ГИМНАЗИЯ С ПРЕПОДАВАНЕ НА ЧУЖДИ ЕЗИЦИ „ЙОАН ЕКЗАРХ“ – ВАРНА
9010 Варна, кв. „Чайка“, п.к. 148; тел. +359 52 302376, veg_varna@5eg.org; http://5eg.org

УТВЪРЖДАВАМ:
ЕМИЛИЯ ВЛАДОВА
Директор на ГПЧЕ "Йоан Екзарх"

ПРАВИЛА ЗА БЕЗОПАСНОСТ НА УЧЕНИЦИТЕ И СЛУЖИТЕЛИТЕ В ГИМНАЗИЯ С ПРЕПОДАВАНЕ НА ЧУЖДИ ЕЗИЦИ „ЙОАН ЕКЗАРХ“ В УЧИЛИЩНАТА КОМПЮТЪРНА МРЕЖА И В ИНТЕРНЕТ ЗА УЧЕБНАТА 2026-2027 ГОДИНА

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Тези правила уреждат основните принципи на училищната политика, правомощията на училищното ръководство, педагогическия персонал и системния администратор, както и правата и задълженията на учениците и родителите, свързани с работата на учениците в училищната мрежа и в Интернет, наричани по-нататък за краткост "мрежата". Правилата са съобразени с изискванията на Европейската комисия по безопасно сърфиране в Интернет и Европейската стратегия за по-добър интернет за децата от 2012 г.

Чл. 2. Училищната политика за работа в Интернет има за цел да осигури и организира използването на образователния потенциал както на училищната мрежа, така и на глобалната мрежа, в съчетание със система от мерки за сигурност и безопасност на учениците.

Чл. 3. Основните принципи на училищната политика за работа в училищната мрежа и в Интернет са:

1. Равен достъп на всички ученици до училищната мрежа;

2. Защита на учениците и служителите на ГПЧЕ „Йоан Екзарх“ от вредно или незаконно съдържание и информация като: кражба на лични данни и снимки, накърняване на личното достойнство и тормоз, порнография, проповядване на насилие и тероризъм, етническа и религиозна нетолерантност, търговия с наркотици, хазарт и др.;

3. Зачитане и защита на личната неприкосновеност;

4. Подготовка и контрол на учениците за компетентно и отговорно поведение;

5. Сътрудничество между училището, родителите и компетентните органи;

Чл. 4. Училищната компютърна мрежа и Интернет се използват от учениците само за образователни цели.

Чл. 5. Правилата за безопасна работа в Интернет, които учениците са задължени да спазват, се поставят на видно място във всеки компютърен кабинет.

II. ПРАВОМОЩИЯ НА ДИРЕКТОРА НА УЧИЛИЩЕТО

Чл. 6. (1) Директорът е длъжен да:

1. Организира и контролира цялостната дейност по изпълнението на тези правила;

2. Осигурява и насърчава свободния и равен достъп на учениците до училищната мрежа и Интернет в съответствие с учебния план и възможностите на училището;

3. Създава възможности за обогатяване и разширяване на образователния процес чрез училищната мрежа и Интернет, включително и в извънучебно време;

4. Утвърждава график за работа на учениците в училищната мрежа и в Интернет извън редовните учебни занятия;

5. Организира и контролира прилагането на мерки, включително и съвместно с Интернет доставчика, ограничаващи достъпа на учениците до вредно или незаконно съдържание в Интернет в съответствие с действащото законодателство в Република България;

6. Предварително одобрява материалите за публикуване в училищния сайт и осигурява наблюдение и контрол върху неговото съдържание в съответствие с принципите на училищната политика;

7. Осигурява ефективен постоянен контрол по спазване на правилата за работата на учениците в училищната мрежа и в Интернет;

8. Осигурява здравословни и безопасни условия на работните места в съответствие с нормативните изисквания;

9. Осигурява при техническа възможност проследяване на трафика, осъществяван чрез училищната мрежа;

10. Информира учениците, че трафикът се следи и при констатирани нарушения може да бъде установено лицето, което ги е извършило;

11. Уведомява родителите за предприетите от ръководството мерки за осигуряване на безопасен и контролиран Интернет достъп в училище;

12. Уведомява незабавно компетентните органи при констатиране на незаконно съдържание в училищната мрежа и в Интернет;

13. Организира в началото на всяка учебна година запознаване на учениците и родителите с училищните правила за безопасна работа в мрежата;

14. Осигурява отговорно лице, което да изпълнява функциите на системен администратор;

15. Предприема мерки за реализиране на отговорността на виновните лица при констатирани нарушения на тези правила;

(2) Директорът може да възлага със заповед изпълнението на задълженията си по ал. 1, т. 5, 6, 7, 9, 10 и 11 на други служители от училището.

III. ПРАВОМОЩИЯ НА УЧИТЕЛИТЕ, РЪКОВОДИТЕЛЯТ НАПРАВЛЕНИЕ ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Чл. 7. Учителите, ръководителят направление информационни и комуникационни технологии са длъжни да:

1. Разясняват правилата за безопасно и отговорно поведение при работа в училищната мрежа и в Интернет.

2. 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.

3. Осъществяват непрекъснато наблюдение и контрол върху работата на учениците в училищната мрежа и в Интернет в учебно и в извънучебно време.

4. Предприемат незабавни мерки за преустановяване на достъпа на учениците до незаконно съдържание в мрежата.

5. Уведомяват незабавно директора на училището при нарушаване на правилата или при установяване на незаконно съдържание в мрежата.

Чл. 8. Учителите, директорът, ръководителят направление информационни и комуникационни технологии не носят отговорност, ако учениците случайно или преднамерено попаднат на вредно или незаконно съдържание в Интернет.

Чл. 9. Ръководителят направление информационни и комуникационни технологии е длъжен да:

1. Осигурява общата безопасност и работоспособност на мрежата.

2. Предлага и прилага мерки, ограничаващи достъпа на учениците до вредно или незаконно съдържание в Интернет в съответствие с действащото законодателство на Република България.

3. Извършва периодичен преглед на училищната мрежа за наличие на възможни заплахи и рискове за сигурността на учениците при работа в Интернет.

4. Следи трафика, осъществяван чрез училищната мрежа.

5. Поддържа и актуализира училищната Интернет страница в съответствие с изискванията на училищната политика.

6. Публикува в училищната Интернет страница само одобрени от директора материали.

7. Уведомява незабавно директора на училището при нарушаване на правилата или при установяване на незаконно съдържание в мрежата.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА УЧЕНИЦИТЕ

Чл. 10. Учениците имат право на:

1. Равен достъп до училищната компютърна мрежа и в Интернет, при спазване на училищната политика.

2. Работа в мрежата и в извънучебно време по утвърден от директора график.

3. Работа в мрежата само под контрола на определено от директора лице.

4. Обучение за компетентно и отговорно поведение в училищната компютърна мрежа и в Интернет.

5. Да бъдат информирани за училищната политика за работа в мрежата.

Чл. 11. Учениците са длъжни да спазват следните правила за безопасна работа в мрежата:

1. Училищната мрежа и Интернет се използват само за образователни цели.

2. Забранено е използването на мрежата за извършване на стопанска или незаконна дейност.

3. Учениците не трябва да предоставят лична информация за себе си и за своите родители като име, парола, адрес, домашен телефон, училище или месторабота и служебен телефон на родителите, без предварително разрешение от тях;

4. Не се разрешава изпращане или публикуване на снимки на ученици или на техни близки, без предварително съгласие на родителите;

5. Учениците не трябва да приемат срещи с лица, с които са се запознали в Интернет, освен след съгласието на родителите;

6. Учениците са длъжни да информират незабавно лицето, под чието наблюдение и контрол работят, когато попаднат на материали, които ги карат да се чувстват неудобно, или на материали с вредно или незаконно съдържание като порнография, проповядване на насилие и тероризъм, етническа и религиозна нетолерантност, търговия с наркотици, хазарт и др.;

7. Учениците не трябва да изпращат или да отговарят на съобщения, които са обидни, заплашващи или неприлични;

8. Учениците не трябва да отварят приложения на електронна поща, получена от непознат подател.

9. Забранено е изпращането на анонимни или верижни съобщения.

10. Забранено е извършването на дейност, която застрашава целостта на училищната компютърна мрежа или атакува други системи.

11. Забранява се използването на чуждо потребителско име, парола и електронна поща.

12. Учениците не трябва да представят неверни данни за себе си с незаконна цел.

13. Забранено е използването на нелицензиран софтуер, на авторски материали без разрешение, както и всяка друга дейност, която нарушава авторски права.

14. При работа в мрежата учениците трябва да уважават правата на другите и да пазят доброто име на училището.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА РОДИТЕЛИТЕ

Чл. 12. Родителите имат право:

1. Да бъдат информирани за училищната политика за безопасна работа в мрежата.

2. Да дават свои предложения в определянето на насоките и мерките за безопасно използване на Интернет в училище.

3. Да получават информация за рисковете и заплахите за безопасността на техните деца при работа в Интернет в училище и вкъщи.

4. Да бъдат своевременно информирани и да участват съвместно с училищното ръководство при разрешаване на всеки конкретен проблем, свързан с нарушаване на правилата от страна на техните деца.

5. Да сигнализират училището, когато получат информация за нарушения по чл. 11.

6. Родителите са длъжни да осигурят контрол и помощ на децата си при ползването на глобалната мрежа – социални мрежи, чатове, приложения и др., както и при спазване на правилата за Интернет безопасност в училище.

Чл. 13. В началото на всяка учебна година родителите се запознават с училищните правила за безопасна работа в училищната мрежа и в Интернет, което удостоверяват с подписа си.

VI. ОТГОВОРНОСТ

Чл. 14. При нарушаване разпоредбите на тези правила на учениците могат да се налагат санкции, предвидени в ЗПУО и Правилника за дейността на училището. Училището и неговите служители вкл.

директор могат да окажат съдействие, но не носят отговорност при случайно или преднамерено нарушаване на тези вътрешни правила като частни случаи от ученици, служители, родители или външни за общността лица.

Чл. 15. Независимо от отговорността по чл. 14, при нарушения, които представляват престъпления, административни нарушения или причиняват имуществена вреда, се носи съответно наказателна, административна или гражданска отговорност.

Настоящите правила са утвърдени със Заповед № РД 09-3/15.09.2026 г. на директора на училището и е в сила до отменянето му по реда на неговото издаване.

ПРИЛОЖЕНИЕ 1

НАРЪЧНИК
ЗА СИГУРНОСТ И БЕЗОПАСНОСТ В ИНТЕРНЕТ

I. ОБЩИ ПРАВИЛА:

1. Не давайте лична информация като име, пароли, адрес, домашен телефон, училището, в което учиш, месторабота или служебен телефон на родителите си/ колегите си/ съучениците си, без тяхно разрешение.

2. Не изпращайте свои снимки или снимки на приятели, съученици, роднини, колеги, учители, познати и др. без преди това да е обсъдено решението с тях или с родители.

3. Не отговаряйте на съобщения, които са обидни, заплашващи, неприлични или ви карат да се чувствате неудобно. Информирайте родителите си/класния ръководител, учител, директор за такива съобщения.

4. Не отговаряйте на електронна поща, получена от непознат подател. Тя може да съдържа вирус или друга програма, която да увреди твоя компютър/ телефон/ таблет.

5. Консултирайте се с родителите си/компетентен колега/учител преди да свалите или инсталирате нова програма/приложение на компютър, телефон, таблет, както и не правете нищо, което може да увреди компютъра ви или чрез дадено действие да се разкрият данни за теб и семейството ти.

6. Нещата, които правите в Интернет, не трябва да вредят на други хора или да противоречат на законите.

7. Внимавайте, когато разговаряте в чат. Помнете правило №1, и че хората онлайн често се представят за такива, каквито не са или търсят определена информация.

8. Ако се случи така, че да попаднете на информация или друго в Мрежата, която не ви харесва или ви плаши по някакъв начин, то можете да подадете сигнал в ДАЗД на тел. 02/933 90 50, Национална телефонна линия 080 019 100, на адрес: web112.net / blob.bg или в Районно управление по местожителство, както и на http://www.cybercrime.bg/bg.

II. КАЧВАНЕ И СПОДЕЛЯНЕ НА СНИМКИ

Неподходящите снимки или видео на дете/ученик/родител/учител са публично достъпни публикации в интернет, които могат да са качени от родителите или други членове на семейството, приятели, съученици и др., които имат изцяло добри намерения към него/нея. Препоръчително е по никакъв повод да не се качват снимки на дете, за които има и най-малкото съмнение, че могат да му навредят. Все пак, споделянето на снимки е често срещано явление в социалните мрежи, затова основна препоръка е подобни снимки да се споделят само с хората от списъка с приятели на човека, който иска да качи снимката, и още по-добре - само с групата на най-близки приятели от реалния живот. Когато снимате със смартфона си, уверете се, че снимките не се качват автоматично в профила на родителя или детето в сайтове като Инстаграм например. В профилите си в социалните мрежи се уверете, че сте настроили снимките си така, че да се виждат само от приятелите Ви. Същото се отнася и за настройките на облачни услуги, в които се съдържат снимки и информация.

1. Снимките на малолетни и непълнолетни, показващи разголени части или сексуални пози, се считат от закона за детска порнография и се премахват от интернет пространството, като се преследват онези, които ги разпространяват. Освен че е важно за един подрастващ човек да уважава тялото и

личността си и да не публикува свои разголени снимки в мрежата, от такова значение е и уважението към интимността и личността на другите.

2. За по-големите тийнейджъри, най-големият риск идва от споделянето на интимна снимка в сайтове за запознанства или от изпращането на такава снимка до близък приятел или гадже, които неволно или умишлено я разпространяват до повече хора. Примерна ситуация - двойка се разделя и едната половинка решава да си отмъсти и да сподели гола снимка на другия в интернет като отмъщение. Освен това, не бива да се пренебрегва фактът, че тийнейджърите са чувствителни към нещата, които техните родители или роднини може да споделят за тях в мрежата. Затова е препоръчително всички публикации, на които те присъстват, да се обсъждат предварително с тях и те да ги одобряват.

3. Големите ученици могат да си изпатят от стара снимка, която някой разчувствал се роднина е споделил за тях в интернет. Тийнейджърите са чувствителни по отношение на имиджа си и бебешките снимки може да не им се сторят толкова сладки, колкото на родители или роднини. Добре е да се разговаря с тях и за онлайн репутацията и влиянието, което свързаните с тях публикации могат да имат един ден върху тях, когато могат да бъдат видени от нови приятели в университета или пък от потенциален работодател.

4. Най-добрата превенция срещу такова съдържание е да не се качват снимки, които по някакъв начин могат да предизвикат дискомфорт в момента или впоследствие. В интернет, снимките и съдържанието остават за дълго и могат да бъдат сваляни и използвани за цели, съвсем различни от първоначалните. Също така, веднъж щом нещо се появи в интернет е почти невъзможно то да бъде премахнато завинаги.

5. Секстинг се нарича размяната на съобщения, снимки или клипове със сексуално съдържание между двама партньори. Думата е съставена от думите „секс“ и „текстинг“ (писане на съобщения на английски).

Секстингът:

- най-често съдържа разголени снимки, но може да съдържа и клипове с друго сексуално съдържание;
- е практикуван както от възрастни, така и от тийнейджъри и понякога деца;
- обикновено се случва доброволно във връзката или флирта между връстници;
- може да доведе до тормоз в истинския свят и в интернет, ако такива снимки или видео бъдат споделени с други хора;
- може да доведе до опити за съблазняване на дете или тийнейджър от страна на възрастен, които се наричат още "груминг" (от английски - подготвяне).
- Последствията: Няма гаранция, че момиче или момче в даден момент няма да реши да си направи по-разголени снимки, които да иска да сподели с гаджето си. Важното е детето/тийнейджърът да е наясно с възможните последствия от секстинга, за да помисли добре, преди да сподели свои разголени снимки:

  - Дори човекът, получил снимката, да не я разпространи умишлено, възможно е някой друг да попадне на нея в телефона, таблета или на лаптопа му/й, след което да реши да я сподели в интернет;
  - Веднъж щом се появят в интернет, снимките и видеата остават там за дълго, ако не и завинаги, а и всеки може да ги свали и да ги използва по какъвто начин реши;

- Макар в даден момент разголените снимки да изглеждат вълнуващи и секси за един тийнейджър, след време те могат да се използват за отмъщение от наранен партньор при раздяла.

- Блокиране и сигнализиране: Потребителят, който е разпространил снимката, трябва да бъде блокиран и докладван на администраторите на сайта. Също така препоръчваме снимката или видеото да бъдат докладвани и на Горещата линия за безопасен интернет или на отдел "Киберпрестъпления" ГДБОП.

III. ОНЛАЙН ТОРМОЗЪТ

Представлява използването на интернет за нанасяне на емоционална вреда върху други хора. Тормозът в интернет може да придобие различни форми. Той може да се състои от създаване на подигравателни видеоклипове или фалшиви профили в социални мрежи като Ask.fm, Фейсбук и Инстаграм, сайтове за споделяне на видео като Vbox7 и YouTube, както и в приложения за комуникация, като Скайп и Вайбър, или в изпращането на обидни съобщения и коментари, чрез същите тези сайтове и платформи. Онлайн тормозът:

- е насочен към по-уязвим познат или съученик, който понася негативни последствия – чувства се зле, става обект на присмехи в училище, затваря се в себе си;
- може да се случва 24/7, защото интернет е достъпен навсякъде и по всяко време;
- обхваща много по-широк кръг от хора, освен единствено семейството и приятелите на младежите, тъй като интернет пространството има огромен брой потребители; може да започне като безобидна шега, но може да бъде и целенасочено отмъщение;
- може да предизвика нежелание за ходене на училище и за общуване, страх от използването на интернет, изолиране от другите, тревожност, дори телесни симптоми като главоболие и болки в стомаха.
- Настройки за сигурност на снимки в социалните мрежи. Често пренебрегвана стъпка при създаването на профили в социални мрежи или споделянето на снимки, е внимателното разглеждане на настройките за сигурност. Добре е родителят да помогне на младия интернет потребител да направи настройките си така, че снимките и публикациите, които той/тя качва в социалните си мрежи, да бъдат видими само от хората в списъка му/й с приятели. Така, рискът лични снимки да бъдат свалени и използвани за направата на колаж, или разпространени в други сайтове без знанието на детето, се намалява значително.
- Прекратяване на комуникацията. Препоръчва се детето да прекрати както разговорите с човека, който го тормози, така и да спре да следи неговите публикации и коментари. Най-добрият вариант е потърпевшият да блокира профила на въпросния човек или хора и да докладва както профила, така и неприятните за него снимки, коментари или публикации. По този начин, конфликтът няма да се засили допълнително, а съдържанието може да бъде изтрито от администраторите. Във всеки случай трябва да се запазят доказателствата за тормоза. Това може да стане със скрийншотове (заснемане на екрана) или с изтегляне на съдържанието, преди то да бъде изтрито от създателя му, в опит да се предпази от последствия.
- Ангажиране на средата. Тормозът е групов феномен. Въпреки че най-видимите участници са потърпевшия/потърпевшата и насилника, в действителност има и други въвлечени хора в ситуацията – поддръжници на тормоза и защитници на оправдания, пасивни наблюдатели, симпатизиращи на жертвата или забавляващи се от ситуацията, покрай които тормозът се случва.

IV. КРАЖБАТА НА ПРОФИЛ

Представлява присвояването на чужд потребителски профил в социална мрежа, платформа за общуване (например Фейсбук), електронна поща или друг сайт. Кражбата става възможна чрез влизане с правилната парола и нейната подмяна с нова и неизвестна за човека, на когото принадлежи профила. Възможно е, след кражбата профилът да се използва без знанието и съгласието на първоначалния собственик. Ако на дете под задължителната за повечето социални мрежи възраст от 13 години (тази възраст е такава, защото по-голямата част от популярни социални мрежи са американски и правилата за ползване са съобразени с американското законодателство) се създава собствен профил във Фейсбук, много е важно при избора на възраст да се избере под 18 години, тъй като за непълнолетните потребители има важни допълнителни защити. Кражбата на профил :

- включва смяната на оригиналната парола, така че собственикът на профила да не може да влезе в него;
- може да включва и смяната на имейл-адреса, с който е регистриран профилът;
- може да бъде част от онлайн тормоз;
- може да доведе до публикуването на снимки и коментари, които собственикът не би публикувал, или до разпращането на съобщения с неприятно съдържание, обиди или заплахи до списъка с приятели на профила.
- Силна парола. Най-често кражбите на профили стават заради лесно разгадаема парола или споделяне на паролата с други хора. На първо място, добре е паролата да бъде достатъчно сложна и трудна за разбиване. Какво означава това? – тя трябва да съдържа минимум 8 символа, от които главни и малки букви, цифри и знаци, като е препоръчително и да не бъде свързана дума. На второ място, паролата е добре да се знае само от собственика на регистрирания профил и да не се споделя с никого, освен с родителите. Третата препоръка е паролата да се сменя достатъчно често – поне веднъж на 6 месеца. Четвърто, силно препоръчително е да се използват различни пароли за различните регистрации на децата (важи и за големите) - по този начин, кражбата на един профил е по-малко вероятно да доведе до кражба и на друг, в различен сайт.
- Допълнителен имейл адрес. Във Фейсбук може да се добави втори имейл адрес към профила, така че ако случайно паролата и оригиналният имейл бъдат откраднати, може да се поиска смяна на паролата през алтернативна поща.
- Лична информация. Препоръчително е детето да споделя възможно най-малко информация за себе си като име, телефон, адрес, училище, снимки.

V. КРАЖБАТА НА ЛИЧНИ ДАННИ

Вид компютърно престъпление, при което се придобиват чужди лични данни, с цел финансова измама или злоупотреба, като теглене от и изразходване на банкова сметка, или кандидатстване и получаване на кредит от чуждо име. Тази опасност, по принцип, не засяга по-малките деца, които не притежават лични документи, банкови сметки или карти. Въпреки това, при тийнейджърите над 14-годишна възраст, този риск става актуален. Кражбата на лични данни:

- се нарича още фишинг (от английската дума за риболов);
- най-често включва искане на лични данни, под претекст за обновяване на базата данни на банка, онлайн магазин, разплащателна система, искане на данни за онлайн профил, под претекст за блокирането му, продажба на стоки, правене на дарение;

- се прави често посредством фалшив имейл от името на съответна финансова или престижна институция или компания.
- Антивирусна програма. Препоръчително е инсталирането на антивирусна програма на личния компютър. Програмата сканира и отстранява вреден софтуер (вирус), който може да се сдобие с пароли и лични данни, запаметени в компютъра. Всеки свален от интернет, или получен от външен източник файл, задължително трябва да се сканира преди отваряне.
- Верижен имейл. Съществуват измами, които под претекст за спешност или важност, изискват от потребителите да препращат получения имейл на техни познати. Най-често, по този начин се разпространяват компютърни вируси. Такива покани за препращане трябва да се игнорират.
- Откраднати банкови данни. При кражба на банкови данни, трябва веднага да се съобщи във финансовата институция, за да се закрие достъпът до сметката.
- Откраднати лични данни. В такъв случай, трябва да се съобщи в МВР и другите институции, издали данните (например КАТ за шофьорска книжка). Потърсете съдействие и от ГДБОП.
- Игри със заплащане. Някои измами в интернет се възползват от неопитността и желанието за забавление на малките деца или млади хора. Измамниците създават, или се възползват, от онлайн игра, за да убедят нейните потребители да платят, за да получат бонус точки или друг вид награди в играта. Често, тези измами се случват през СМС, и значително увеличават сметката на мобилните услуги. В такива случаи е важно бързо да се сигнализира на мобилния доставчик за номера, на който децата са изпращали СМС, и той да бъде блокиран.

VI. РОДИТЕЛИТЕ

Важно и необходимо е да помогнат на децата да изградят умения за общуване и боравене с огромно количество информация, ако искат те да са в безопасност.

- Отделете време да сърфирате заедно, да изследвате нови приложения и сайтове или да играете заедно на любимите му игри. Достатъчно е дори ако Ви разказва и показва какви игри харесва и как се играят. Ако и Вие обичате да играете – прекрасно! Това е чудесен начин да разберете какво прави детето Ви в интернет, с кого и как общува там. Така и Вие ще сте по-осведомени и ще изградите по-голяма близост и доверие с детето си и във виртуалния свят.
- Разговорите е добре да се превърнат в обичайна част от общуването с детето. Избягвайте ситуации тип „полицейски разпит“. За целта е добре въпросите да не са осъдителни, а да са добронамерени и да показват искрена заинтересованост и любознателност. Ето няколко въпроса, които биха могли да Ви бъдат от полза: - Какви сайтове и приложения посещаваш? Разкажи ми повече за тях. (Добре е един подобен разговор да започне непринудено и естествено.) - С какво са ти интересни тези сайтове и приложения? - Иска ли се регистрация, за да влезеш в тях? - Какво освен имейл е нужно, за да се регистрираш? (Дали сайтът изисква име, адрес, телефон, други лични данни? Това е удачен момент да разкажете на детето какво са „лични данни“, кои не е добре да бъдат публикувани и кои може да споделя в интернет). - Хайде да разгледаме заедно какви са възможностите за настройки на профила ти? А как можеш да потърсиш помощ или съвет?
- От техническа гледна точка има няколко начина да повишите сигурността за Вашето дете: - Инсталирайте приставката WOT (Web of Trust) към браузъра на настолния компютър или лаптоп, който използва детето ви. Тя маркира (на принципа на светофара – зелено, жълто, червено) нивото на безопасност на всеки сайт, който се появява при търсене, в социалните мрежи или при

други публикации. - За мобилните устройства (смартфон и таблет) може да инсталирате Dolphin браузър, който е сигурен и добре защитен, или да изтеглите WOT като отделно приложение. - При най-малките деца (до 9-10 години) препоръчваме използването на програми за родителски контрол, с уговорката че първо бива разговор с детето, в който да му разкажете за тях и с какво му помагат - изберете правилната за Вашето дете и Вас самите програма тук. - Ако ползвате Windows 7, 8 или 10 можете да създадете детски профил на детето си. Информацията как да направите това, както и повече информация за основните стъпки, които родителите трябва да предприемат когато пуснат детето си за пръв път в мрежата, можете да намерите в наръчника "Как да не загубим детето си във виртуалния свят".

VII. ОСНОВНИ ПРАВИЛА И НАСТРОЙКИ ВЪВ ФЕЙСБУК

1. Поверителност (Privacy) От този раздел можете да настройвате: Кой вижда публикациите ви? Кой може да се свърже с вас? Кой може да ви търси по имейл или телефон? Препоръчително е да направите настройките си така, че публикациите ви да са видими само за приятелите ви във Фейсбук.

2. Дневник и отбелязване (Timeline and Tagging) От този раздел можете да ограничите другите хора да постват на вашата стена и да включите одобрение от ваша страна, преди дадена публикация, на която сте отбелязани, да се показва в профила ви. Това става от "Кой може да добавя неща в дневника ми". Одобрението на снимки, на които сте отбелязани, можете да включите от "Как да управлявам отбелязването от други хора и предложенията за отбелязване".

3. Сигнализирай/Блокирай На всеки профил в долния десен ъгъл на корицата (cover) има бутон. Натискайки го, излиза падащо меню, чиито последни две опции са: Сигнализирай/Блокирай (Report/Block) и Премахни от приятели (Unfriend). Когато изберете тази опция, можете да изберете 1 от 4 действия спрямо конкретния профил:

- Unfollow – няма да виждате повече новини от профила, но ще продължавате да бъдете приятели и съответно профилът да вижда вашите публикации.
- Unfriend – профилът ще бъде извън списъка ви с приятели и съответно няма да бъде допуснат само до публичната информация за вас.
- Block – нито вие, нито профилът ще можете да се свързвате един друг или да виждате информация за себе си.
- Submit a Report – можете да сигнализирате съдържание, поставено от профила, или самия профил. Избирайки да сигнализирате профила, трябва да уточните за какво го сигнализирате. Възможностите са:

  - Профилът използва фалшиво име – Фейсбук стимулира своите потребители да използват истинските си имена.
  - Човекът е дразнещ – избирайки това оплакване, е необходимо да доуточните още, избирайки от 3 опции: - Изпраща спам покани за приятелство. - Изпраща спам съобщения. - Публикува дразнещи неща.
  - Човекът се преструва на мен или на някого, когото познавам – изберете дали профилът се представя за вас, ваш приятел или известна личност.
  - Профилът публикува неподходящо съдържание: - Неподходяща профилна снимка. - Сексуални. - Друго.
  - Този профил е фалшив – това означава, че профилът е създаден, за да тормози вас или друг човек.

- Профилът представя бизнес или организация – Фейсбук насърчава организациите и институциите да си създават страници, а не профили.

VIII. ВИДОВЕ ВИРУСИ ВЪВ ФЕЙСБУК

1. Facebook вирус с детско порно е опасно приложение, което циркулира във Facebook под формата на порнографски клипчета. Изглежда сякаш съобщението, което съдържа прикаченото видео, е изпратено от Ваш приятел и е безопасно. Въпреки това след отваряне става ясно, че е свързано с детска порнография. Някои жертви споделят, че съдържа фраза като „гледай това ако си любопитен". Веднъж отворен, вирусът автоматично се свързва с Facebook профила Ви и споделя това видео с всичките Ви Facebook приятели.

2. Facebook вирус за смяна на цвета е коварен вариант на Facebook вируса, който се основава на съобщение, предлагащо да промените фона на социалната мрежа на розов, червен, черен или друг цвят. Също като други типове на тази зараза, и това може да попадне във входящата Ви кутия от някой от контактите Ви, който също е бил подведен от това съобщение. Обикновено включва зловреден линк, който помага на измамниците да получат повече трафик към тяхно онлайн проучване. Ако кликнете на този линк, ще пратите това съобщение на всичките си контакти.

3. Facebook вирус с предложение за приятелство е опасна заплаха, която праща покани за приятелство от акаунта на потребителя до непознати хора, или дори по-лошо, такива, които вече са били блокирани от потребителя. Има данни че понякога вирусът успява да изпрати повече от 100 покани на случайни хора. Целта при създаването и използването на това все още не е разкрита. Въпреки това някои експерти твърдят, че този вирус може да се използва за превземане на компютри, изключване на антивирусни програми и подобни дейности.

4. Facebook вирус за автоматично публикуване на стената е кибер инфекция, създадена за повишаване на трафика към конкретни домейни. Освен това може негативно да се отрази на сигурността на компютъра и да се опита да открадне лична информация. Вирусът кара хората да посещават уебсайта като показват подвеждащо съобщение, което гласи „Най-сексапилното видео на всички времена" или др. и включва линк, водещ до неизвестен сайт. Освен това автоматично публикува на стената Ви и се разпространява по този начин. Ако видите подобно съобщение, което сякаш е публикувано от Ваш приятел, трябва да го премахнете от стената си незабавно.

5. Facebook вирус по съобщенията е друг вариант на Facebook вируса, който се разпространява чрез чат прозореца. Този вирус изскача със съобщение, което сякаш е от Ваш приятел и включва нормално изглеждащ линк. Разбира се, никога не трябва да кликвате на линка, защото той инфектира компютъра Ви с вирус, способен да изключи антивирусната и да свали друг малуер на системата Ви. Разбира се, ако кликнете на линка, този вирус ще продължи да се разпространява чрез Вашия Facebook акаунт.

6. Facebook вирус чрез покани е различен вид вирус, който се разпространява из Facebook от години. Разпространява се чрез имейли и таблото за съобщения на Facebook и съобщава за огромна опасност на социалната мрежа. За да сме по-конкретни, то предупреждава за Facebook заплаха, която идва като съобщение с приставка, наречена Покана и „отваря Олимпийски факел и превзема цялото С на компютъра Ви". Въпреки това нашите експерти по сигурността са установили, че това съобщение съдържа троянец и други видове вируси. Трябва да премахнете това измамническо съобщение веднага щом го получите.

7. Facebook преследващ вирус е опасно Facebook приложение, което се разпространява из социалната мрежа. Принадлежи на измамници и се използва за кражбата на личната информация на

потребители, а не за да показва на хората кой тайно гледа техния Facebook профил. Ако се хванете на Facebook приложението за преследване, ще бъдете пренасочени към зловреден сайт, който изглежда като типичната начална страница на Facebook. Моля, НЕ въвеждайте личната си информация там, защото ще я загубите, както и Facebook акаунта си!

8. Facebook „hahaha“ вирус е последната версия на Facebook вируса. Това е сериозен малуер, който се разпространява чрез социалната мрежа и се използва за превръщането на компютъра в машина за биткоин майнинг. Веднъж след като накара жертвите си да си свалят зловредния .Zip файл, настъпват сериозни забавяния на компютъра и подобни проблеми. Моля, не позволявайте на този зловреден софтуер да остане на компютъра Ви, защото не се знае за какви зловредни дейности ще се използва.

IX. ЗАЩИТА ОТ НЕЖЕЛАНА ЕЛЕКТРОННА ПОЩА

1. Не проявявайте инициатива за получаване на e-mail писма, интернет страници, които предлагат безплатни или небезплатни услуги и стоки, често предлагащи да ви изпратят промоции по email. Откажете такава услуга.

2. Раздавайте e-mail адреса си само при нужда. Когато давате по един или друг повод e-mail адреса си, се запитайте следните две неща: първо дали организацията или човекът, който го получава, ще ви изпрати нежелан e-mail; второ може ли да разчитате, че e-mail адресът ви няма да бъде даден на трето лице. Ако и на двете отговорът е „да“, просто не си давайте адреса или дайте някой второстепенен.

3. Не отговаряйте на нежелана поща. Никога не отваряйте прикачени файлове в съобщения от непознат изпращач. Ако не познавате името в полето „От“ не отваряйте прикачения файл.

4. Ако получите неочаквано съобщение със странен прикачен файл от познат изпращач, то би могло да съдържа вирус. Много червеи се разпространяват до всички контакти, които намерят в пощата на заразения компютър. Такива съобщения често имат странна тема или име на прикачения файл. Често това е шеговито съобщение, насърчаващо получателя да види картинка или да прочете прикачен текстови файл. Винаги изисквайте потвърждение от изпращача преди да отворите съобщение или прикачен файл от такъв вид.

5. Проверявайте пълното име на прикачения файл. Скритите разширения от името на файла могат да Ви заблудят да отворите заразен прикачен файл от имейла. Винаги проверявайте дали имейл приложението показва пълното име на прикачения файл, включително разширението. Вируси и червеи могат да се съдържат във файлове, които изглеждат като картинки, например с разширение .jpg. Но е възможно да имат скрито разширение, като .exe или .vbs към името на файла, което означава, че прикачения файл не е картинка, а програма, която ще се стартира щом се отвори прикачения файл.

6. Внимавайте с фалшивите предупреждения за вируси. Фалшивите предупреждения за вируси са известни като "hoaxes". Това е вид верижно писмо, което подвежда потребителите да вярват, че са получили вирус и ги насърчава да препратят предупреждението на всеки, когото познават.

7. Не отваряйте спам. Имейл, съдържащ нежелана реклама може да бъде използван за пренасяне на вируси и червеи. От съображения за сигурност, би трябвало да изтривате всички рекламни съобщения от непознат изпращач веднага без да ги отваряте.

8. Не използвайте само една пощенска кутия за всичко. Направете си няколко различни пощи и ги разделете по предназначение. Определете поне по една отделна пощенска кутия за:

- лична кореспонденция

- служебна кореспонденция (ако имате такава)
- регистрации в сайтове в интернет, и други публични места, които не са от особена важност.
- регистрация във форуми

9. Избягвайте да препращате писма между вашите пощенски кутии.

10. Избягвайте да препращате писма до няколко човека едновременно. Особено такива, от типа - "препратете го до 7 човека и ще ви се случи нещо хубаво" или "помогнете на болното ми дете, като препратите това писмо на много хора, еди кой си ще ми даде за всеки 3 имейла 5 цента (примерно). Тези писма се разпространяват с цел събиране на действителни имейл адреси, тъй като при препращане, към писмото се добавят автоматично и адресите на предните получатели. След няколко препращания, в едно такова писмо се събират няколко стотици реални имейл адреса, които след това се продават на фирми за спам.

11. Ако все пак искате да препратите някакъв текст или информация, която сте получили, копирайте текста и го изпратете като ново писмо. Не препращайте предното, въпреки че е примамливо по-лесно. Така ще предпазите приятелите си от бъдещ спам.

12. Ако поради някаква причина държите да препратите оригиналното писмо, сложете адреса в BCC (Blind Carbon Copy) вместо в CC. Така никой от получателите няма да види адресите на другите получатели. Причината да го използвате не е да скриете получателите един от друг, а да ги предпазите, в случай че адресната книга или електронната поща на някой от тях стане достъпна на спам-бот (например поради вирусна инфекция на компютъра му).

13. Печалба от лотария: не сте спечелили. Спамърите използват най-различни примамливи заглавия на писмата, за да накарат получателя да ги отвори. Много потребители наистина отварят подобни писма. Дори след отварянето веднага да го изтриете, самото отваряне на писмото би могло да потвърди, че адреса съществува и вие сте го получили. Затова просто свикнете с мисълта че:

- Не сте спечелили лотарията на Yahoo, Националната лотария и никоя друга лотария, в която не сте участвали
- Няма крал или принц на Нубия, който да иска да ви изпрати 10 милиона долара, нито някой адвокат от Тамбукту иска да му помогнете да получи 5 милиона от застраховката на катастрофиралите роднини на еди кой си.
- Не е необходимо незабавно да потвърдите данните за банковата ви сметка. Всъщност изобщо не е необходимо да ги потвърждавате с електронна поща, по какъвто и да е повод.
- Нямате наследство, за което неочаквано непознат ви праща съобщение по пощата. Ако имахте, нямаше да се свържат с вас по този начин.
- Никога всъщност не сте пращали това "Върнато писмо"
- Не сте спечелили iPod Nano. Вашият IP не е спечелил 5000 британски лири.

14. Отписване от бюлетин, за който не помните да сте се записвали. Често срещан напоследък метод, използван от спамърите за намиране на активните пощенски адреси. Изпраща се бюлетин с линк за отписване (уж) от получаването му. Отписвайки се, всъщност потребителят потвърждава, че използва пощенската кутия, с което веднага се записва в спам листите. Вместо да се отписвате, блокирайте получаването на писма от този адрес.

15. Не отваряйте писма, които са фишинг атаки. Най-добрият начин да се защитите от фишинг атаки е като никога не отваряте фишинг писма, но често е трудно да се разпознае кое писмо е фишинг атака. Можете да ги разпознаете по:

- Обръщението е "Dear Customer" или "Dear User", а не вашето име.
- В писмото пише, че акаунтът ви ще бъде прекратен в случай че не потвърдите данните си незабавно. /Наскоро спамърите използваха подобен похват когато скайп се срина за 1 ден. Разпространиха съобщения , че скайп ще чисти неактивни акаунти и се искаше да се разпрати съобщение на поне 15 потребителя, за да се докаже активност /
- Имейлът идва от акаунт, приличащ, но не еднакъв с този, който използва известна фирма, организация и др. Ако не сте сигурни дали писмото е фишинг или не, най-добре е да не отваряте линковете, които са публикувани в него, а да напишете на ръка адреса на сайта, който ви е необходим.
- Ако сте получили такова писмо, за предпочитане е да блокирате адреса, от който е изпратено. Когато го блокирате, вие давате указания на пощенския клиент, че това е спам и не трябва да се приема. Повечето потребители обаче просто изтриват спама и той продължава да идва в кутията.

Вашият смартфон също трябва да има антивирусна програма, която предлага опция за търсене и заключване през интернет, с цел опазване на личната информация в него – снимки, профили, пароли и др, както и намирането му, ако е откраднат или загубен.

1. CM Security AppLock AntiVirus Лекият софтуер не утежнява работата на мобилното устройство, докато работи, но, за сметка на това, го пази от вируси, троянски коне, зловреден или шпионски софтуер и най-различни уязвимости в сигурността. CM Security AppLock AntiVirus предлага най-различни режими на сканиране на системата: сканиране на операционната система и приложенията, сканиране на SD картата, сканиране по време на инсталация и така нататък. Хубаво е също, че менюто й е налично и на български език.

2. AntiVirus Security – FREE Софтуерът на AVG предлага защита от вируси, зловреден и шпионски софтуер и дори зловредни SMS-и, като гарантира пълна сигурност на личните ни данни. Освен че сканира всичките ни приложения, медийни файлове и дори настройки в реално време, AntiVirus Security – FREE ни позволява дори да намерим загубения си или откраднат телефон с помощта на Google Maps, както и да изтрием дистанционно личните си данни, в случай че не сме успели да го открием.

3. Norton Security and Antivirus Norton е известно име в сферата на антивирусния софтуер и компанията не е пропуснала да разработи безплатен продукт съвместим и с Android. Софтуерът търси и премахва приложения съдържащи зловреден софтуер или вируси, и подобно на AntiVirus Security – FREE, позволява дистанционно заключване на загубен или откраднат телефон. Освен за зловредни приложения, софтуерът на Norton ни предупреждава и за сайтове, които се опитват да откраднат личните ни данни или парите ни.

4. Kaspersky Internet Security Приложението предпазва телефона или таблета ни от всякакъв вид заплахи, включително вируси, шпионски софтуер, троянски коне и други. Поддържа опция за намиране или изтриване на данните при загубен/откраднат телефон или таблет и разполага с функция наречена „Аларма“ за откриване на мобилното устройство в случай че е близо до нас, но все пак не можем да го намерим.

5. Mobile Security & Antivirus Mobile Security & Antivirus е мобилният еквивалент на популярната антивирусна услуга на компанията Avast. Приложението предпазва телефона или таблета ни от

фишинг атаки, зловреден и шпионски софтуер, Троянски коне и други и, също като повечето предложения по-горе, ни помага да намерим или поне да изтрием данните в изгубеното си мобилно устройство. Налице е също опция за изпращане на SMS, който ни уведомява, че SIM картата в изгубеното ни устройство е била сменена.

Обърнете внимание на разширенията на криптираните файлове, които ви се предлагат във Фейсбук, на електронната поща и др., и не отваряйте такива с разширения .CRYPT, .vvv, .zzz, .aaa, .abc, .ccc, .ecc, .ezz, .exx, .xyz , .micro, .ttt, .xxx, .mp3 и др.

1. Ако сте получили Facebook съобщение, че ваш приятел ви е споменал персонално в коментар и след натискане браузърът ви сваля файл с разширение *.jse не го приемайте. За всеки случай проверете компютъра си за зловреден код с този онлайн скенер: www.eset.com/bg/home/products/online-scanner/

2. След като проверката за вируси приключи рестартирайте и направете нова проверка с този скенер: www.bitdefender.com/scanner/online/free.html

3. Ако все пак сте свалили и стартирали файла, направете проверката за зловреден код (по-горе), като докато тя тече спрете интернета на компютъра си. След това променете паролите на интернет банкирането си (най-добре от различен компютър), фейсбук акаунта, мейла и всички други важни и критични услуги, които ползвате. Обновете операционната си система с инсталиране на последните ъпдейти от Control panel - Windows update. Нека новите ви пароли са над 10 знака с различни символи.

4. Ако достъпвате Facebook през смартфон и след като сте получили известие за споменаване от ваш приятел сте натиснали и приели най-вероятно са започнали в браузъра да се показват агресивни съобщения, че телефонът ви е заразен с вирус, с приканване да натиснете бутон, за да се изтрие. Не натискайте нищо! Веднага рестартирайте смартфона. След това инсталирайте антивирус от онлайн магазина и го пуснете да сканира устройството. След това отново рестартирайте. И в този случай промяната на всички пароли е силно препоръчителна.

5. Ако все пак сте отворили странен видеофайл или съобщение във фейсбук, което заразява профила ви и публикува вместо вас, незабавно сменете паролата си и рестартирайте смартфона, компютъра, таблета или лаптопа. След това продължете със антивирусно сканиране и подмяна на пароли за достъп, запаметени в браузъра и профила.