ОБЩИНА ВАРНА
ДИРЕКЦИЯ "ПРЕВЕНЦИИ"

БЕЗОПАСЕН ИНТЕРНЕТ

Наръчник за обучители на връстници

Магдалена Малева, VI клас
СОУ "Св. Климент Охридски" - гр. Варна

www.prevencii.com
www.p2prevention.bg

СЪДЪРЖАНИЕ:

Ако НЕ използваш интернет спри да четеш тук… Този наръчник не е предназначен за теб!

Все още си тук? Нека предположа, Интернет заема голяма част от твоето ежедневие. Дори по–голяма отколкото си представяш. Не се притеснявай, това не е задължително нещо лошо. Аз също използвам Интернет за почти всичко през деня си. Но пък познавам някои от особеностите на Web-а, които ще ти бъдат полезни и най-вече ще ти помогнат да бъдеш в безопасност. Безопасността в Интернет обичайно не е нещо, за което мислим докато сърфираме в социалните мрежи, пазаруваме от любимите си магазини или създаваме поредния си профил в някой нов сайт.

Сега предстои стъпка по стъпка да те запозная с рисковете, криещи се в Интернет пространството и нещата, които трябва да знаеш преди да отвориш браузъра си.

Интернет или **Web** („Уеб" от англ. „мрежа, паяжина") представлява глобална мрежа изградена от множество по – малки мрежи, които свързват устройствата от целия свят и правят възможно ежедневието ни такова каквото е. Това, което е било част от мрежата остава там за неопределен период от време. С други думи, всяка снимка, видеоклип и лична информация, които качиш стават част от тази мрежа и си остават в нея под една или друга форма. Необходимо е всеки от нас да носи своята лична отговорност за това какво споделя с другите в мрежата, защото една съвсем нормална снимка с училищната униформа дава информация на останалите, къде учиш. Едно невинно тагване може да покаже на потенциален недоброжелател точното ти местоположение. Споделяйки възрастта си, емоционалното си състояние или твоите лични проблеми с другите в Интернет може да се окаже перфектната възможност, за някой да се възползва от теб и това не е сценарий от някой холивудски филм.

Това е историята на едно момиче, което на 13 годишна възраст става жертва на сексуален тормоз, чрез Интернет, защото дори за миг не е предполагала, че човекът отсреща не е този, за когото се представя. Това е историята на Алисия Козакевич, която през 2001 година започва да общува с непознат в социална мрежа. Той се представя за приятелски настроен тийнейджър на нейната възраст, а всъщност това е бил 38 – годишния Скот Тайрий. В продължение на една година този мъж е „отглеждал" момичето, постепенно печелейки нейното доверие като винаги я изслушвал, когато тя имала проблеми и винаги бил насреща, когато искала да споделя с него. Терминът „отглеждане" се използва, когато се говори за похитител и негова жертва в Интернет, когато става въпрос за тежко престъпление с цел примамване на непълнолетно или малолетно лице и изграждане на близка емоционална връзка с него като в голям процент от случаите това завършва с отвличане с цел сексуална експлоатация. Именно това се е случило с Алисия, която в навечерието на Нова година срещу 2002 г. е

подканена от Скот да се срещнат за първи път на живо съвсем близо до мястото, където тя живее. Доверието и любопитството на Алисия надделяват и тя се съгласява да се видят. Тогава Скот я вкарва насилствено в неговия бус и я откарва в мазата на своята къща, където я изнасилва многократно и заснема всичко на видеозаписи, които излъчвал на живо в някакъв сайт, за да гледат и други с неговите наклонности, които дори плащали за това. Това му изиграва лоша шега, защото един от хората, който гледал на живо въпросните кадри разпознал момичето от плакатите и снимките от новините за нейното изчезване и решил в крайна сметка да уведоми ФБР за това. Свързва се с полицията от уличен телефон, тъй като се опасявал, че ще го проследят и ще бъде осъден заради това, че е гледал кадрите. Събирайки улики, полицията намира чатовете на момичето с похитителя и по този начин проследяват неговия IP адрес, което ги отвежда точно на местопрестъплението. Алисия е спасена, а Скот Тайрий е осъден на 19 години затвор за сексуално посегателство над малолетно лице.

Сега през 2021 година Алисия Козакевич е на 32 години и има собствена кампания срещу сексуалното насилие над деца. Често жертви на подобно престъпление биват обвинявани от обществото, че това, което им се е случило е по тяхна вина, което допълнително засилва травмата от преживяното.

ТРАФИКЪТ НА ХОРА И ИНТЕРНЕТ

Трафикът на хора представлява съвременна форма на робство с цел трудова и/или сексуална експлоатация, продажба на новородени, незаконна продажба на органи с цел донорство или склоняване на други лица към просия. Това, което го прави сериозен и глобален проблем, е че буквално всеки би могъл да стане жертва. Особено застрашени са хората, които:

- Имат ниско образование;
- Не са достатъчно информирани за това какво е правилно да се прави, когато пътуват по работа или за почивка в чужбина;
- Са прекалено доверчиви и биха приели помощ от хора, с които са се запознали в социална мрежа, а дори не са ги виждали на живо;
- Са емоционално нестабилни;
- Споделят твърде лична информация за себе си и своето емоционално състояние с околните;
- Са склонни да се срещнат на живо с някой, който им е предложил покана за приятелство в Интернет;
- Пътуват сами в чужбина без да уведомят своите близки и роднини къде отиват и за колко време;
- Биха позволили на някой да задържи личните му документи при проверка;

• Приемат покани за приятелство от хора, които не познават в социалните мрежи.

Важно е да се отбележи, че независимо от своя социален статус, семейно положение, пол, нагласи и опит всеки би могъл да се превърне в жертва на трафик на хора. И това става още по-лесно благодарение на Интернет. Много по-лесно за един трафикант е да прикрие себе си зад фасадата на фалшив профил в социална мрежа и да спечели доверието на своята жертва така, че тя сама да дойде при него.

Ето как може да се случи това. Похитителя се свързва с потенциалната си жертва (да вземем за пример момиче на 21 г. възраст), след което постепенно създава емоционална връзка с нея и печели нейното доверие. В неопределен период от време тя е манипулирана така, че да се влюби в него. Всичко това, докато не дойде момента, в който й отправя предложение да се видят, тъй като той пътува по-работа в съседен град, близо до града в който тя живее. Намират се всякакви причини да се срещнат на друго, непознато за нея място под претекст, че той е възпрепятстван, но много би искал да я види. Друг възможен сценарий е да й купи самолетен билет за рождения й ден и да я покани на гости в държавата, в която му се налага да работи за неопределен период от време, докато събере достатъчно пари, за да се прибере в своята държава и да изпълни мечтите и плановете си, от които тя също е част. Ако момичето допусне грешката да замине, за да се види с него, шансовете са в полза на това да бъде отвлечена и да се превърне в жертва на трафик на хора с цел сексуална експлоатация и принудена да проституира в някоя отдалечена точка на света. Този метод за въвличане на някой в трафик на хора се нарича „Loverboy" и е масово разпространен, защото в много случаи работи. Това, с което е характерен е възползването от наивността и чувствителността на жертвата, като на практика тя сама попада в капана. И всичко това е възможно благодарение на Интернет.

Изключително лесно е набелязването на жертвите от трафиканти, чрез социалните мрежи. Това е мястото, където всички ние споделяме много лична информация за нас като например: възраст, месторабота, къде учим, кои са нашите роднини, къде обичаме да ходим, какво обичаме да правим в свободното си време и не на последно място нашите лични проблеми, преживявания и емоции. Това е удобен начин за един трафикант да избере „перфектната" жертва, която с минимални усилия да въвлече в трафик на хора с цел сексуална или трудова експлоатация. Въпреки това, обикновено, тези престъпници прекарват много време в опити да спечелят доверието на жертвите си. Понякога това отнема месеци или дори година в чата, които прерастват в срещи на живо, а в последствие и в любовни връзки. Характерното за един трафикант на хора, е че той умее изключително добре да манипулира жертвите си и да ги накара да повярват в уж добрите му намерения.

ОНЛАЙН – ТОРМОЗ

Този тип тормоз се среща най-вече сред деца и тийнейджъри и представлява системна проява на грубо отношение към някого с цел упражняване на психическо насилие. Онлайн – тормозът може да приема различни форми:

➢ **Качване на чужди (злепоставящи) снимки или видео в социалните мрежи** - с цел унижение или отмъщение.

Това е често срещана практика, особено сред подрастващи и тийнейджъри и се използва като начин за отмъщение при караница или любовна раздяла.

➢ **Език на омразата** – обиди, заплахи, хейт, подигравки, клюки…

Всички сме ставали свидетели на подобен тип общуване в мрежата. Има голяма вероятност дори ти, който четеш това да си бил жертва на език на омразата. Една от причините за масовата му проява е липсата на физически и очен контакт като вместо това пред нас стои екрана на нашия телефон или компютър. Това кара човек да загуби преценка за това какво казва и дори да не осъзнава, колко жесток може да бъде към другите. Ако в училище някой е системно тормозен, той винаги може да се премести в друго, или просто да избяга от конфликтната ситуация. Нещата не стоят по този начин в Интернет, защото там тормозът може да продължава 24 часа в денонощието и без ограничения. Един от рисковете, които крие това е да се развие значителна психическа травма, която в последствие да накара потърпевшия да не се доверява и да не общува с околните, да понижи самооценката и мотивацията си. Има хора, които не могат да се справят с такова напрежение и нямат подкрепа от никого, като накрая подобни случаи дори завършват със самоубийство.

Ето какво да правиш ако станеш жертва на език на омразата или на онлайн-тормоз:

• Ако е възможно учтиво помоли човека, да бъде свалена публикацията, която те злепоставя;
• Ако не спира да ти пише, го блокирай вместо да откликваш с агресия. Всякакъв вид отговори от твоя страна само ще засилят неговото желание да те тормози;
• Докладвай профила му. Това може да стане по два начина. Единият е да използваш бутона за блокиране от социалната мрежа в която се е случил проблема, а другият е да докладваш на www.safenet.bg
• Сподели на приятел или потърси съвет от някого – не е добра идея сам да се справяш с подобен проблем.

➢ **Сексторшън** – форма на изнудване, при която непълнолетно лице е принуждавано да извършва сексуални действия. Жертвата е заплашвана с компрометиращо съдържание (снимка, видео), което ще бъде споделено в социална мрежа ако не изпълни желанията на насилника. В раздел **„Други опасности"** е описан подробно възможен случай на сексторшън и какво да правиш, ако се случи на теб.

ИНТЕРНЕТ ЕТИКА – „НЕТИКЕТ"

Нещо, което малко хора знаят е, че дори когато сме онлайн, трябва да спазваме общоприетите норми за поведение. Така наречения „етикет" на общуване в реалния свят важи и във виртуалния. По този начин всеки би се чувствал добре, а проблемите, описани по-горе нямаше да съществуват. Уви, реалността е друга и промяната трябва да дойде от нас самите.

И запомни… Отговорността за постъпките ти в Интернет е изцяло твоя!

ПАРОЛИ

Преди да прочетеш тази тема е добре да се запознаеш с част от понятията свързани с нея. Така ще ти е много по-лесно да научиш информацията и да я разбереш.

➢ **Хеш** – хеширането на парола буквално означава тя да бъде закодирана.

Това става посредством сложни математически алгоритми, които взимат паролата в „суров" вид, например: 123456, след което я преобразуват в поредица от разбъркани букви и цифри.

Например: **e10adc3949ba59abbe56e057f20f883e**

Процесът на хеширане на парола е необратим! В случай, че информацията с пароли на потребители „изтече" от базата данни тя ще бъде под формата на хеш и това би затруднило всеки, който е с намерение да я използва за злоупотреби.

➢ **Алгоритъм** – сложна система от математически формули, чрез които паролите биват трансформирани в хеш.

➢ **Хакер** – човек, който има добри или отлични софтуерни познания и ги използва злонамерено, за да преодолее защитите на уебсайтове, приложения, бази данни и сървъри. Главната цел е кражба на данни и злоупотреба с тях в негова полза. Съществуват и така наречените етични хакери. Те също се стремят да саботират защитите на базите данни, като по този начин имат за цел да разберат как да подобрят системите за сигурност.

➢ **База данни** – всеки уебсайт има свое място, на което съхранява огромно количество информация необходима за функционирането му. Това място се нарича база данни и представлява съвкупност от свързана информация, организирана по определен начин, който е специфичен за отделните уебсайтове. Там се съхранява и информацията на потребителите - потребителски имена, пароли, имейли, възраст и други лични данни, които попълват при регистрация.

Твоята парола е единствената бариера между личните ти данни и другите в Web пространството. Въпреки това шансовете са в полза на вероятността паролата ти да е слаба и дори сравнително лесна за „разбиване". Затова по-късно ще ти покажа как да създадеш наистина силна парола.

Съществуват **6 широко разпространени** алгоритъма за превръщане на парола от „суров" вид в хеш форма. Ето как изглежда паролата „123456" след като се преобразува с всеки един от тези алгоритми:

Първия алгоритъм е **MD5** и ето как изглежда паролата „123456", когато се преобразува чрез него -e10adc3949ba59abbe56e057f20f883e
Вторият е **SHA1** ("123456") =
7c4a8d09ca3762af61e59520943dc26494f8941b
Третият е **SHA224** ("123456") =
f8cdb04495ded47615258f9dc6a3f4707fd2405434fefc3cbf4ef4e6
Четвъртият е SHA256 ("123456") =
8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92
Петият е **SHA384** ("123456") =
0a989ebc4a77b56a6e2bb7b19d995d185ce44090c13e2984b7ecc6d446d4b61ea9991b76a4c2f04b1b4d244841449454
и шестият SHA512 ("123456") =
ba3253876aed6bc22d4a6ff53d8406c6ad864195ed144ab5c87621b6c233b548baeae6956df346ec8c17f5ea10f35ee3cbc514797ed7ddd3145464e2a0bab413

Ето ги и два от методите, които хакерите използват за да „разбиват" пароли:

● **Речников подход (англ. - Dictionary method)** – с течение на времето и разбиване на милиони пароли в хакерските общности е създаден „речник" на най – често използваните пароли по цял свят. Някои от тези пароли са: „qwerty"; „password"; „123456"; „111111"; „letmein"; „000000". Този речник съдържа около 14 милиона подобни пароли и единственото, което хакерът прави е да ги сложи в програма, която да опитва да влезе в профила ти, с една от тях. Програмите могат да правят това с невероятна скорост и в случая паролата, която взехме за пример по–рано „123456" може да бъде разбита за по-малко от една секунда!

• **Груба сила (англ. - Brute force)** – този подход е доста неефективен, тъй като хакерът използва програма, която опитва всяка една възможна комбинация от букви, цифри и знаци, за да улучи вашата парола и това отнема изключително много време. Успешен е тогава, когато потребителя има твърде кратка парола, която се състои само от букви или само от цифри. Това е и причината повечето сайтове да изискват парола, която да съдържа букви и цифри, както и да е със седем или повече от седем символа.

• **"Rainbow" таблица** – понеже преобразуването на парола от хеш форма обратно в суров вид е практически невъзможно, съществуват таблици, които съдържат милиони пароли, но в техния хеш вариант преработен от всеки един широко разпространен алгоритъм. Ето как изглежда паролите **„qwerty"** и **„000000"** в „Rainbow" таблици:

Алгоритъм	„qwerty" – хеш форма
Md5	d8578edf8458ce06fbc5bb76a58c5ca4
SHA1	b1b3773a05c0ed0176787a4f1574ff0075f7521e
SHA224	5154aaa49392fb275ce7e12a7d3e00901cf9cf3ab10491673f97322f
SHA256	65e84be33532fb784c48129675f9eff3a682b27168c0ea744b2cf58ee02337c5
SHA384	1ab60e110d41a9aac5e30d086c490819bfe3461b38c76b9602fe9686aa0aa3d28c63c96a1019e3788c40a14f4292e50f
SHA512	0dd3e512642c97ca3f747f9a76e374fbda73f9292823c0313be9d78add7cdd8f72235af0c553dd26797e78e1854edee0ae002f8aba074b066dfce1af114e32f8

табл. 1

Алгоритъм	„qwerty" – хеш форма
Md5	670b14728ad9902aecba32e22fa4f6bd
SHA1	c984aed014aec7623a54f0591da07a85fd4b762d
SHA224	**bfa29bfcdeca6e46328173e334f60d8c26c03cf82fb7f88a1ec15ed7**
SHA256	91b4d142823f7d20c5f08df69122de43f35f057a988d9619f6d3138485c9a203
SHA384	4cb4d582543c9696e30e4e87c1a549c6911dd7ff2b0079604df4b77cef86bb845e5868b4f2f46af895adf6c4dfa6a627
SHA512	64fcc6f6bc7a815041b4db51f00f4bea8e51c13b27f422da0a8522c94641c7e483c3f17b28d0a59add0c8a44a4e4fc1dd3a9ea48bad8cf5b707ac0f44a5f3536

табл. 2

Ако хакер получи достъп до паролата ти от базата данни тя винаги ще бъде в хеш форма. Това което той прави е да я сравни с паролите от „Rainbow" таблицата. В случай, че твоята парола е **„000000"**, а алгоритъма, който е използвал сайта, за да я превърне в хеш е **SHA224** (виж табл. 2), хакерската програма я сравнява с тези от таблицата. Ако има съвпадение паролата ти е успешно хакната. Колкото по различна и уникална е паролата ти, толкова по-силна и надеждна е тя и вероятността тя да фигурира в „Rainbow" таблица е много малка или нулева.

При лесна парола като тази това се случва за по-малко от 1 секунда. Затова паролите не бива да съдържат често срещани думи или цифрови знаци. Колкото по различна и уникална е паролата ти, толкова по-силна и надеждна е тя.

Ето как често използваните сайтове като Facebook, Youtube, Twitter и много други се опитват да разрешат проблема с хакерските атаки. Това, което правят е да добавят „сол" към паролите в базата данни. „Солта" е поредица от символи, букви и цифри, които програмистите на сайтовете добавят към паролата преди да я превърнат в хеш и да замаскират паролата в „суров" вид.

Пример за „сол": $6i@

Нека приемем, че Facebook използва тази „сол" и я слага след всеки първи, четвърти и последен знак на паролите (тази информация е строго пазена от Facebook и в случая примера е измислен с примерна цел). В този случай паролата „000000", би изглеждала така:
0$6i@000$6i@00$6i@ (в „суров" вид продължава изглежда по този начин „000000").

След това се преобразува в хеш:

1085ed31e7101c67e4fae392b11fdb0eef6074a21af43f81e6f4d538

Ако го сравним с тези от горната таблица ще видим, че този хеш е напълно различен тези, когато паролата е без добавена „сол". Това е ефективен метод за предотвратяване на хакването на профили, чрез „Rainbow" таблиците. Въпреки това, е добре да направиш паролата си достатъчно силна. Ето защо:

Да кажем, че за Facebook използваш паролата „ytrewq"(qwerty на обратно). В случая Facebook ще добави „сол" към тази парола, но ти използваш същата парола и в друг сайт, който не добавя „сол" към паролите на потребителите си. Ако хакер „разбие" паролата ти в другия сайт ще има паролата ти и за Facebook.

Важно!

• Не използвай една и съща парола за всеки сайт, защото, ако тя бъде „разбита" всичките ти профили ще бъдат хакнати! Паролите за онлайн-банкиране трябва да бъдат съвършено различни от тези, които имаме в другите сайтове;
• Създай парола, която да съдържа букви (малки и големи), цифри и символи, която да е възможно най-уникална. Това е гаранция, че тя няма да бъде хакната чрез „Rainbow" таблиците;
• Ако влезеш в профила си от чуждо устройство не забравяй след това да излезеш от него и никога не разрешавай на браузъра да запомня паролата ти;
• Не съхранявай на компютъра си своите пароли, ПИН кодове, ЕГН и други подобни лични данни в текстов формат или под каквато и да било друга форма. Съществуват много злонамерени софтуери, които веднъж попаднали на устройството ти, търсят подобни данни, за да бъдат откраднати и използвани за „разбиване" на профилите ти;
• Не позволявай на браузъра да запомня паролите ти. Защо ли? Въпреки че това ти спестява времето, в което всеки път ще въвеждаш своята парола, съществува риск. Някой, който използва устройството ти в даден момент може да попадне в профила ти и дори има лесен начин, по който да разбере каква е тя, буквално за секунди. Още една причина е, че това се превръща в несъзнателен навик и следващия път, когато ти се наложи да използваш чуждо устройство, за да си провериш Фейсбука, може да я запазиш без дори да се усетиш.

Как да създадеш силна парола?

Противно на очакванията ти, това не е никак сложна задача. Когато създаваш парола единственото нещо, което трябва да направиш е добре да развихриш въображението си, защото това ще гарантира нейната уникалност.

Пример:

@3iuH1str0ngPd - тази парола съдържа в себе си изречението – „Аз и ти имаме една силна парола".

Аз - @3 (кльомба и числото 3)

и – i („и" изписано с латинска буква)

ти – u (от английската дума „you", използвайки само последната буква, която звучи по същия начин както се изговаря „you")

имаме – H (първата буква от английската дума „have“. Изписана е като главна за разнообразие).

силна – str0ng (английската дума „strong“, но изписана с нула вместо „o“)

парола – Pd (първата и последната буква от английската дума „password“, като първата е главна).

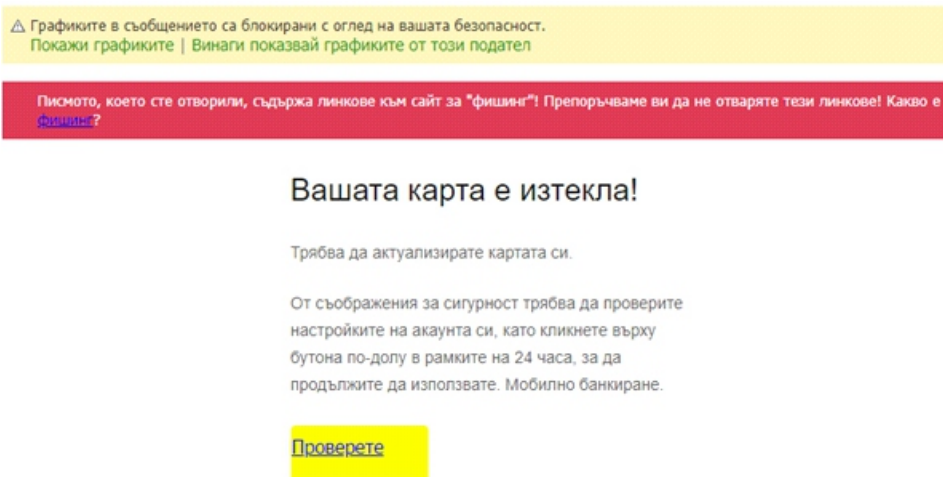
По този начин всеки един символ има някакво значение и това прави паролата в пъти по-лесна за запомняне и значително по-трудна за хакване, а с добавена „сол“ и превърната в хеш е на практика невъзможна за „разбиване“.

ОНЛАЙН ИЗМАМИ

Обект на измами са предимно пълнолетните лица, поради това, че имат банкови сметки, пазаруват онлайн работят или си търсят работа.

Класически пример за онлайн измама е **Phishing**, „фишинг" (идва от английската дума fishing, „риболов"). Това представлява линк, който е изпратен на обикновен потребите в повечето случаи чрез имейл съобщение.

Ето и пример за фишинг.



След като потребителят отвори линка е помолен да попълни своите лични данни като - име, парола, телефонен номер или друга лична информация. По този начин той сам дава своите данни на този, който е изпратил линка.

В други случаи може сам да попаднеш на линк за фишинг използвайки Google или друга онлайн търсачка. Необходима е секунда невнимание, за да отвориш линк, без да забележиш, че в адресната лента не е изписано оригиналното име на сайта, който искаш да посетиш. След което, въвеждайки своите потребителско име и парола, осигуряваш на някого достъпа до профила си.

Как да се предпазиш? Дори и да има проблем с данните ти е добре да знаеш, че банките нямат политика да изискват изпращането на твоята лична информация чрез Интернет. Те биха се свързали с теб по телефона и ще пожелаят да отидеш лично до офис на банката, за да им осигуриш необходимата информация.

ЗЛОНАМЕРЕН СОФТУЕР

Първата асоциация, която може би ти хрумва е - вируси. И въпреки, че често двете понятия се използват като еднозначни, то съществуват ключови разлики между тях.

Вирусите представляват вид злонамерен софтуер, който има способността да се възпроизвежда (копира) сам, като „заразява" различни файлове (снимки, видеа, текстови файлове и т.н) и ги препраща към други устройства. Тъй като те могат да „заразяват" само файлове, в днешно време те са лесно откриваеми дори от най-слабите антивирусни програми. Това е и причината вече да не са толкова широко разпространени.

От друга страна злонамерения софтуер е такъв, който е необходимо да бъде инсталиран (и това го прави различен от вируса) под формата на приложение (програма), от потребителя без да подозира, че го прави. Оттам този тип софтуер се дели на няколко типа според целите си:

• За проследяване и кражба на лични данни – наричат се ***KeyLoggers*** *(Кийлогърс)* и единственото, което правят е да проследяват действията на потребителя, докато използва устройството си. След, което запазва снимки на екрана, информация за това, къде е кликнато с мишката или какво е писано на клавиатурата в един регистър, до който има достъп създателят на този софтуер. Оттам той има информация за това, кои сайтове са посещавани, какви пароли са въвеждани и може да я използва, за да проникне в профилите на нищо неподозиращата жертва. Ако трябва да сравним този тип софтуер с реалния живот, то това е все едно някой да гледа през рамото ти, когато въвеждаш ПИН кода си на банкомата.

Начините да се предпазиш са да не теглиш файлове от съмнителни имейли, сайтове или такива изпратени ти от хора, които не познаваш. Освен това не бива да влизаш в своите профили от чужди устройства, тъй като не знаеш дали те не са наблюдавани от подобен софтуер, и разбира се никога от устройства, които са свързани към публични Wi fi мрежи.

• За криптиране – ***Ransomware*** *(Рансъмуер)* е софтуер, който притежава способността да заключва определени данни от устройството. По този начин ги прави недостъпни за потребителя, а уловката е, че той трябва да заплати определена сума, която хакера иска от него, за да му върне отново достъпа до данните. Сумата се изисква под формата на някоя криптовалута, защото така много по-трудно може да бъде открит престъпника, който получава парите. Най-често големи компании стават потърпевши, като статистиките сочат, че от този вид схема са нанесени щети за милиарди долари.

Въпреки това, ако имаш много ценна информация, която не би искал да загубиш или да се наложи да откупуваш от някого е добре да я запазваш на външен хард диск, който няма вътрешен достъп до операционната система на твоя компютър. В други случаи Ransomware-а може да блокира браузъра, или монитора ти като по този начин не заключва данните ти, но отново прави така, че да загубиш достъпа до тях и да направи компютъра ти неизползваем. Отново е добре да ти напомня, че трябва да внимаваш за местата, от които теглиш своите програми и да не се изкушаваш да теглиш нещо безплатно от „пиратски" сайтове.

• За безразборно изтриване на информация – ***Jigsaw Ransomware*** *(Рансъмуер „мозайка")* – Веднъж инсталиран на компютъра ти, той ще започне на абсолютно случаен принцип да трие информация от твърдия диск на компютъра ти. По този начин операционната система се срива, защото подобно на разбита мозайка, започват да липсват части от нея и тя не може да продължи да функционира нормално.

Този процес е необратим, за разлика от гореописаните. Затова обърни отново внимание на методите описани след тях, за да успееш да предотвратиш това да ти се случи!

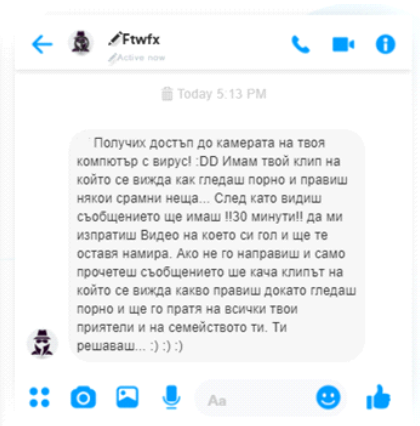
Trojan Horse *(Троянски кон)* – Всеки един от тези типове злонамерен софтуер може да бъде дегизиран като „Троянски кон". Това е отново тип злонамерен софтуер, който имитира обикновен безвреден софтуер. Най-често е под формата на **.exe** файл (файл за изпълнение), и щом го отвориш автоматично се инсталира на твоя компютър и започва да изпълнява това, за което е програмиран.

Какво може да направиш? Проверявай редовно дали антивирусната ти програма е актуализирана до последната налична версия. Ако има актуализации, които компютъра ти предлага да инсталираш, за да обновиш своята операционна система го направи без да отлагаш във времето. По този начин увеличаваш шансовете за засичане на подобен злонамерен софтуер, попаднал на компютъра ти.

ДРУГИ ОПАСНОСТИ

Понякога за съжаление жертвите сами привличат своите похитители. Пример за това е момиче или момче, което използва nickname (прякор) в социална мрежа, който е провокативен или със сексуален характер. Това дава знак на похитителя, че лесно може да започне приятелски разговор, който бързо да премине към сексуална тема. Оттам се увеличават и шансовете избраният човек да стане жертва на сексуална злоупотреба.

В други случаи подходът за злоупотреба може да е доста агресивен. Това е такъв пример:



Ако това се случи на теб е добре да знаеш, че в голям процент от случаите този, който изпраща съобщението всъщност не притежава такъв клип. Жертва ставаш тогава когато отговориш на съобщението и изпратиш клип, защото тогава вече наистина ще разполага с такъв материал, който ще използва срещу теб, за да продължи с тормоза и изнудването. Този метод е ефективен, тъй като използва страхът на жертвата от това, че има малко време, за да реши как да постъпи. Ето какво можеш да направиш в такава ситуация.

Първи вариант - ако все пак си отворил съобщението, можеш да поискаш да видиш въпросното видео, което имат и да помолиш за малко повече време за реакция. В това време, което ще спечелиш, подай сигнал за онлайн престъпление на някой от следните контакти:

- Валиден за целия европейски съюз номер за деца в риск **116 111**.
- E-mail адрес hotline@online.bg или helpline@online.bg.
- www.safenet.bg
- www.cybercrime.bg

Вторият вариант – той е по-скоро превантивен. Не отваряш текстови съобщения от съмнителни профили или от хора, които не познаваш. По този начин ще предотвратиш възможността да те изнудват. Така дори и да разполагат с подобно видео, то ще бъде безполезно за тях и техните цели.

Порнография

Интернет прави порнографското съдържание абсолютно достъпно за децата, което може да формира погрешни нагласи и разбирания за това кое е нормално и кое не. Примери:

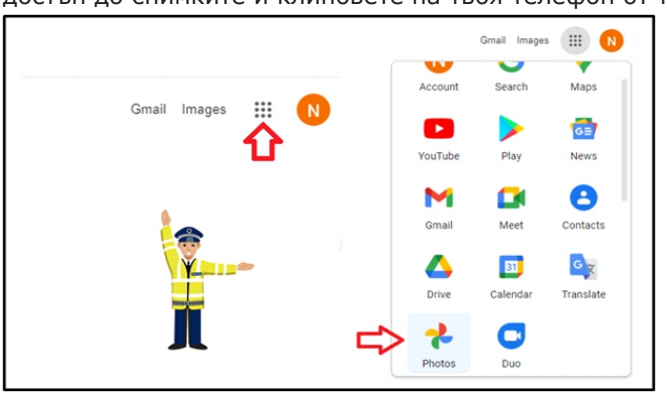
- Безопасността по време на секс не е нещо важно.
- Агресията в сексуалния акт е нещо нормално и дори привлекателно.
- Сексуални отношения, в които жената е изцяло доминирана са напълно нормални.
- Любовта не е на фокус в интимните отношения.

Дори е възможно при деца и тийнейджъри, които редовно гледат порнография да развият определени стереотипи за ролите на двата пола в една връзка. Това може да им попречи да бъдат в пълноценна връзка и да имат здравословен сексуален живот.

<u>Нещата, за които трябва да внимаваш и полезни съвети</u>

Забравен профил в Google.

Ако забравиш профила си в Google отворен на чуждо устройство рискуваш да станеш жертва на злоупотреба с твоите снимки и клипове намиращи се в твоя телефон. Това е възможно, тъй като често без да се замислим даваме разрешение на своя телефон да се синхронизира с профила ни в Google. Ако си забравиш профила отворен на чуждо устройство някой може да получи достъп до снимките и клиповете на твоя телефон от тук:



Забравен профил във Facebook.

Сигурно ти се е случвало да чуеш от твой приятел, че профилът му във Facebook е „разбит". „Разбитите" профили в много случаи изобщо не са резултат от хакване. Достатъчно е само да забравиш да излезеш от профила си, след като си влязъл от друго устройство в училище, на работа или използваш устройството на приятел или познат. Бъди внимателен и не забравяй бутона за изход от акаунта ти!

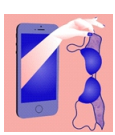
Не използвай Wi fi мрежи със свободен достъп.

Намираш се в центъра и решаваш да използваш Wi fi мрежата на някое кафене в близост до теб. По този начин поемаш огромен риск! Ето защо – някой, който също е в близост до това кафене, създава фалшива Wi fi мрежа със същото име като това на кафенето. От този момент нататък всеки, който се свърже с тази мрежа и я използва, за да влезе в своите акаунти, става жертва на кражба на лични данни, включително и ти. Създателя на тази мрежа има способността да следи всеки един поток от информация минаващ през нея и по този начин успява да хакне профилите на своите жертви. Този способ е също ефективен, когато извършителя иска да зарази потребителите на мрежата му със злонамерен софтуер.

Свържи всичките си акаунти със своя мобилен телефон ако това е възможно.

Много просто. Да приемем, че някой е разбрал каква е паролата ти. Ако той направи опит да влезе в този профил от друго (ново) устройство, ще се наложи да въведе, изпратения код за сигурност на твоя мобилен номер. В противен случай ще му бъде отказан достъп. С други думи трябва да притежава и паролата и телефона ти, за да успее да „разбие" профила, а това е малко вероятно.

Секстинг и рисковете които крие.



Секстинг представлява изпращането на снимки и видеа със сексуално съдържание. Дали някога си изпращал подобно съдържание и какъв е риска да бъде използвано срещу теб от някой на когото си го изпратил? Дори този някой да не е публикувал въпросните снимки, само секунда невнимание от негова страна може да е причината трети лица да ги видят. Тук твоята лична отговорност играе важна роля за предотвратяването на това. Ето защо не бива да изпращаш подобно съдържание на никого.

ПРИМЕРНИ ОБУЧИТЕЛНИ СЕСИИ ПО ТЕМАТА „БЕЗОПАСЕН ИНТЕРНЕТ".

Примерна Сесия 1: Въвеждащо обучение на тема „Безопасен интернет".
(метод: Брейнсторминг)

1. Представяне – **5 мин**.
- Кои сме ние?
- Днес ще поговорим за …
- Тази тема е актуална и важна, защото ...

2. Брейнсторминг – Какви са опасностите в интернет? – **5мин**.
(Основната идея на метода Брейнсторминг, използван точно в този момент, след представянето е изключително добър способ за ангажиране вниманието на аудиторията и провокиране на разсъждения по конкретната тема. Тук освен очакваното участие от аудиторията, процесът може да се допълни с ваши идеи или теми, които смятате, че е задължително да бъдат обсъдени. Добър начин за това е те да бъдат въведени като въпрос към аудиторията, например „Смятате ли, че тук има място и за тема като Трафик на Хора?").

Важно – Не пропускайте да завършите брейнсторминга с обобщение на изведените идеи и при необходимост, добавяне на такива.

3. Основна част от сесията: - *Приблизително* **25 - 30 мин**.

Обстойно разглеждане на някои от предложените теми:

- Онлайн измами;
- Социални мрежи;
- Пароли;
- Онлайн-тормоз;
- Трафикът на хора и Интернет.

Важно – Съобразете избора и реда на темите с интересите на групата, както и времето, което ще отделите за всяка една от тях. Не е необходимо всяка една от 6те предложени теми, да бъде засегната, а и не забравяйте, че имате пълната свобода да ги замените с други, например:

- Изнудване;
- Фишинг;
- Вируси;
- Онлайн отговорност;
- Мерки за предпазване.

4. Заключение: **5 мин.**

Примери:
- Обратна връзка (Полезна ли Ви бе темата?; Кое бихте искали да обсъдим следващия път?; Какво ви заинтригува най-много?)
- Насочване към допълнителни информационни ресурси по темата и насърчаване към сигнализиране за онлайн злоупотреби: safenet.bg, cybercrime.bg
- Повече за нас може да научите на сайта: prevencii.com

Обща продължителност: **45 мин**.

Примерна Сесия 2: Въвеждащо обучение на тема „Безопасен интернет".
(метод: Визуализация)

1. Представяне – **5 мин.**
- Кои сме ние?
- Днес ще поговорим за …
- Тази тема е актуална и важна, защото ...

2. Визуализация (В случай, че разполагате с мултимедия и подходящи материали). - **10мин**.

➢ Видео материал –
Пример: Сега бихме искали да ви представим нагледно една от темите, на които днес искаме да обърнем внимание.
➢ Презентация.
➢ Реални примери за злоупотреби, фалшиви сайтове, интернет измами, потенциално опасно поведение онлайн. (Тези примери бихме могли да презентираме под формата на снимков материал или показване в реално време.

(Основната идея на визуализацията като метод е да представи нагледно темата, която предстои да бъде обсъдена. Това е добър подход, предвид факта, че повечето хора възприемат по-лесно информация, когато е представена визуално).

Важно – От предвидените 10 минути, следва да бъдат отделени, не повече от 5 до 6 минути за визуално представяне на материал/и. В останалото време, след края на визуализацията, е важно да обобщим видяното. Това може да се осъществи чрез кратка дискусия с групата или чрез директно въведение в една от темите, „загатнати" в показания материал.

3. Основна част от сесията: - *Приблизително* **25 мин**.
Обстойно разглеждане на предложените теми:

➢ Онлайн измами;
➢ Социални мрежи;
➢ Пароли;
➢ Онлайн-тормоз;
➢ Трафикът на хора и Интернет.

Важно – Съобразете избора и реда на темите с интересите на групата, както и времето, което ще отделите за всяка една от тях. Не е необходимо всяка една от 6-те предложени теми, да бъде засегната, а и не забравяйте, че имате пълната свобода да ги замените с други, например:
➢ Изнудване;
➢ Фишинг;
➢ Вируси;
➢ Онлайн отговорност;
➢ Мерки за предпазване.

4. Заключение:
Примери:
- Обратна връзка (Полезна ли Ви бе темата?; Кое бихте искали да обсъдим следващия път?; Какво ви заинтригува най-много?)

- Насочване към допълнителни информационни ресурси по темата и насърчаване към сигнализиране за онлайн злоупотреби: safenet.bg, cybercrime.bg
- Повече за нас може да научите на сайта: prevencii.com.

Обща продължителност: **45 мин**.

***

Примерна Сесия 3: Въвеждащо обучение на тема „Безопасен интернет".
(метод: Казуси)

1. Представяне – **5 мин.**
- Кои сме ние?
- Днес ще поговорим за …
- Тази тема е актуална и важна, защото ...

2. Подготовка за работа по казуси – 1**0мин**.
Този метод е по-подходящ за по-напредналите доброволци (обучители). Изискват се умения за работа с групи, наблюдателност, подготовка, умения за справяне с различни видове групи (активни, пасивни, агресивни и т.н).

Примерен казус 1:
Ваша приятелка ви споделя, че преди час неизвестно лице се е свързало с нея в социална мрежа, твърдящо, че притежава нейни голи снимки. Човекът изисква от нея, след 30 минути, да си включи камерата и да позира гола в продължение на няколко минути, за да не разпространи снимките, които има в социалните мрежи. Как бихте й помогнали? (Време за работа по групи – **7-8 минути**).

➢ *След решаването на казуса, можете да попитате групата следното: „Бихте ли споделили, ако на вас ви се случи подобно нещо?*"

Примерен казус 2:

Мария, току що навършила 20 години, е момиче с много силно присъствие в Инстаграм. Профилът и има над 30,000 последователи, а снимките, които качва са меко казано предизвикателни като основно снима тялото си и снимките и получават средно около 100 000 харесвания за отрицателно време. Вчера тя е получила бизнес предложение от непозната жена, която се представя за собственик на фирма, занимаваща се с продажба на бански костюми. Офертата е да стане тяхно рекламно лице срещу доста добро заплащане. Условията, които й поставят са да им изпрати кратко видео, в което позира с най-изрязаното бельо, което има, за да видят дали тялото и отговаря на техните изисквания и дали реално тя стои зад този профил. Тя изпраща видеото, след което получава покана за интервю в съседен град, на което предстои да бъдат направени пробни снимки с техните продукти. Тя е твърдо решена да отиде, но не иска да казва никого. Мария се свързва с вас и ви моли да отидете с нея на интервюто, за да не е сама и това да си остане само между вас. Как бихте постъпили? (Време за работа по групи – **7-8 минути**).

Указания: Разделете аудиторията на две или повече РАВНИ групи като заданието и на двете групи е да представят всевъзможни решения на казуса, след което да се обсъдят и да се изведе най-доброто възможно решение.

Важно - Наблюдавайте внимателно работата на групите и спазвайте стриктно времето, което сте им задали за работа. Напомняйте им, че времето за вземане на решение е ограничено. В случай, че един казус се изчерпа бързо, можете спокойно да използвате втори казус. Преди да започнат работа по казуса, кажете на групите, че търсим възможно най-много решения на казуса и че всяко предложено такова е ценно.

3. Основна част от сесията: - *Приблизително* **20-25 мин**.
Обсъждане на предложените решения.

- Дайте възможност на групите да се редуват в предлагането на възможни решения.
- Старайте се да включите максимален брой участници в предлагането и дискутирането на решенията.

Важно – След като изчерпаме максимално темата е важно да дадем възможност на всеки, който би искал да смени групата си, да го направи. С това целим да установим дали дискусията е повлияла по някакъв начин на тяхното мнение по темата.

4. Заключение:
Примери:
- Обратна връзка (Полезна ли Ви бе темата?; Кое бихте искали да обсъдим следващия път?; Какво ви заинтригува най-много?)
- Насочване към допълнителни информационни ресурси по темата и насърчаване към сигнализиране за онлайн злоупотреби: safenet.bg, cybercrime.bg
- Повече за нас може да научите на сайта: prevencii.com.

Обща продължителност: **45 мин**.

***

Примерна Сесия 4: Въвеждащо обучение на тема „Безопасен интернет".
(метод: Дискусия)

1. Представяне – **5 мин.**
- Кои сме ние?
- Днес ще поговорим за …
- Тази тема е актуална и важна, защото ...

2. Подготовка за дискусия – **10мин**.
Методът дискусия е по-подходящ за по-напреднали обучители. Преди да изберете този метод се уверете, че сте максимално подготвени по темата.

Въпрос: Какви са ползите и негативите от социалните мрежи за нас?

Указания: Разделете аудиторията на две РАВНИ групи като заданието на едната е да помисли и изведе САМО ползите от социалните мрежи, а другата САМО негативите. (Време за подготовка – 5 **мин**).

Важно - Наблюдавайте внимателно работата и на двете групи и преценете по какъв начин ще успеете да включите в дискусията максимален брой от участниците. Мислете за последващи въпроси в случай, че групата е пасивна и има необходимост от допълнителна провокация. (въпроси, чиито отговори биха провокирали всеки).

Например:
- Каква е ползата от броя на харесванията и споделянията, които получаваме в социалните мрежи?
- Защо се чувстваме зле, когато присъствието ни в социалните мрежи не е високо оценено?
- Кога и как разбираме, че сме достатъчно оценени в социалните мрежи?

Важно!
С приоритет са въпроси, които възникват в процес на дискусията. Въпросите, предложени от нас, са само в случай, че аудиторията е пасивна.

3. Основна част от сесията: - *Приблизително* **25 мин**.
Провеждане на дискусията.

- След всяка изложена теза, дайте възможност на „опониращата група" да изложи контра-аргументи.
- Включете максимален брой участници в дискусията. (Това би могло да се постигне с помощни въпроси от типа: „Някой може ли да допълни с нещо?", „Кой друг споделя това мнение? Защо?", „Има ли някой, който не е съгласен с това мнение? Защо?".
- Не забравяйте, че ВИЕ водите дискусията и винаги можете да посочите някой, който да сподели собственото си мнение.

Важно – След като изчерпаме максимално темата е важно да дадем възможност на всеки, който би искал да смени групата си, да го направи. С това целим да установим дали дискусията е повлияла по някакъв начин на тяхното мнение по темата.

Най-важното! Бъдете максимално подготвени по темата. Не бихте искали успехът на дискусията да зависи изцяло от работата и активността на групата!

4. Заключение: - **5 мин**.
Примери:
- Обратна връзка (Полезна ли Ви бе темата?; Кое бихте искали да обсъдим следващия път?; Какво ви заинтригува най-много?)
- Насочване към допълнителни информационни ресурси по темата и насърчаване към сигнализиране за онлайн злоупотреби: safenet.bg, cybercrime.bg
- Повече за нас може да научите на сайта: prevencii.com.

Обща продължителност: **45 мин**.

2022

EMAIL

prevencii.varna@gmail.com

WEB

www.prevencii.com
www.p2prevention.bg
www.safenet.bg
www.cybercrime.bg