мрежата;
- да си сътрудничат регулярно и тясно с учителите им и класните ръководители по отношение на обучението при използване на мрежата и да предразполагат своите деца да споделят повече;
- да подпомагат своите деца в трудни моменти и да ги предпазват от вредни прояви в интернет пространството в следствие на тях;
- да съдействат на специализираните органи по киберсигурност при наличие на опасност и рисково поведение на своите деца;
- да се грижат за оптималното хардуерно и софтуерно обезпечаване на своите деца по повод сигурността в интернет.

Разбира се с тези задължения не се изчерпва цялата роля на родителя по предпазването на детето си от опасностите на интернет, но те са тези, без които киберсигурноста би била трудно постижима цел.

5. РОЛЯ НА УЧИТЕЛИТЕ.

И учителите подобно на родителите както стана вече ясно са страна, субект по отношение на киберсигурноста на децата в мрежата. В училище обаче като че ли основен проблем (особено през последните години) е детската агресия. Тази агресия има доста удобна форма в мрежата под формата на онлайн тормозът, чийто форми вече бяха разгледани подробно по-горе. Форма, която като че ли не е достатъчно призната като част от задълженията по преодоляването й от учителите в училищата, най-вече поради скритостта й и понякога отложеното въздействие. Например за физически конфликти между учениците става ясно още в междучасията особено, когато се разиграват в класната стая или близост до контролираните училищни територии, там

участниците в тях много често са ясни от пръв поглед, не така стоят нещата обаче когато става въпрос за конфликти и тормоз в интернет. В мрежата тези конфликти първо може да са много по-яростни[12], по продължителни, по въздействащи и обхватни (например унижението на един ученик от друг в реална обстановка си остава известно най-често в класа или най-много в училището от което са те, докато в мрежата поради нейната широка достъпност едно такова унижение може да стане достояние на целият приятелски кръг особено, чрез социалните мрежи), участниците в тях може да не са едновременно на едно и също място и време. Отложеното въздействие се характеризира с това, че резултатите от тези конфликти може да не са видими в деня, седмицата и дори месеца на възникването им, те въздействат много често с натрупване (многократни и дълговременни поствания с обидни квалификации, присмивания в социалните мрежи например) може да доведе до депресивни състояния и дори до суициди. Това прави тези конфликти по-малко забележими от учителите пред физическия конфликт в класната стая в междучасието, където резултатът и участниците веднага се установяват е се вземат мерки. Освен това „в много от случаите училището и учителите се чувстват безсилни или не считат, че е тяхна работа да се притесняват за проблеми от този род, тъй като те засягат учениците, когато се намират извън сградата на училището. Макар повечето учители да разбират сериозното въздействие на онлайн тормоза върху децата и свързаните с него притеснения, те не го приемат като проблем, свързан с училището.”[9, с. 13]

Въпреки това обаче трябва да се отбележи, че учителите от една страна отговарят за живота и здравето на децата по време на учебните часове, но и са отговорни при забелязване на някакви белези на проблеми да уведомят съответните институции отговорни по тяхната закрила и защита на техните интереси и права.

Така че учителите имат двойна функция:

- да помагат на децата, които имат проблеми, след като са станали жертва на онлайн тормоз и едновременно с това да предприемат мерки срещу онези, които злоупотребяват при ползването на мобилни телефони и интернет, а също така да изслушват и да предлагат адекватни съвети;
- да повишават осведомеността и да предоставят информация на децата и на родителите на онези, за които съществува сериозен риск да проявяват агресивно и оскърбително поведение в интернет; да оповестяват какви рискове поемат момчетата, които гледат на по-стъпките си като на шега и начин да изпъкнат със смелостта си, а всъщност с действията си нанасят вреда на други хора.”[9, с. 13] На базата на тази си двойна функция в Наръчника за учители. Младите хора между виртуалното и реалното. Разработване и прилагане на казуси в учебна среда, част от проектът TABBY[13] са изведени следните 11 задължения на учителя и училищния персонал по отношение на предпазването на децата в мрежата:
- да провеждат уроци, свързани с онлайн тормоза, за усвояване на ефективни социални умения, техники за разрешаване на конфликти, ефективно вземане на решения, комуникационни

[12] „Емоционалната и физическата отдалеченост, дължащи се на използването на електронни средства за комуникация, позволяват бързо преминаване от идеи към действие, без време за обмисляне на смисъла на конкретните постъпки и за социално взаимодействие. В киберпространството хората притежават по-малко социални, контекстуални и емоционални белези, отколкото при общуването лице в лице. Поради това те в много по-малка степен проявяват чувствителност или изпитват угризения за поведението си и често проявената агресия в мрежата се възприема като нормална форма на общуване. ” [9, с.14]

[13] „Проектът TABBY (Threat Assessment of Bullying Behavior in Youth online – Оценка на опасността от агресивно поведение на подрастващите в интернет) обхваща предизвикателствата, пред които са изправени учителите, педагогическите съветници в училище, инструкторите, директорите, родителите и учениците във връзка с използването на електронните средства за комуникации от подрастващите, на интернет и мобилните телефони, както и на други интерактивни устройства, които предполагат заплаха от онлайн-агресия, онлайн-тормоз и sexting (изпращане на послания или изображения със сексуално съдържание). Целта на проекта е увеличаване на познанията и уменията за предпазване на младите хора, които използват интернет, мобилни телефони, социални мрежи, училищни и извън-училищни мрежи, от превръщането им в жертви от страна на техните връстници или други подрастващи или дори възрастни. .”[9, с. 4]

умения и да подчертават важността на доброто отношение и взаимното уважение;

- да предлагат конкретни напътствия за превенция и прекратяване на онлайн тормоза;
- да се грижат за подобряването на конкретната социална среда в класната стая;
- да обучават подрастващите как да реагират и, което е дори по-важно, кога да пренебрегват проявите на онлайн тормоз"[9, с. 18-19] като тук бихме добавили и на другите видове опасности;
- да обучават страничните наблюдатели колко е важно да се говори, да се оказва помощ на жертвите и да се съобщава за евентуални притеснения;
- да подготвят подрастващите самостоятелно да се предпазват и да реагират на проблеми, свързани с онлайн тормоза и безопасността в интернет;
- да работят в сътрудничество с родителите на децата за развиването на самоконтрол и загриженост за доброто на другите;
- да отделят индивидуално внимание на онези ученици, които са засегнати от онлайн тормоз като извършители или като жертви;
- да участват в постигането на набелязаните цели, като посочват възможните опасности и предават на пострадалите ефективни умения за превенция и справяне с тормоза;
- да работят с извършителите, да разкриват причините за съответното поведение от страна на учениците;
- да провеждат занимания, които насърчават нужните умения и проявите на съпричастност, за да помогнат на извършителите да разберат и съпреживеят въздействието, което с постъпките си оказват върху другите."[9, с. 18-19]

Що се отнася до учителите имаме и нормативна база, която регламентира тяхната роля за безопасността във виртуалното пространство на територията на училището и това са „Правилата за безопасна работа на учениците в училищната компютърна мрежа и в Интернет" на Държавната агенция за закрила на детето, където в чл. 9 са изброени следните няколко:

- Разясняват правилата за безопасно и отговорно поведение при работа в училищната мрежа и в Интернет.
- Използват възможностите на Интернет за обогатяване и разширяване на учебната дейност като възлагат на учениците конкретни проучвания, предоставят списък с подходящи Интернет адреси и др.
- Осъществяват непрекъснато наблюдение и контрол върху работата на учениците в училищната мрежа и в Интернет в учебно и в извънучебно време. Удостоверяват регистрацията на учениците по чл. 7.
- Предприемат незабавни мерки за преустановяване на достъпа на учениците до незаконно съдържание в мрежата.
- Уведомяват незабавно директора на училището или на обслужващото звено при нарушаване на правилата или при установяване на незаконно съдържание в мрежата."[11]

В член 1 на същия документ, освен учителите е включен и педагогическия персонал в българското училище, който да информира и предпазва децата при опасности в интернет. Най-важния представител от този педагогически персонал е педагогическия съветник (а защо не и училищен социален работник), който както е известно е ангажиран именно с проблемите на децата в училище, по отношение на агресията между тях, наркотичната и алкохолна зависимост и като цяло от лошите въздействия, от една страна и от друга подпомага развитието им като „мини" общество в училището по отношение на честванията, празненства, информационни кампании и т.н..

Всичко това се пренася обаче и във виртуалното пространство, където педагогическия съветник трябва да може да отговори на изискванията на новото време и пространство като в своята пряка работа с децата, той освен традиционните беседи с тях трябва да включи в своята работа и други методи и средства на новото време като работа чрез личен блог, уеб страница, също така и с така модерният „фейсбук" (или другите социални мрежи), за да съумее да достигне до младите хора и да ги информира и предпази, както от досегашните опасности на реалния свят така и на тези във виртуалното пространство.

6. КАКВО ДА СЕ НАПРАВИ ЗА НАПРЕД – предпазване на децата и тийнеджърите от опасности в интернет в бъдеще.

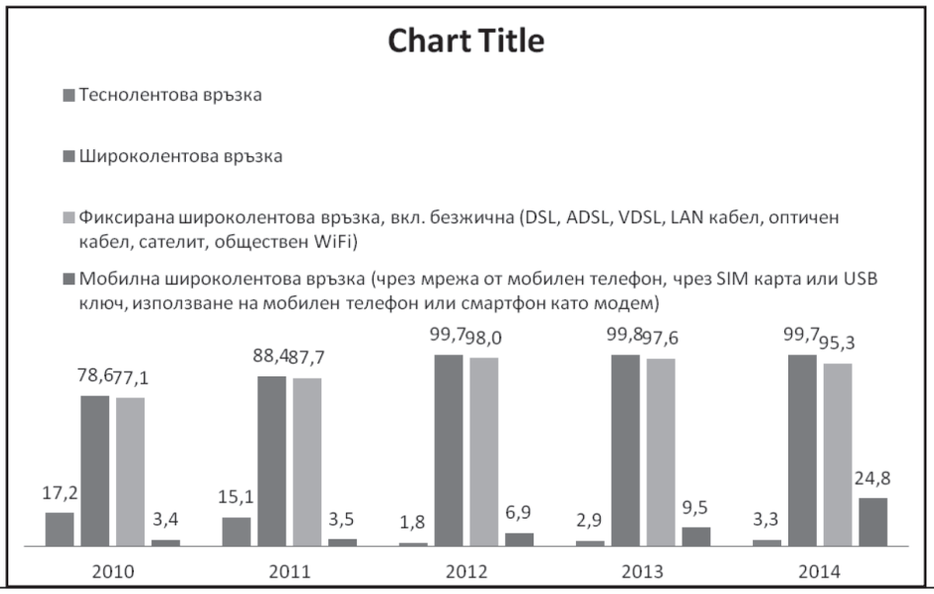
Това което е направено до момента е съставянето на Учебник по безопасен интернет, което по същество е едно учебно помагало[14] „…с конкретни примери и методически съвети към педагозите как да дискутират темата с децата се дават прости и ясни отговори на конкретни казуси."[2] Основният проблем обаче, е че това помагало не е задължително за училищата, което намалява възможностите за ползването му във всички училища на страната. На практика се получава, че който учител по информационни технологии, знае за него и желае да го използва реално го използва и в час.

Друг важен проблем е липсата на единен държавен образователен стандарт по отношение на киберсигурноста. Необходимо е да се направи реорганизация в учебната програма, с включването на мерките за осъществяване на киберсигурноста, която да гарантира обхвата на децата още от предучилищната детска възраст до завършването в 12 клас така, че да се създадат трайни навици в децата, а и да се повишава непрекъснато тяхната информираност и умения по бързо променящите се технологии и интернет възможности.

Необходимо е и на общоевропейско ниво да се изработи единен закон, който да гарантира киберсигурноста и да се справя с проблемите по нейното нарушаване.

Необходимостта от всички изброени до тук мерки и препоръки ясно се доказва от данните на НСИ за използването на интернет от населението в Диаграма №3.

Диаграма №3: Достъп до интернет по видове външни връзки[15]



[14] Помагалото е разработено от фондация "Партньори - България" като част от кампанията на евродепутатките Илияна Йотова и Филиз Хюсменова за сигурността на децата в мрежата."[2]

[15] „Относителният дял е изчислен на база домакинствата, които имат достъп до интернет. От 2012 г. не се наблюдава достъпът до интернет по видове устройства."[8]

Както се вижда от нея наблюдава се сериозен ръст на „Мобилната широколентова връзка (чрез мрежа от мобилен телефон, чрез SIM карта или USB ключ, използване на мобилен телефон или смартфон като модем)", само за една година (от 2013 до 2014г.)с почти два пъти и с над 10 пъти за 4 години (2010-2014г.) това означава, че е налице тенденция интернета да става все по-достъпен и мобилен през телефоните до хората и до децата. Това означава, че риска за тях от опасностите в интернет става все по-голям и сред все по-голям контингент от деца. До този извод се стига от наблюдаването на трайното изместване на обикновените мобилни телефони без възможности за включване към интернет от такива с възможност както и смартфоните и други. Освен това имаме и тенденция по намаляването на тарифите на този тип мобилен интернет от една страна и от друга увеличаване на мегабайтите включени в пакетите, като тенденциите са и до тяхното окончателно отпадане и на практика до ползването на неограничен трафик от данни. Това заедно с намаляването на цените на самите мобилни телефони води до тяхното повсеместно разпространение и постепенно изместване на другите видове устройства като настолните компютри, лаптопите например. Ако се запитате това каква връзка има с използването на интернета от страна на децата тя е повече от очевидна, защото до сега господството на настолните компютри и лаптопите даваше по труден достъп до интернет от страна на децата. Настолните компютри имат недостатъка да са непреносими или поне са достатъчно трудно преносими, т.е. само в къщи или в училище може да се ползват, а пък лаптопите са достатъчно големи и скъпи, за да могат да бъдат, толкова достъпен източник и средство за ползване на интернет. При тези две устройства имаше все пак успокоението, че детето може да се контролира малко по-лесно най-малкото кога да ги използва. Тези недостатъци при мобилните телефони от съвременното поколение ги няма и така всяко дете, на което е взет телефон (с цел уж да бъде контролирано къде е и какво прави) се сдобива с възможността още повече да влиза в интернет, когато и от където си поиска с и без родителски надзор, с и без учителски надзор, което го задължава то самото да има повече отговорност за това какво прави в интернет, да има необходимата информация да се защити при опасност и проблем. Всичко казано до тук ни дава правото да направим и прогноза, че до 2020 година интернет ще се разпространява основно, чрез мобилни връзки, което ще означава, че почти всяко дете ще разполага напрактика с неограничен интернет, което означава, че трябва до тогава да е направено необходимото по запознаването им с опасностите в интернет, с начините за предпазването им с тези опасности.

Към момента съществува програма за обучение и на трите групи заинтересовани лица - децата, родителите и учителите им по повод киберсигурноста, която прави организацията - Национален информационен център за безопасен Интернет, недостатък в някаква степен е това, че те са заплатени, което поставя пречки за по-слабите финансово училища и родители, които трудно биха си го позволили. Ето защо навлизането в учебната програма на повече часове по киберсигурност, а защо не и като отделен предмет в масовото българско училище е повече от необходимо.

В заключение може да се добави, че новите информационни и комуникационни технологии и интернета като важна свързваща ги част са важна необходимост за всеки човек. Те позволяват създаването на модерен и съвременен вид на това, с което работим и професионално се занимаваме, те са алтернативно средство за комуникация, дискутиране, обмен на информация, и подпомагащо провеждането на професионалните, учебните и социалните процеси. Те са вече част от нашият живот и в бъдеще все повече ще навлизат и ще заемат все по-нови територии от битието и социалната ни среда. Този процес е необратим, но въпроса, който възниква е как да съумяваме да ги използваме рационално и с мяра, без поемането на излишни рискове така че те ползотворно да ни служат, а не да ни вредят.[13]

7. КЪДЕ МОГАТ УЧИТЕЛИ, РОДИТЕЛИ И ДЕЦА ДА СЕ ОБЪРНАТ ЗА ПОМОЩ?

➢ Българска линия за онлайн безопасност тел.: 124-123 и на http://web112.net/NewSignal.aspx (гореща линия за борба с незаконно и вредно за деца съдържание в Интернет)

➢ Child helpline international.org тел.: 116 111 и на http://116111.eu/ (и двата телефона са безплатни и могат да бъдат избирани от цялата страна)

➢ Национален информационен център за безопасен Интернет - http://www.safenet.bg/bg/ (работи за повишаване на дигиталната грамотност на децата и младите хора)

➢ Държавна агенция за закрила на детето тел.: + 359 2 933 90 50 и на E-mail: stopech@sacp.government.bg

➢ Дирекция "Социално подпомагане", отделите „Закрила на детето"

12 прости правила за осигуряване на киберсигурност при използване на устройствата за връзка с Вашата виртуална среда

1. Винаги да се ползва актуална версия на лицензирана антивирусна програма. След инсталация на самата антивирусна програма да се даде възможност да се самоактуализира с цел обновяване на информацията за вирусните сигнатури. Препоръчително е използването на лицензиран софтуер.
2. Паролите от електронната поща, профилите и акаунтите и други изискващи подобен тип ползване в мрежата да се пазят извън ресурсите на компютъра. Същите тези пароли да се задават по достатъчно сложен начин като се използват всички възможности от комбинации, които позволява генератора им – например използването на цифри, букви, символи и т.н. Хубаво е да се ползват различни пароли за различните профили и да се сменят през определен период от време.
3. Преди влизане в даден сайт или профил първоначално да се погледне какви са отзивите от антивирусната програма, а не автоматично да се влиза.
4. При използване на външни устройства (флаш памет, външен твърд диск, и т.н.) задължително да се проверяват с антивирусната програма преди тяхното ползване или при предоставянето им от непознат човек те да не се използват.
5. Да не се предават лични данни, сканирани документи с лични данни, документи за собственост и други посредством мрежата, освен при проверени получатели и при проверени устройства и връзки.
6. Да не се качват компрометиращи лични или на членове от семейството снимки или видео, в интернет пространството. Преди да се качи нещо е хубаво да се допитате поне до още един близък, роднина или учител за мнение.
7. При регистрации и създаване на акаунти да се дава минимално количество информация от лично естество.
8. Да се забрани през настройките на устройството автоматично използване на камерата и микрофона на самото устройство.
9. Да не се оставят включени без надзор устройствата или те да бъдат заключени с достатъчно добра парола.
10. Да не се допускат оставени включени акаунтите или профилите при ползване на обществени или чужди устройства. Винаги излизайте с Изход.

11. При получаване на писма или други файлове от непознати да не се отварят или преди това да се пуснат през антивирусна програма, ако все пак се налага да се отварят.
12. При съмнение или при проблем във виртуалното пространство винаги да се търси помощ от родител, учител или специалист по киберсигурност.

Подобни правила са изготвени и в чл. 13 на Правила за безопасна работа на учениците в училищната компютърна мрежа и в Интернет, които обаче са строго фокусирани за работата в училищната мрежа, разбира се те са валидни в голяма степен и за домашната, но ни се струва, че предложените наши 12-сет са по общи и по фокусиране въобще при работа в мрежата и нейните възможности.

ЦИТИРАНА ЛИТЕРАТУРА:

1. Барозу, Ж. „Съобщение на Комисията Европа 2020 Стратегия за интелигентен, устойчив и приобщаващ растеж.“ Брюксел, 2010.
2. Вестник 24 часа, статия Тръгват часове по безопасен интернет в училище 28.12.2009 - http://www.24chasa.bg/Article.asp?ArticleId=326751 (Посетен на 28.10.2015г.)
3. Дарикнюз, статия Обучават родители да предпазват децата си в интернет 10 юни 2015 - http://dariknews.bg/view_article.php?article_id=1451541 (Посетен на 28.10.2015г.)
4. Какво представлява онлайн-тормозът? - http://bul.tabby.eu/10501072108210741086-10871088107710761089109010721074108311031074107 2-10861085108310721081108 5-10901086108810841086107910981090.html (Посетен на 28.10.2015г.)
5. Кирякова, М., Георгиева, Д., Лефтерова, В., Веселинска, Ф., Добрев, В., Проследяване на социалната активност в интернет (Facebook и Linkedin), София, 2012. http://moodle-test.fp.uni-sofia.bg/pluginfile.php/9583/mod_resource/content/0/Studentski_razrabotki_2012/Dokladi/rabota_Facebook_LinkedIn.pdf (Посетен на 28.10.2015г.)
6. Ларсен, К., К. Крумов. Социална психология: Нов поглед към личността и социалния свят. София, 2010.
7. Наръчник за учители. Младите хора между виртуалното и реалното. Разработване и прилагане на казуси в учебна среда - http://www.safenet.bg/images/sampledata/Materiali/Mladite_hora_mezhdu_virtualnoto_i_realnoto.pdf (Посетен на 28.10.2015г.)
8. Национален статистически институт (НСИ) - http://www.nsi.bg/bg/content/2808/%D0%B4%D0%BE%D1%81%D1%82%D1%8A%D0%BF-%D0%BD%D0%B0-%D0%B4%D0%BE%D0%BC%D0%B0%D0%BA%D0%B8%D0%BD%D1%81%D1%82%D0%B2%D0%B0%D1%82%D0%B0-%D0%B4%D0%BE-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82 (Посетен на 28.10.2015г.)
9. Онлайн тормозът наръчник за учители - http://bul.tabby.eu/10481079109010771075108311031085107 7-10851072-10731088108610961091108810721090107 2.html(Посетен на 28.10.2015г.)
10. Пиаже, Ж. Психология на интелекта. София, 1996.
11. Правила за безопасна работа на учениците в училищната компютърна мрежа и в Интернет - http://www.stopech.sacp.government.bg/file.php?fid=97.

12 . Стойчева, М., Васов, С., Върбановска, Т., Захариев, С., Стратегии за работа на социалният работник с юноши (13-18), страдащи от различни форми на пристрастеност към интернет http://moodle-test.fp.uni-sofia.bg/pluginfile.php/9662/mod_resource/content/0/Studentski_razrabotki_2012/Dokladi/Internet_zavisimost.pdf (Посетен на 28.10.2015г.)

13. Wiki на Александрова., А., Генчев, А., Добрев., В., Акривопулу, Й., и Петров., Р.,- Рефлективно – есе http://moodle-test.fp.uni-sofia.bg/mod/wiki/view.php?id=5512

ЗАПЛАХИ И РИСКОВЕ В ИНТЕРНЕТ

Дарин Йончев

CEH,CHFI, Security+, MCT, MCSE,MCITP

ОТ КОГО ДА СЕ ПАЗИМ?

- Професионални крадци на информация
- Кибер терористи (Cyber terrorsuts)
- Специални служби за разузнаване
- Е-Активисти (hacktivist)
- Е-Вандали (Script kiddies)
- Отмъстителни “приятели” или колеги
- … или всеки, който е част от мрежата и желае нещо от нас

АНАТОМИЯ НА ИНТЕРНЕТ АТАКИТЕ

1. Избор на цел
2. Разучаване на целта
3. Откриване на уязвимост
4. Експлоатиране на уязвимостта
5. Извършване на зловредно действие

Какво е CIA?

ИНСТРУМЕНТИ- ВИДОВЕ ЗЛОВРЕДЕН КОД

- Вируси (Viruses)
- Червеи (Worms)
- Троянски коне (Trojan)
- Логически бомби (Logic Bombs)
- Шпионски софуер (Spyware)
- Adware
- Keyloggers
- Password Crackers
- Rootkit
- DDoS
- Bot net

ТОВА, ОТ КОЕТО АНТИВИРУСНАТА ПРОГРАМА НЕ МОЖЕ ДА ВИ ОПАЗИ

- Социално инженерство
- Фишинг
- Спам
- Тормоз в Интернет (Online harassment)
- Крадене на самоличност (Impersonation)

- Загуба на онлайн репутация
- Умишлена заблуда и манипулация

ОПАСНОСТИ В СОЦИАЛНИТЕ МРЕЖИ

- Лесно достъпни. Навсякъде с нас посредством мобилните приложения.
- Лесен начин за наблюдаване и събиране на лична информация
- Крадене на самоличност.
- Разпространение на радикални идеи, клевети и омраза
- Фишинг
- Спам

КАКВО ДА ПАЗИМ?

- Данни
  - *Конфеденциални данни*
  - *Лични данни*
  - *Интелектулана собственост*
  - *Чужди данни*
  - *Трудно възстановими данни*
- Репутация
  - *Какво знае интернет за мен? Добро ли е или лошо?*

Какво мога да си позволя да загубя?

НЯКОЛКО ПРОСТИ ПРАВИЛА

- Антивирусна програма с актулани вирусни дефиниции
- Изполвайте Firewall – подсигурете входовете и изходите
- Използвайте съвременен и автентичен софтуер.
- Потвърдете идентичността на отрсрещнаната страна преди да предоставите лична информация.
- Уверете се че изпращате лични данни, пароли или номера на кредитни карти само по криптирани връзки. (HTTPs)
- Избягвайте подозрителни сайтове. Внимавайте къде ви пращат линкновете, които използвате.
- Използвайте pop-up blocker или ad blocker.
- Бъдете особено подозрителни към електронии съобщения от непознати. Особенно ако има правописни грешки или съмнениия за ‘автоматичен превод’.
- Подхождайте критично към твърде примамливи предложения. Най-вероятно не сте спечелили от лотария, в която не участвате.
- Внимавайте какво публикувате в интернет и кой би могъл да го види.
- Използвайте трудни за отгатване пароли. Колкото по-дълги, толкова по-добре.
- Избягвайте използването на флаш памет от публични или ненадежни компютри.
- Избягвайте да въвеждате лични данни или банкова информация от публични компютри.
- Подсигурете си резервни копия на информацията. На допълнителн диск или в облака изборът е ваш.

ОПАЗВАНЕ НА ЦЕННА ИНФОРМАЦИЯ И БЕЗОПАСНО ОПЕРИРАНЕ СЪС СРЕДСТВА

Юрий Генов

Председател на Комитета по информационни технологии

към Асоциацията на Банките в България

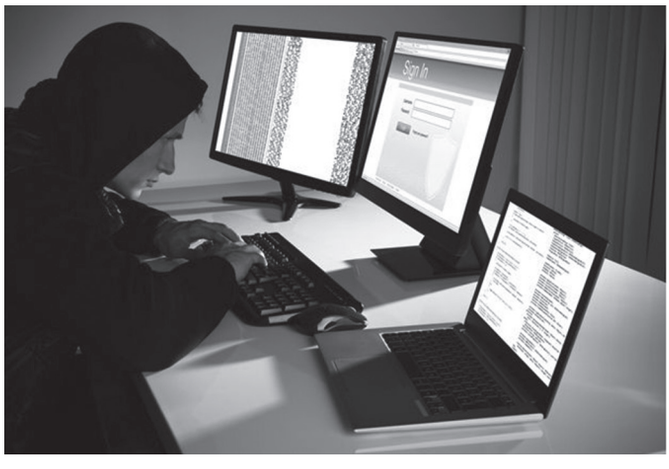
ОСНОВНИ ВЪПРОСИ

- Какво се промени в заплахите през последните 5 години
- Колко умен и опасен е престъпника
- Основни видове финансови киберпрестъпления
- Споделяне на опит
- Въпроси и отговори

КАКВО СЕ ПРОМЕНИ ПРЕЗ ПОСЛЕДНИТЕ 5 ГОДИНИ

- Финансовите организации инвестираха в сигурността си
- Заплахите пресякоха държавните граници
- Атаките се насочиха към личните устройства
- За или Против криптовалутите
- Превземането на втория канал за идентификация

КОЛКО УМЕН И ОПАСЕН Е ПРЕСТЪПНИКЪТ?





ОСНОВНИ ВИДОВЕ ФИНАНСОВИ КИБЕРПРЕСТЪПЛЕНИЯ (аналогични на реалните престъпления)

- Откраднатa самоличност форми на социално инженерство
- Завладяване на работната станция или смартфона
- man in the middle
- Фишинг
- Фалшиви електронни фактури - CEO fraud
- Мулета

СПОДЕЛЯНЕ НА ОПИТ

Стандартни съвети

- Пачвай операционната система
- Сменяй пароли и не ги споделяй
- Не отваряй съмнителни писма
- Пази дебитните и кредитните карти, особено ПИН и CVV
- Използвай проверени финансови инструменти

Личен опит

- Наблюдавай своето устройство
- Наблюдавай своя потребител
- Познавай кореспондентите си
- Използвайте виртуални карти за интернет разплащания
- Контролирай редовно състоянието на сметките си

СИГУРНОСТ В КИБЕРПРОСТРАНСТВОТО

доц. д-р Димитрина Полимирова

Национална лаборатория по компютърна вирусология към

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

1. ОСНОВНИ ПРОБЛЕМИ

1.1. Битка между злонамереното и добронамереното мислене.

1.2. Мотиви за извършване на престъпления:

• Лично облагодетелстване.

1.3. Киберпространство:

• Обобщен израз на изградената от съвременното общество информационна инфраструктура, включваща всички йерархични нива на съвременната глобална мрежа.

1.4. Особена невидимост на информационните престъпления:

• Престъпление има, но извършител няма.

1.5. Кибер атаки:

• Манипулиране на информационната среда по такъв начин, че се променя идентичността на отделния потребител, компютър или мрежа, заблуждава се насрещната страна за правомерността на определени действия, извличат се по нерегламентиран начин данни, чието използване носи преки финансови или морални загуби на физически или юридически субекти, преодолявайки регионални, национални или глобални граници.

Видове кибер атаки:

• *Активни*

Съдържат в себе си определен сценарий, който предполага планиране и извършване на поредица от действия, свързани с промяна на определена програмна среда и нейните компоненти.

• *Пасивни*

Съдържат в себе си определен сценарий, който включва предварително планирана поредица от действия, но този сценарий се отличава с това, че при него не се цели и не се постига промяна в програмната среда, а само се търси достъп до атакуваните ресурси и информационни потоци, като се реализира функцията наблюдение и анализ.

2. АТАКУВАЩИ ПРОЦЕСИ В ГЛОБАЛНАТА МРЕЖА

- Вируси
- Червеи
- Троянски коне
- Шпионски софтуер (spyware)
- Rootkit-ове
- Задни вратички (backdoors)
- Botnet-и
- Keylogger-и

3. ПОТЕНЦИАЛНИ ЗАПЛАХИ В ГЛОБАЛНАТА МРЕЖА

3.1. Достъп (Access)

• Атака, свързана с конфиденциалността на информацията

3.2. Модификация (Modification)

• Атака, свързана с интегритета на информацията

3.3. Отказ от услуга (DoS)

• Атака, свързана с наличността на информацията

3.4. Отхвърляне (Repudiation)

• Атака, свързана с достоверността на информацията

4. ПОТЕНЦИАЛНИ ВРЕДИ ОТ КИБЕР АТАКИ

4.1 Неоторизиран достъп до компютри и компютърни мрежи:

• Постигане на частичен или пълен достъп до определени ресурси в компютри и компютърни мрежи

• Неупълномощените и незаконни действия от страна на атакуващия хакер са в състояние да причинят изключителни материални и нематериални щети.

4.2. Злонамерено изпълнение на програми за модифициране или разрушаване на данни, кибервандализъм

• Модифицирането на данни е със значително присъствие в сценариите за информационните атаки в киберпространството.

• Изисква се изграждане на система от превантивни действия още в момента, когато започва да се планира създаването на следващата WEB базирана информационна система.

4.3. Лъжлива или злонамерена информация за идентичността на потребителя

• В т.нар. електронно досие на отделен гражданин или служител във фирма се осъществява подмяна на данни в отделни полета или тотална подмяна на цялото досие.

• Известни са също така и успешни опити на хакерски атаки, имащи за цел манипулиране на отделни информационни полета, на отделни информационни единици и на цели информационни потоци към, от и на сателитните системи.

5. МЕТОДИ И СРЕДСТВА ЗА ЗАЩИТА

5.1. Методи и средства за защита на мрежи и канали за връзка:

• Защитата на информационната инфраструктура, съставена от т.нар. технически средства, в която влизат компютрите, мрежите и каналите за връзка.

5.2. Методи и средства за защита на софтуерни системи

• За да се гарантира приемливо ниво на защита, е необходимо да се извършат:

1. Подготовка на операционната система;
2. Подготовка на драйверите;
3. Подготовка на приложенията.

5.3. Повишаване на сигурността при достъп до интернет приложения

• Преглеждане на опциите на всички Интернет приложения и настройването им в посока на един консервативен профил

• Включване и активно използване на отделните средства за криптиране на съдържанието

• Активно използване на всички налични средства за електронен подпис

5.4. Повишаване на сигурността на данните

• Данните са най-променливия информационен поток във функционирането на една информационна инфраструктура и поради това са най-силно изложени на възможността за реализиране на хакерска атака чрез тях.

6. ЗАКЛЮЧЕНИЕ

Въпросът за сигурността е едно от големите предизвикателства, свързано с разширяващите се услуги, предлагани към гражданите в глобалната мрежа.

Сигурността се е превърнала в стока, продавана и купувана на пазара:

• Ценовият механизъм балансира разходите за обезпечаване на сигурност и специфичната необходимост от сигурност.

• Много рискове за сигурността остават без решение или решенията достигат бавно до пазара поради неговите несъвършенства.

• Специфични политически мерки, отнасящи се до тези несъвършенства, ще подобрят пазарните процеси и същевременно ще усъвършенстват функционирането на законовите рамки.

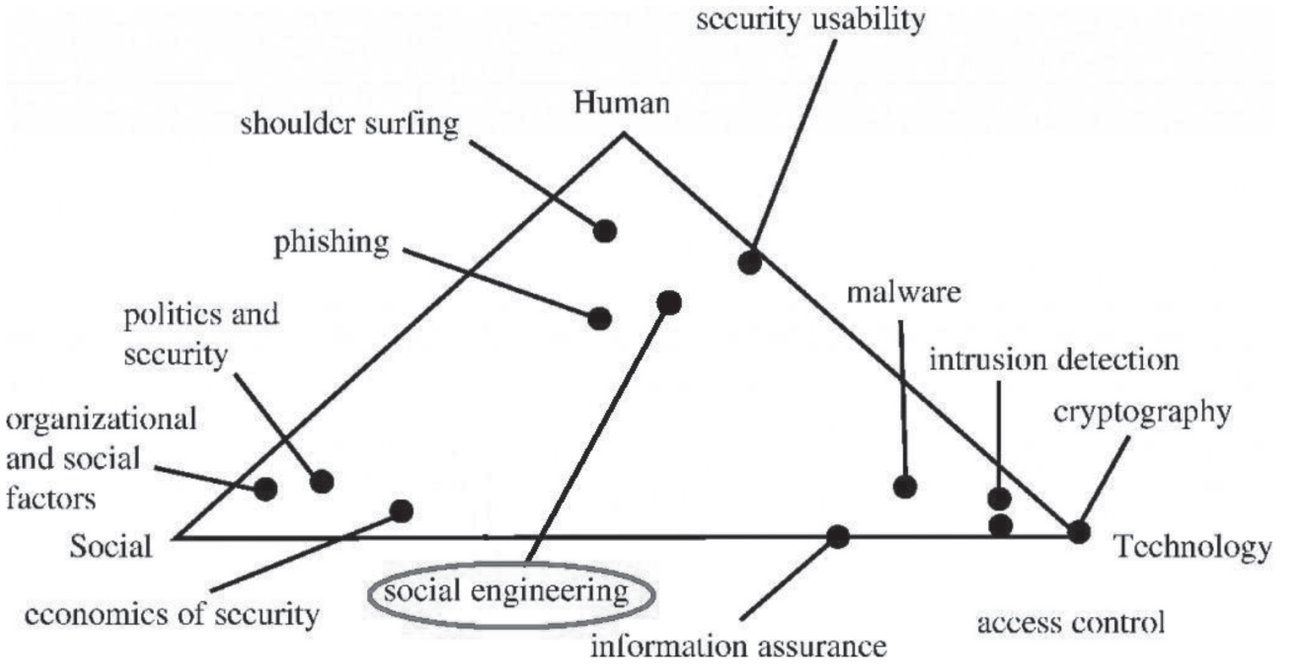
КОМПРОМЕТИРАНЕ НА ИНФОРМАЦИОННАТА БЕЗОПАСНОСТ ЧРЕЗ МЕТОДИТЕ НА СОЦИАЛНИЯ ИНЖЕНЕРИНГ

Капитан Добрин Махлянов
ДИРЕКЦИЯ СИГУРНОСТ НА ИНФОРМАЦИЯТА
МИНИСТЕРСТВО НА ОТБРАНАТА

СОЦИАЛЕН ИНЖЕНЕРИНГ

"Действие, което цели да подтикне индивида към извършване на дейности, които не са в негов интерес"

МЯСТО



ФАЗИ

- Събиране на информация за обекта
- Установяване на отношения за обекта
- Експлоатиране на обекта
- Възползване от придобитата информация от обекта

МОТИВАЦИЯ НА АТАКУВАЩИЯ

- Пари
- Отмъщение
- Личен интерес
- Външен натиск
- Шпионаж
- Вътрешен контрол

МЕТОДИ ЗА СОЦИАЛЕН ИНЖЕНЕРИНГ

- Технически умения (“хакване на компютри”)
- Социални умения (“хакване на хора”)

ДИРЕКТНА КОМУНИКАЦИЯ

- Директен подход
- Важен потребител
- Техническа поддръжка
- Безпомощен потребител

ФИЗИЧЕСКИ МЕТОДИ

- Надничане (shoulder surfing)
- Ровене в боклука
- Извличане на информация от изхвърлени носители на информация

ТЕХНИЧЕСКИ МЕТОДИ

- Social Enggineer Toolkit
- Фишинг
- Подправени уеб страници
- Използване на недоверени сертификати
- Разбиване на стандартни пароли
- Предварително инфектирани носители на информация

Аферата “Robin Sage”

- 25 годишен специалист по кибер защита +
- 10 години стаж по специалността +
- Известни приятели в Facebook и Twitter =
- Предложение за работа в Google



Сигурностт@ на младите в интернет.

Предизвикателствата пред киберсигурността.

Българска

© Редактор Йордан Божилов

64 стр.

© Издателство: Елестра ЕООД

София, 2015