



Класификация на информацията
Ниво 1 [TLP-GREEN]

**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ, АДМИНИСТРАЦИЯ
И УСЛУГИ „АТАНАС БУРОВ“ – ГР.СИЛИСТРА**
7500 гр.Силистра, бул.“Македония“ 121; тел:+359 86 821 859; info-1900506@edu.mon.bg

ЗАПОВЕД

№ РД 14-...*77*...../.....*27*...09.2024г.

На основание чл. 259, ал. 1 от Закона за предучилищното и училищното образование, във връзка НАРЕДБА № 15 от 22 юли 2019 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти и решение на педагогическия съвет от 25.09.2024 г.

УТВЪРЖДАВАМ:

**Правила за безопасност на ученици в компютърната мрежа и интернет
в ПГСУАУ „Атанас Буров“ през учебната 2024/2025г.**

ДИРЕКТОР:..

/Д. Михайлова/



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

ПРАВИЛА

за безопасност на учениците в

компютърната мрежа в училището и в интернет

Компютърната мрежа в училище се използва в педагогическите ситуации и учебни часове само за образователни цели. Цялата мрежа обхваща компютрите, свързани с кабелни и/или безжични връзки, ситуирани в компютърните кабинети, оборудвани класни стаи и административните помещения на образователната институция, както и устройствата (персонални смартфони, лаптопи и планшети) с безжичен достъп до интернет.

Правилата са разработени от Държавната агенция за закрила на детето, в партньорство с Главна дирекция „Борба с организираната престъпност”, Национален център за безопасен интернет, Министерство на образованието и науката, Регионално управление на образованието – София-град, ръководители на образователни институции от Съюза на работодателите в системата на народната просвета в България, Сдружението на директорите в средното образование на Р България.

Целите на правилата са да се:

- *гарантира правото на учениците на достъп до подходяща информация и материали в мрежата;*
- *осъществи презентация и синтезира на едно място информацията за опасностите в интернет;*
- *предоставят конкретни насоки за закрила на детето и безопасно поведение в компютърната мрежа в училище и в интернет;*
- *подобри координацията и отговорностите на участниците и/или всички заинтересовани страни.*

ОСНОВНИТЕ ПРИНЦИПИ ЗА РАБОТА В КОМПЮТЪРНАТА МРЕЖА В УЧИЛИЩЕ И В ИНТЕРНЕТ :

1. Равен достъп на всички ученици;
2. Защита на учениците от вредно или незаконно съдържание и информация като: самонараняване, търговия с наркотици, хазарт, пропагандиране на вредни и опасни навици и действия като анорексия, булимия, порнография, толериране на различни форми на насилие, проповядване на тероризъм, етническа и религиозна нетолерантност, самоубийство и др.;
3. Зачитане и защита на личната неприкосновеност;



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

4. Подготовка и контрол на учениците за безопасно и отговорно поведение онлайн;
5. Сътрудничество в дух на толерантност и добронамереност между училището и родителите/настойниците.

УЧЕНИЦИТЕ ИМАТ ПРАВО НА:

1. Равен достъп до мрежата на образователната институция, с изключение на компютрите в административните помещения.
2. Работа с устройствата (компютри, лаптопи и таблети) в мрежата с подкрепата на педагогически специалист.
3. Обучение за безопасно и отговорно поведение в мрежата на образователната институция и в интернет.
4. Информация за правилата за работа в мрежата.
5. Сигурна цифрова среда в училището.
6. Ползване на мобилните си устройства извън учебния процес (почивката и междучасията), а при изрично указание на учител – и в учебния час/педагогическата ситуация за целите на учебния процес.

ЧАСТ I.

Отговорности на ръководителите на образователните институции, на професионалистите, работещи с ученици и с информационно-комуникационни технологии (ИКТ)

Директорът на училището:

1. Организира дейността по изпълнението на тези правила и осигурява достъп до компютърната мрежа, ефективен и постоянен контрол, планирането на мерки по организацията за спазване на правилата за работата на децата и учениците в мрежата и защита от вредно или незаконно съдържание в интернет.
2. Осигурява при техническа възможност проследяване на трафика, осъществяван чрез мрежата на образователната институция.
3. При констатиране на случаи на кибертормоз, незаконно съдържание и поведение в мрежата на образователната институция и/или в интернет уведомява незабавно компетентните органи – Дирекция „Социално подпомагане“, по местопребиваване на детето и Главна дирекция „Борба с организираната престъпност“, специализираният отдел „Киберпрестъпност“ на МВР. В тези случаи оказва нужното съдействие на компетентните органи с цел установяване на извършителите и предприема мерки за противодействие и премахване на съответното съдържание от мрежата на образователната институция. Може да получава и консултантска помощ от Националния център за безопасен интернет.
4. Организира в началото на всяка учебна година запознаване на учениците и родителите/настойниците с правилата за безопасна работа в мрежата.



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

5. Осигурява отговорно лице (служител или нает външен специалист), което да изпълнява функциите на системен администратор.

Учителите, педагогическите специалисти и ръководителите по направление ИКТ:

1. Разясняват правилата за безопасно и отговорно поведение при работа в мрежата на образователната институция и в интернет.
2. Осъществяват постоянно наблюдение и контрол върху работата на учениците в мрежата на образователната институция в учебно време.
3. Предприемат незабавни мерки за преустановяване на достъпа на учениците до незаконно и вредно съдържание в мрежата.
4. Уведомяват незабавно директора на училището при нарушаване на правилата, случаи на кибертормоз или при установяване на незаконно и вредно съдържание или поведение в мрежата.
5. Оказват подкрепа на учениците – обект на кибертормоз, чрез първоначална психологическа подкрепа от училищния психолог.
6. Сигнализират при необходимост Дирекция „Социално подпомагане“ по местоживее на ученика с цел оценяване на нуждата от насочване към социални услуги за оказване на последваща подкрепа.

Системният администратор (служител в образователната институция или нает външен специалист):

1. Осигурява общата безопасност и функционалност на мрежата.
2. Предлага и прилага мерки, ограничаващи достъпа на учениците до вредно или незаконно съдържание и поведение в интернет в съответствие с действащото законодателство на Република България.
3. Извършва периодичен преглед на компютърната мрежа на образователната институция за наличие на възможни заплахи и рискове за сигурността на децата и учениците при работа в интернет.
4. Следи графика, осъществяван чрез компютърната мрежа на образователната институция.
5. Предприема незабавни мерки за преустановяване на достъпа на учениците до незаконно и вредно съдържание в мрежата.
6. Уведомява незабавно директора на детската училището при случаи на незаконно съдържание или поведение в мрежата.
7. Съдейства за установяване на извършители на кибертормоз и прилага мерки за ограничаване на такива случаи.

ЧАСТ II.

Права и отговорности на родителите

Родителите имат право да:

1. Получават информация за рисковете и заплахите за безопасността на техните деца при работа в интернет в училището и вкъщи.



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

2. Бъдат своевременно информирани, ако детето им е обект на кибертормоз в училището.
3. Участват съвместно с ръководството на образователната институция при разрешаване на всеки конкретен проблем, свързан с нарушаване на правилата от страна на техните деца.
4. Участват със свои предложения в определянето на правилата и мерките за безопасно използване на интернет в училището.
5. Получат информация за информационно-сигнализационни платформи като www.gdbop.bg; www.cybercrime.bg; www.spasidete.com; www.safenet.bg; www.facebook.com/bgcybercrime.

Родителите носят отговорност да:

1. Помогнат на детето си да изгради умения за онлайн общуване и безопасно използване на интернет.
2. Осъществяват постоянен контрол за сигурността на детето си в интернет.
3. Проявяват интерес към активността на детето си в мрежата, включително създаването на профили в социални мрежи и регистрации в сайтове и мобилни приложения, както и да разяснят последствията от създаването и/или разпространението на определено съдържание.
4. При установяване, че детето им е жертва на кибертормоз, да сигнализират на отдел „Киберпрестъпност“ към Главна дирекция „Борба с организираната престъпност“ (<http://www.cybercrime.bg/bg>), или Центъра за безопасен интернет (<https://www.safenet.bg/>), както и могат да потърсят съдействие от Дирекция „Социално подпомагане“ по местоживее на детето с цел оказване на психологическа подкрепа на детето. В този случай трябва да уведомят директора на образователната институция.
5. Съхраняват здравето на детето, като проследяват времето за използване на интернет.
6. Уведомят директора на образователната институция, когато им стане известно, че детето им е обект на тормоз от друго дете, с което е в едно и също училище.

ЧАСТ III

Общи правила за безопасно общуване в интернет за учениците:

1. Не дават лична информация: име, адрес, парола от електронна поща, профил в социална мрежа, личен телефонен номер, училището, в което учат.
2. Не дават информация за местоработата или личен и служебен телефонен номер на родителите, настойниците, близките, приятелите, съучениците и познатите си без тяхно разрешение.
3. Не изпращат и не качват онлайн снимки и видеа на приятели, съученици, роднини, учители, близки, познати, без преди това да е обсъдено с тях.
4. Не отговарят и не отварят прикачени файлове на електронна поща, получена от непознат подател.



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

5. Нещата, които правят в интернет, не трябва да вредят на други хора или да противоречат на установените правила (част от тях са уредени в закони).
6. Забранено е да се използва чуждо потребителско име, парола и електронна поща.
7. Не пишат и да не качват нищо, което може да е обидно или унизително.
8. Незабавно информират възрастен (родител, учител, директор, педагогически съветник), когато попаднат на материали, с вредно или незаконно съдържание, което може да бъде порнография, проповядване на насилие и тероризъм, етническа и религиозна нетолерантност, търговия с наркотици, хазарт и др. Могат да подадат сигнал на денонощната и безплатна Националната телефонна линия за деца 116 111, на отдел „Киберпрестъпност“ на ГДБОП (<http://www.cybercrime.bg/bg>), на Центъра за безопасен интернет на адрес: www.safenet.bg, или на техния телефон 124 123, или през чат-модула на www.safenet.bg.
9. Не отговарят на съобщения, които са обидни, заплашителни, неприлични или ги карат да се чувстват неудобно. Информират родителите си, класния ръководител, учител, директор, педагогически съветник.
10. Ако някой ги обижда или тормози онлайн, не отговарят, а докладват на отговорен възрастен (родител, учител, директор, педагогически съветник) или подават сигнал на посочените адреси: www.gdbop.bg; www.cybercrime.bg; www.spasidete.com; www.facebook.com/bgcybercrime; www.safenet.bg.
Правят екранна снимка (скрийншот) на съответния разговор или съдържание като електронно доказателство, което предават на отговорен възрастен (родител, учител, директор, педагогически съветник).
11. Внимават, когато разговарят в чат.
12. Не приемат срещи с лица, с които съм се запознал/а в интернет, освен след съгласието на родителите им. Хората, с които се запознават онлайн, не винаги са тези, за които се представят. Опитват се винаги да проверявам дали човекът отсреща наистина е този, за когото се представя чрез проверка по име, имейл, снимка и контролен въпрос. При съмнение могат да подат сигнал или да потърсят съвет през сайта на Центъра за безопасен интернет www.safenet.bg.
13. Използват настройките за безопасност и защитата на личните данни на социалните мрежи, мобилните приложения и браузърите.
14. Използват функцията за безопасно сърфиране. Не посещават сайтове в интернет, които са със съдържание, неподходящо за детска аудитория.
15. Използват трудни (дълги, с главни и малки букви, цифри и специални знаци) и различни за всеки сайт пароли.
16. Използват антивирусна програма, която следва редовно да се обновява.
17. Заедно с отговорните възрастни (родител, учител, директор), поддържат последните актуализирани версии на всички програми и приложения.
18. Когато ползват общи компютри, винаги проверяват дали съм излязъл/излязла от профила си, след като свърши часа. В случай, че намерят устройство, на



Класификация на информацията

Ниво 0 [TLP-WRITE]

**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

косто друг ученик е работил, но не е затворил профила си, веднага ще излизат без да преглеждат, променят или добавят информация в профила му.

19. Трябва да имат предвид, че когато публикуват невярна и изопачена информация за друг човек, дори с ясната мисъл, че това е шега, това може да доведе до злоупотреба и до неприятни преживявания за този човек.

Приложение№1 СЪВЕТИ ЗА ЗДРАВЕТО

Приложение№2 СХЕМА ЗА УВЕДОМЯВАНЕ В СЛУЧАЙ НА КИБЕРТОРМОЗ

Приложение№3 КРАТЪК РЕЧНИК

Приложение№4 ЗАЩИТА НА КОМПЮТЪРНИТЕ МРЕЖИ ОТ ОПАСНА ЕЛЕКТРОННА ПОЩА



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

Приложение №1

СЪВЕТИ ЗА ЗДРАВЕТО

За да не увредите зрението си:

- ✓ разстоянието между очите и монитора трябва да бъде около половин метър;
- ✓ разстоянието между очите и клавиатурата да бъде около половин метър;
- ✓ върху монитора не трябва да попада пряка слънчева светлина;
- ✓ не работи в стая, където има смесена светлина – слънчева и изкуствена;
- ✓ вредно за очите е, ако зад монитора да има прозорец без щори и завеси;
- ✓ за да отпочиват очите, от време на време отмествайте погледа от монитора и поглеждай през прозореца или към най-далечния край на стаята върху далечен обект;
- ✓ един път в годината проверявай зрението си при очен лекар (офталмолог).

При работа с клавиатурата:

- ✓ не прегъвай китката, когато пишеш;
- ✓ сгъвай леко пръстите на ръката и отпускай палеца;
- ✓ добре е да използваш клавиатура с клавиши, които са под лек наклон.

При работа с мишката:

- ✓ мишката трябва да бъде с размера на дланта;
- ✓ не движки мишката само с палеца и малкия пръст;
- ✓ ползвай подходяща подложка за мишката.

Мебелите

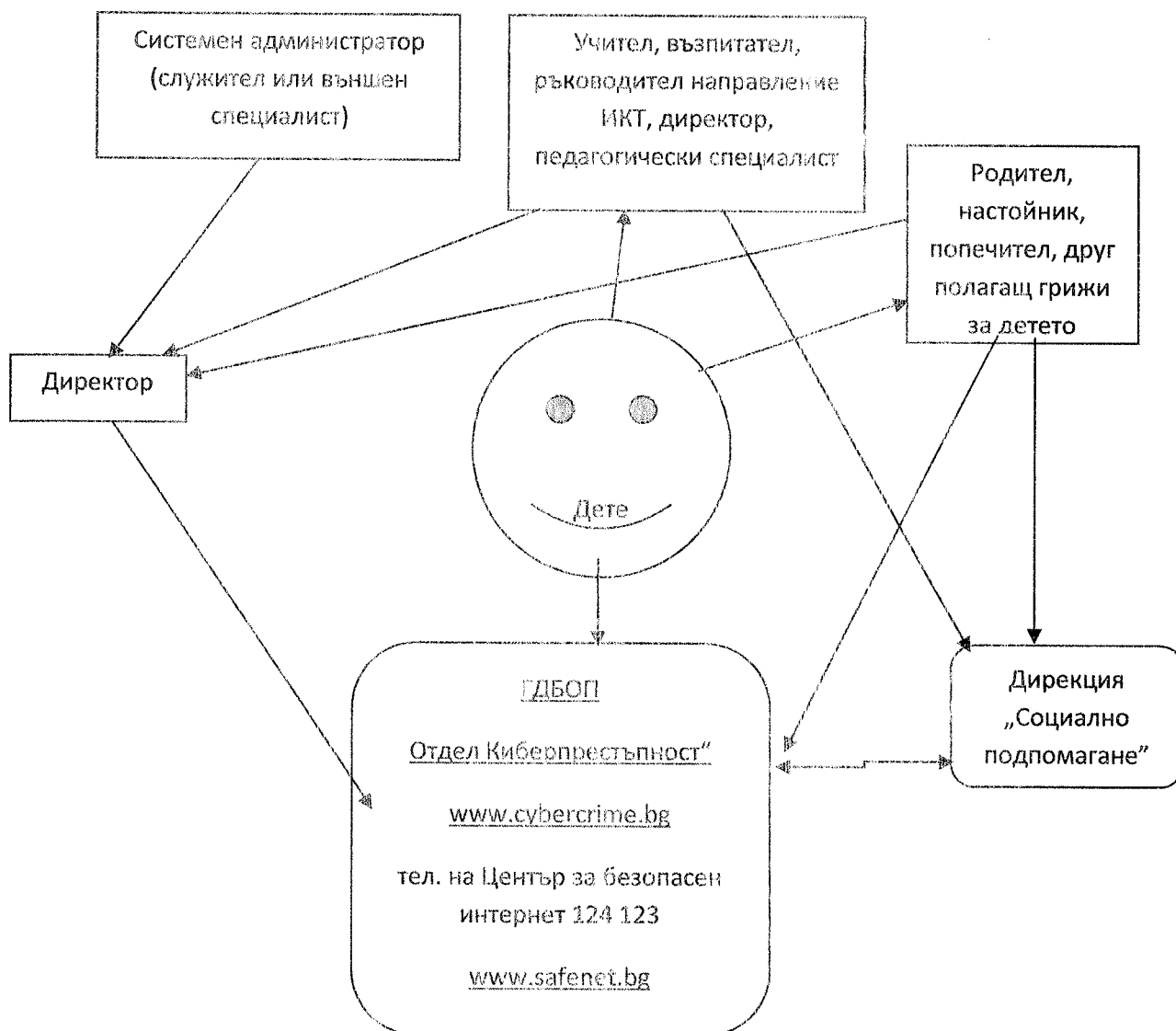
- ✓ столът трябва да бъде на колелца, с регулируема височина на седалката и облегалката, която трябва да осигури опора на гръбначния стълб в областта на кръста;



- ✓ бюрото трябва да бъде стабилно и устойчиво на вибрации.

Приложение №2

СХЕМА ЗА УВЕДОМЯВАНЕ В СЛУЧАЙ НА КИБЕРТОРМОЗ





**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

Приложение №3

КРАТЪК РЕЧНИК

КАЧВАНЕ И СПОДЕЛЯНЕ НА СНИМКИ – Снимки или видео на дете, ученик, родител, учител, директор, психолог, ресурсен учител, близки, приятели, познати или непознати лица са публично достъпни изображения в интернет, които могат да са качени от родителите или други членове на семейството, приятели, съученици и др. Тези, които са ги споделили/качили в интернет, може да имат изцяло добри намерения към него/нея. Когато се касае за снимки, за които не сте автор, същите не могат да бъдат ползвани и популяризирани без съгласието на техния автор. Но такова съдържание може да накърнява личността и достойнството на лицето. Препоръчително е по никакъв повод да не се качват снимки на дете, за които има и най-малкото съмнение, че могат да му навредят и без негово съгласие. 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. Важно е, когато се снима със смартфон, да се уверите, че снимките не се качват автоматично в профила на родителя или детето в сайтове като Инстаграм например. В профилите си в социалните мрежи трябва да сте сигурни, че сте настроили достъпа до 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.

ФАЛШИВИ НОВИНИ – Създателите на фалшиви новини използват традиционни медийни похвати за привличане вниманието на читателя, например провокиращи заглавия, но успяват да го заблудят и да го накарат да повярва, че информацията, която чете, е истинска.

Как да разпознаем фалшивите новини:

- Правете разлика между хумористични и сериозни новинарски сайтове. Запитайте се

–
познавате ли медията и имате ли ѝ доверие? Проверете дали заглавието, което често е гръмко и помпозно отговаря на съдържанието на новината;



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СМЛИСТРА**

7500 гр. Смилистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

- Проверете дали журналистът е посочил конкретно източника на информация или информацията се базира на друга статия. Проверете дали основният източник на информация е достоверен. Винаги поглеждайте началото или края на статията, където обикновено е посочен източникът на информация. Ако се касае за информация, която произлиза от държавна институция, проверете официалната ѝ страница дали фигурира тази новина или потърсете експерт по темата от дадената институция. Ако не е посочен източник, е редно да се съмнявате в достоверността на новината. В повечето достоверни материали се посочва начина на събиране на информацията и автора на публикацията. Препоръчително е да се сравни информацията, ако е публикувана в различни източници;
- Ако попаднете на статия, публикувана в непознат за вас блог, а информацията не е тиражирана никъде другаде, това е знак, че новината може би е фалшива. Винаги търсете и други резултати по темата, а ако те са малко или никакви, по-добре не разпространявайте новината;
- Проверете датата на публикацията, тъй като често стари и неактуални новини се пускат като нови.

ОНЛАЙН (КИБЕР)ТОРМОЗЪТ представлява използването на интернет за нанасяне на емоционална вреда върху други хора. ТорМОЗЪТ в интернет може да има различни форми. Той може да минава през разпространяване на подигравателни и обидни снимки и видеоклипове в сайтове за споделяне на видеосъдържание като Vbox7 и YouTube, създаване на фалшиви профили с обидно съдържание в социални мрежи като Ask.fm, Фейсбук и Инстаграм, както и в съобщения и изображения в приложения за комуникация като Скайп и Вайбър, или в изпращането на обидни съобщения и коментари, в същите сайтове и платформи.

КРАЖБАТА НА ПРОФИЛ (хакнат 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 профилът. 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 ЛИЧНИ ДАННИ е вид компютърно престъпление, при което се придобиват чужди лични данни с цел финансова измама или злоупотреба като теглене от банкова сметка, или кандидатстване за кредит от чуждо име. Тази опасност по принцип не засяга по-малките деца, които не притежават лични документи, банкови сметки или карти. Но при тийнейджърите над 14-годишна възраст този риск става актуален.



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

ФИШИНГ АТАКИТЕ са най-разпространената форма на Интернет измама и широко използван похват от компютърни престъпници за получаване на важна информация. Това престъпление се нарича „фишинг“ („phishing” – “зарибяване”, произлиза от fishing – риболов), защото електронните съобщения, които се разпращат, са като „въдици” с основна цел получателите да се „хванат” на тях поради своята неопитност и неосведоменост, като им отговорят. При фишинга измамниците 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 изпратят лични данни и данни за банкова сметка в отговор или да се въведат на уебсайт, към който има връзка. Тези данни са например потребителски имена, пароли и номера на кредитни карти.

КАК СЕ ПАЗАРУВА БЕЗОПАСНО В ИНТЕРНЕТ? Преди да пазарувате от електронен магазин, е полезно да обърнете внимание налична ли е информация за името, адреса и телефона на търговеца. Не пропускайте да проверите и дали доставчикът е посочил изрично правото Ви по закон да се откажете от поръчката в рамките на 14 дни. Полезно би било да прочетете във форумите отзиви от други потребители, които вече са пазарували от въпросния електронен магазин, към който сте се насочили. Търговецът е длъжен да Ви информира за основните характеристики на всяка от предлаганите от него стоки и услуги. Той трябва да посочи тяхната цена с включени всички данъци и такси, както и стойността на пощенските или транспортните разходи, ако не се включени в крайната цена. На сайта следва да бъде посочен начинът на плащане, доставка и изпълнение на договора. Ваше право е да върнете, закупената от електронен магазин стока, ако се окаже дефектна. Рекламацията си за дефектна стока следва да предявите в някои от обектите на търговеца, от който сте я закупили. Ако търговецът уважи рекламацията Ви, в рамките на месец трябва или да ремонтира безплатно за Вас стоката или да я замени с нова. В случай че не успее да стори едно от двете, следва или да намали цената, или да върнете стоката, а той да Ви възстанови заплатената за нея сума.



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

Приложение №4

**ЗАЩИТА НА КОМПЮТЪРНИТЕ МРЕЖИ ОТ ОПАСНА ЕЛЕКТРОННА
ПОЩА**

1. Не трябва да се проявява инициатива за получаване на имейл писма, интернет страници, които предлагат безплатни или платени услуги и стоки, често предлагачи да ви изпратят промоции по e-mail. Откажете такава услуга.

2. Имейл адресът се споделя само при нужда. Когато се предава по един или друг повод, се внимава за следните две неща: първо дали организацията или човекът, които го получават, ще ви изпрати нежелан имейл; второ, може ли да се разчита, че имейл адресът няма да бъде даден на трето лице.

3. Не се отварят имейлите в нежелана поща. Никога не се отваряйте прикачени файлове в съобщения от непознат изпращач. Ако не се познава името в полето „От“, не отваряйте прикачения файл.

4. Ако се получи неочаквано съобщение със странен прикачен файл от познат изпращач, то би могло да съдържа вирус. Много зловредни програми 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. Проверява се пълното име на прикачения файл. Скрытите разширения от името на файла могат да заблудят да отворите заразен прикачен файл от имейла. Винаги се проверява дали имейл приложението показва пълното име на прикачения файл, включително разширението. Вируси и червен 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 прикаченият файл не е картинка, а програма, която ще се стартира, щом се отвори прикачения файл.

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



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

7. Не отваряйте имейл, съдържащ нежелана реклама. Той 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 се използва само една пощенска кутия за всичко. Специалистите по киберсигурност препоръчват да се откриват няколко различни пощи и да се разделят по предназначение.

9. Избягвайте също така да препращате писма между няколко ваши пощенски кутии.

10. Не е препоръчително да се препращат 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, например. 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 ВСС (Blind Carbon Copy) вместо в СС. 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 адресът е реален и вие сте го получили.

14. Отписване от бюлетин, за който не помните да сте се записвали. Често срещан 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 влиза 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



**ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО СТОПАНСКО УПРАВЛЕНИЕ,
АДМИНИСТРАЦИЯ И УСЛУГИ "АТАНАС БУРОВ" - СИЛИСТРА**

7500 гр. Силистра, ул. "Македония" 121; тел.+359 86 821 859; e-mail: info-1900506@edu.mon.bg

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 потребители, 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 линкове, 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 пощенският клиент, че това е спам и не трябва да се приема. Повечето потребители обаче просто изтриват спама и той продължава да идва в кутията.