



ОСНОВНО УЧИЛИЩЕ „РАН БОСИЛЕК“

5300 Габрово, ул. “Орлово гнездо” 12, www.ranbosilek.com

тел.: 066 / 807 516 e-mail: info-700102@edu.mon.bg

ПРАВИЛА

ЗА БЕЗОПАСНОСТ НА ДЕЦАТА И УЧЕНИЦИТЕ В

КОМПЮТЪРНАТА МРЕЖА В УЧИЛИЩЕТО И В ИНТЕРНЕТ

1) Цели

- Да се гарантира правото на детето и учениците на достъп до **подходяща и безопасна информация** в мрежата.
- Да се осъществи **превенция**, като се събере на едно място важна информация за рисковете в интернет.
- Да се предоставят **конкретни насоки** за закрила на детето и безопасно поведение в училищната мрежа и в интернет.
- Да се подобри **координацията и отговорностите** на участниците и всички заинтересовани страни.

2) Обхват

Правилата се отнасят за всички ученици, учители, непедагогически персонал, външни партньори, родители и посетители, които ползват училищни устройства, лични устройства в училищната мрежа или интернет услуги, свързани с училището.

3) Основни принципи

- **Безопасност на първо място** – превенция, навременно сигнализиране и подкрепа.
- **Дигитална етика** – уважение, коректност и спазване на авторски права.
- **Защита на личните данни** – минимизиране на данни, информирано съгласие, поверителност.
- **Прозрачност и отговорност** – ясни правила, роли, контрол и отчетност.

4) Роли и отговорности

Директор: утвърждава правилата, осигурява ресурси, определя отговорни лица, контролира изпълнението.

Заместник-директор/координатор по безопасност онлайн: организира превенцията, обученията и реакцията при инциденти.

Учители: преподават дигитална култура и безопасност; наблюдават и насочват учениците; подават сигнали при инциденти.

Класни ръководители: запознават учениците и родителите с правилата; събират декларации за информираност.

Педагогически съветник/психолог: подкрепя ученици при онлайн рискове (насилие, тормоз, изнудване), участва в планове за подкрепа.

Администратор на мрежата/техник: поддържа филтри за съдържание, антивирусна защита, контрол на достъпа и логове според закона.

Ученици: спазват правилата, пазят личните си данни, сигнализируют за рискове.

Родители: запознават се с правилата, подкрепят децата, наблюдават домашното ползване на интернет.

5) Правила за безопасно поведение на учениците

- Не споделяй лични данни (трите имена, адрес, телефон, пароли, снимки на документи).
- Общувай **уважително**; не участвай в обиди, омраза, подигравки, разпространяване на слухове.
- Не отваряй съмнителни линкове, прикачени файлове или покани от непознати.
- Не изпращай и не публикувай снимки или видео на други лица **без тяхно съгласие**.
- При съмнителен контакт, заплаха, тормоз или искане за среща – **незабавно уведомявай** учител, родител или училищния психолог.
- Използвай училищната поща и платформи само за учебни цели.
- Спазвай авторските права – посочвай източници, не плагиатствай.
- При съмнение за фалшива новина – проверявай източниците, консултирай се с учител.

6) Техническа и организационна защита

- **Филтриране на съдържание** и блокиране на сайтове с насилие, порнография, хазарт, реч на омраза, измами.
- **Антивирусна защита** и автоматични актуализации на всички училищни устройства.
- **Потребителски профили и пароли** – минимален достъп според ролята, силни пароли и периодична смяна.
- **Логове и мониторинг** – технически записи за сигурност, при спазване на изискванията за защита на лични данни.
- **Резервни копия** на важни данни и план за възстановяване при инцидент.
- **Политика за лични устройства (донесени от дома):** достъп само до гост-мрежа с филтър; забрана за споделяне на интернет през мобилна точка в клас; забрана за нерегламентирано заснемане.

7) Рискове в интернет – разпознаване и превенция

- **Онлайн тормоз и насилие:** обиди, заплахи, изнудване, изолация, нежелано споделяне на лични данни или изображения.
- **Груминг и измами:** представяне за друго лице, искане на снимки, пари или срещи.
- **Зависимости и прекомерна употреба:** баланс между учене, почивка и дигитално време.
- **Неподходящо съдържание:** насилие, порнография, реч на омраза, екстремизъм.
- **Фишинг и зловреден софтуер:** идентифициране на подозрителни имейли, сайтове и файлове.

8) Процедура при инцидент

1. **Сигнализиране:** ученик, учител или родител уведомява незабавно класния ръководител, координатора по безопасност или директора.
2. **Първични действия:** осигуряване на безопасност на детето; **неизтриване** на доказателства (екрани, връзки); ограничаване на достъпа до вредното съдържание.

3. **Документиране:** кратко описание, дата, участници, доказателства; регистрация в училищния дневник за инциденти.
4. **Уведомяване на родители** и при нужда – на компетентни институции (отдел „Закрила на детето“, полиция, регионално управление на образованието).
5. **Подкрепа:** включване на педагогическия съветник/психолог; индивидуален план за подкрепа.
6. **Корективни мерки:** педагогически мерки според правилника; образователни и възстановителни дейности.
7. **Анализ и превенция:** преглед на случая и мерки за недопускане на повторение.

9) Учебна употреба и класна стая

- Устройствата се използват **само** за учебни дейности, определени от учителя.
- Забранено е използването на чатове, игри и социални мрежи по време на час, освен ако са част от урока.
- Заснемане в клас се допуска единствено по учебна необходимост и **след съгласие** на заснетите лица.
- Учителят определя времеви рамки за работа онлайн и наблюдава екраните при възможност.

10) Социални мрежи и публичност

- Училищните профили и страници се администрират от упълномощени лица.
- Публикации със снимки/видео на ученици се правят **само** при налично писмено съгласие на родителите/настойниците.
- Не се публикуват списъци с класове, лични данни, оценки или чувствителна информация.

11) Защита на личните данни

- Събира се **само необходимата** информация за учебни цели.
- Данните се съхраняват сигурно и за ограничен период, според вътрешните правила за архив.
- Учениците и родителите се информират за целите на обработване и правата им.
- При нарушение на сигурността се задейства процедура за инцидент и уведомяване.

12) Обучение и информираност

- Ежегодни занятия по **дигитална грамотност и онлайн безопасност** за ученици по възрастови групи.
- Обучения за учители относно методи за превенция и реакция.
- Среци с родители: разпознаване на рискове, родителски контроли, баланс екран– време.

13) Санкции и корективни мерки

- Нарушенията се разглеждат по реда на училищния правилник и закона.
- При системни или тежки нарушения се уведомяват компетентните органи.
- Предпочитат се **възпитателни и възстановителни** мерки: разговор, консултации, задания по темата, общественнополезни дейности в училище.

14) Влизане в сила, преглед и актуализация

- Правилата влизат в сила от датата на утвърждаването им със заповед на директора.
- Преглеждат се **ежегодно** и при нужда се актуализират (например при технологични промени или нормативни изисквания).
- Всички ученици и родители се запознават срещу подпис; правилата се публикуват на интернет страницата на училището.

15) Отговорност

Отговорността за гарантиране правата на децата и защита на техните интереси е споделена отговорност между семейството, обществото и държавата, чрез нейните органи и институции. Въпреки това, тази отговорност е разпределена, като тя се пада приоритетно на семейството, по-специално на родителите, настойниците, попечителите или другите лица, при които детето е настанено, тогава когато е била предприета мярка за закрила по отношение на него. Отчитайки трудовата ангажираност на родителите, в някои от случаите и трудностите, които изпитват в отглеждането и възпитанието на детето, в основополагащия международен акт за правата на детето Конвенцията на ООН за правата на детето, както и в редица нормативни актове от националното ни законодателство, е посочено как обществото, социалните и образователните институции, и държавата изпълняват тези свои отговорности за оказване на адекватна подкрепа на семейството, за закрила на детето и за защита на неговите права и интереси. Съгласно Конвенцията на ООН за правата на детето, родителите имат първостепенна отговорност за осигуряване висшите интереси на детето да бъдат първостепенно съображение. Родителите или, според случая, законните настойници, попечители или други лица, при които детето е настанено, носят отговорност за отглеждането и развитието на детето. Държавата, чрез нейните органи, трябва да предприеме подходящи стъпки, за да подкрепи родителите при изпълнението на техните отговорности. Ако някои родители не могат или се затрудняват, то в тези случаи се намесват отговорните държавни институции, за да осигурят спазването на правата на детето и задоволяването на неговите нужди. Задължение на държавата е осигуряване развитието на институции, заведения и услуги. В тази връзка ролята на образователните институции е изключително важна и ключова. Те могат да допринесат за обучението и превенцията на рисковете не само на децата, но и на родителите, като по този начин могат да имат двойна полза за децата. В тази посока настоящите правила, дават основни познания за опасностите, които крие виртуалното пространство с цел осигуряване закрилата на детето от вредни за него информация, материали и контакти.

Основните принципи за работа в компютърната мрежа в училище и в интернет са:

1. Равен достъп на всички деца и ученици;

2. Защита на децата и 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;

4. Подготовка и контрол на децата и учениците за безопасно и отговорно поведение онлайн;

5. Сътрудничество в дух на толерантност и добронамереност между училището и родителите/настойниците.

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 таблети) с безжичен достъп до интернет.

Децата и 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 за целите на учебния процес.

ВАЖНО! Правилата за безопасна работа в интернет, които децата и учениците са задължени да спазват, се поставят на видно място в образователната институция, както и в

компютърните кабинети, така и на сайта на детската градина/училището. В началото на учебната година на първата родителска среща през месец септември 2023г. всички деца и техните родители/настойници/попечители са запознават с тях. Педагозите периодично напомнят за тях и за сигурността в интернет в подходящи форми и дейности, в които се включват децата/учениците и родителите им.

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

Директорът на детската градина/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 децата и учениците и родителите/настойниците с правилата за безопасна работа в мрежата. Отговорници за класните ръководители 1-7 клас и ЗКК – Васвие Адем.
5. Осигурено отговорно лице, което да изпълнява функциите на системен администратор и завеждащ компютърен кабинет – Васвие Адем /учител в ОУ „Ран Босилек“/.

Учителите, педагогическите специалисти и ръководителите по направление ИКТ са длъжни да:

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 децата и учениците в мрежата на образователната институция в учебно време.
3. Предприемат незабавни мерки за преустановяване на достъпа на децата и 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 деца и ученици – обект на кибертормоз, чрез първоначална психологическа подкрепа от училищния педагогически съветник – Невена Стоенчева, чрез разговор от страна на педагог/кл. ръководител за снижаване на напрежението у детето.
6. Сигнализират при необходимост Дирекция „Социално подпомагане“ по местоживееие на детето/ученика с цел оценяване на нуждата от насочване към социални услуги за оказване на последваща подкрепа.

Системният администратор:

1. Осигурява общата безопасност и функционалност на мрежата.
2. Предлага и прилага мерки, ограничаващи достъпа на децата и 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 трафика, осъществяван чрез компютърната мрежа на образователната институция.
5. Предприема незабавни мерки за преустановяване на достъпа на децата и учениците до незаконно и вредно съдържание в мрежата.

6. Уведомява незабавно директора на детската градина/училището при случаи на кибертормоз, нарушаване на правилата или при установяване на незаконно съдържание или поведение в мрежата.

7. Съдейства за установяване на извършители на кибертормоз и прилага мерки за ограничаване на такива случаи.

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.

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 и 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 и директора на ОУ „Ран Босилек“

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.

Общи правила за безопасно общуване в интернет за децата и учениците (адаптирани за тях)

Ако се затруднявам в тяхното разбиране, мога да получа подкрепа от родител или от учител, за да ми бъдат обяснени:

1. Не давам лична информация: име, адрес, парола от електронна поща, профил в социална мрежа, личен телефонен номер, училището, в което уча.

2. Не давам информация за местоработата или личен и служебен телефонен номер на родителите, настойниците, близките, приятелите, съучениците и познатите си без тяхно разрешение.

3. Не изпращам и не качвам онлайн свои снимки и видеа, без преди това да е обсъдено и взето решение с родителите ми.

4. Не изпращам и не качвам онлайн снимки и видеа на приятели, съученици, роднини, учители, близки, познати и др., без преди това да е обсъдено с тях, а в случаите, когато се касае за мои приятели, съученици, да е съгласувано от тяхна страна и с родителите им.

5. Не отговарям и не отварям прикачени файлове на електронна поща, получена от непознат подател. Тя може да съдържа вирус или друга зловредна програма, която да увреди компютъра/телефона/таблета или да го направи уязвим за външен достъп.

6. Ще се посъветвам с родителите си/учител, преди да сваля или инсталирам нова програма/приложение на компютър, телефон, таблет, както и не правя нищо, което може да увреди компютъра или чрез дадено действие да се разкрият данни за мен и семейството ми.

7. Нещата, които правя в интернет, не трябва да вредят на други хора или да противоречат на установените правила.
8. Известно ми е, че е забранено да се използва чуждо потребителско име, парола и електронна поща.
9. Не пиша и не качвам нищо, което може да е обидно или унижително за мен или за други хора.
10. Незабавно информирам възрастен (родител, учител, директор, педагогически съветник), когато попадна на материали, които ме карат да се чувствам неудобно или 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.
11. Не отговарям на съобщения, които са обидни, заплашителни, неприлични или ме карат да се чувствам неудобно. Информирам родителите си/класния ръководител, учител, директор, педагогически съветник за такива съобщения.
12. Ако някой ме обижда или тормози онлайн, не отговарям. Докладвам го на отговорен възрастен (родител, учител, директор, педагогически съветник). Мога и сам да докладвам, като подам сигнал на самия сайт или на посочените адреси: www.gdbop.bg; www.cybercrime.bg; www.spasidete.com; www.facebook.com/bgcybercrime; www.safenet.bg и го блокирам. Добре е да направя веднага екранна снимка (скрийншот) на съответния разговор или съдържание като електронно доказателство, което предавам на отговорен възрастен (родител, учител, директор, педагогически съветник).
13. Внимавам, когато разговарям в чат. **Помня правило №1: че хората онлайн не винаги са тези, за които се представят и могат да търсят определена информация, с която да злоупотребят с мен или с другите хора. Правило №2 е че не правя нищо на друг човек в мрежата, което не искам да ми се случи и на мен.**
14. Ако се случи да попадна на информация или друго съдържание в Мрежата, което не ми харесва или ме плаши по някакъв начин, мога да подам 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 .

15. Не трябва да приемам срещи с лица, с които съм се запознал/а в интернет, освен след съгласието на родителите ми. Помня, че хората, с които се запознавам онлайн, не винаги са тези, за които се представят. Опитвам се винаги да проверявам дали човекът отсреща наистина е този, за когото се представя чрез проверка по име, имейл, снимка и контролен въпрос, на който би трябвало да знае отговора, ако е наистина този. При съмнение може да подам сигнал или да потърся съвет през сайта на Центъра за безопасен интернет www.safenet.bg.

16. Използвам настройките за безопасност и защитата на личните данни на социалните мрежи, мобилните приложения и браузърите.

17. Използвам функцията за безопасно сърфиране. Не посещавам сайтове в интернет, които са със съдържание, неподходящо за детска аудитория.

18. Използвам трудни (дълги, с главни и малки букви, цифри и специални знаци) и различни за всеки сайт пароли.

19. Използвам антивирусна програма, която следва редовно да се обновява. Заедно с отговорните възрастни (родител, учител, директор), поддържам последните актуализирани версии на всички програми и приложения.

20. Ако ползвам общи компютри, винаги проверявам дали съм излязъл/излязла от профила си, след като свърши часа. В случай, че намеря устройство, на което друг ученик е работил, но не е затворил профила си, веднага ще изляза без да преглеждам, променям или добавям информация в профила му.

КРАТЪК РЕЧНИК И ДОПЪЛНИТЕЛНИ СЪВЕТИ:

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. 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.

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 поголямата 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 защиты.

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.

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 –

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.

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, едн който 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 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 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 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 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.