ПРОФЕСИОНАЛНА ГИМНАЗИЯ ПО ОБЛЕКЛО „КНЯГИНЯ МАРИЯ ЛУИЗА”
гр. София, бул.”Черни връх” №37, тел: 862-88-84, 862-23-85,
e-mail: pgo@abv.bg, http://www.pgo-sofia.com

УТВЪРЖДАВАМ:
ИНЖ. ПАУЛИНА КОСТОВА
Директор на ПГО „Княгиня Мария Луиза”

Правила за безопасна работа на учениците в училищната компютърна мрежа и в интернет

учебната 2023 / 2024 година

гр. СОФИЯ
2023 г.

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 правата на родителите, свързани с работата на учениците в **училищната мрежа и в Интернет**, наричани по-нататък за краткост "мрежата".

Чл. 2. Училищната политиката 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. Правилата се прилагат в училищата и обслужващите звена от системата на народната просвета, които осигуряват на учениците достъп до училищната компютърна мрежа и в Интернет.

Чл. 4. Основните принципи на училищната политика за работа в училищната мрежа и в Интернет са:

1. Равен достъп на всички ученици;
2. Защита на учениците от вредно или незаконно съдържание и информация като: 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 и родителите;

Чл. 5. Училищната компютърна мрежа и Интернет се използват от учениците само за образователни цели.

Чл. 6. 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 или на обслужващото звено

Чл. 8. (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 училищната Интернет страница и осигурява наблюдение и контрол върху нейното 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 и вкъщи.
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 изпълнението на задълженията си по ал. 1, т. 5, 6, 7, 9, 10 и 11 на други служители от училището или обслужващото звено.

III. Правомощия на учителите и системните администратори

Чл. 9. Учителите 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. Удостоверяват регистрацията на учениците по чл. 7.
4. Предприемат незабавни мерки за преустановяване на достъпа на учениците до незаконно съдържание в мрежата.
5. Уведомяват незабавно директора на училището или на обслужващото звено при нарушаване на правилата или при установяване на незаконно съдържание в мрежата.
Чл. 10. Учителите не носят отговорност, ако учениците случайно попаднат на вредно или незаконно съдържание в Интернет.
Чл. 11. Системният администратор 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 или на обслужващото звено при нарушаване на правилата или при установяване на незаконно съдържание в мрежата.

IV. Права и задължения на учениците

Чл. 12. 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. 13. 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, 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.
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. 14. Родителите имат право:
1. Да бъдат информирани за училищната политика за безопасна работа в мрежата.
2. Да участват със 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 в къщи.
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. 13.
6. Получат информация за информационно-сигнализационни платформи като www.gdbop.bg; www.cybercrime.bg; www.spasidete.com; www.safenet.bg; www.facebook.com/bgcybercrime.

Чл. 15. 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 местоживеене на детето с цел оказване на психологическа подкрепа на детето. В този случай трябва да уведомят и директора на образователната институция.
5. Съхраняват здравето на детето, като проследяват времето за използване на интернет.
6. Уведомят директора на ПГО „Княгиня Мария Луиза", когато им стане известно, че детето им е обект на тормоз от друго дете, което също е от гимназията

VI. Отговорност

Чл. 16. (1) При нарушаване разпоредбите на тези правила директорът, учителите носят отговорност по Кодекса на труда.
(2) При нарушаване разпоредбите на тези правила системният администратор, в зависимост от правоотношенията му с училището, носи дисциплинарна или гражданска отговорност.
(3) При нарушаване разпоредбите на тези правила на учениците могат да се налагат наказанията, предвидени в чл. 199 ал. 1 от Правилата за прилагане на ЗПУО. Наказанията се налагат при условията и по реда, предвидени в ЗПУО
Чл. 17. Независимо от отговорността по чл. 16, при нарушения, които представляват престъпления, административни нарушения или причиняват имуществена вреда, се носи съответно наказателна, административна или гражданска отговорност.

Част VII. Общи правила за безопасно общуване в интернет за учениците **Като ученик съм длъжен** да спазвам следните правила. 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, детската градина/училището, в което уча.
2. Не давам информация за месторабoтата 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 (част от тях са уредени в закони).
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 унизително за мен или за други хора.
10. Незабавно информирам възрастен (родител, учител, директор, психолог), 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

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.

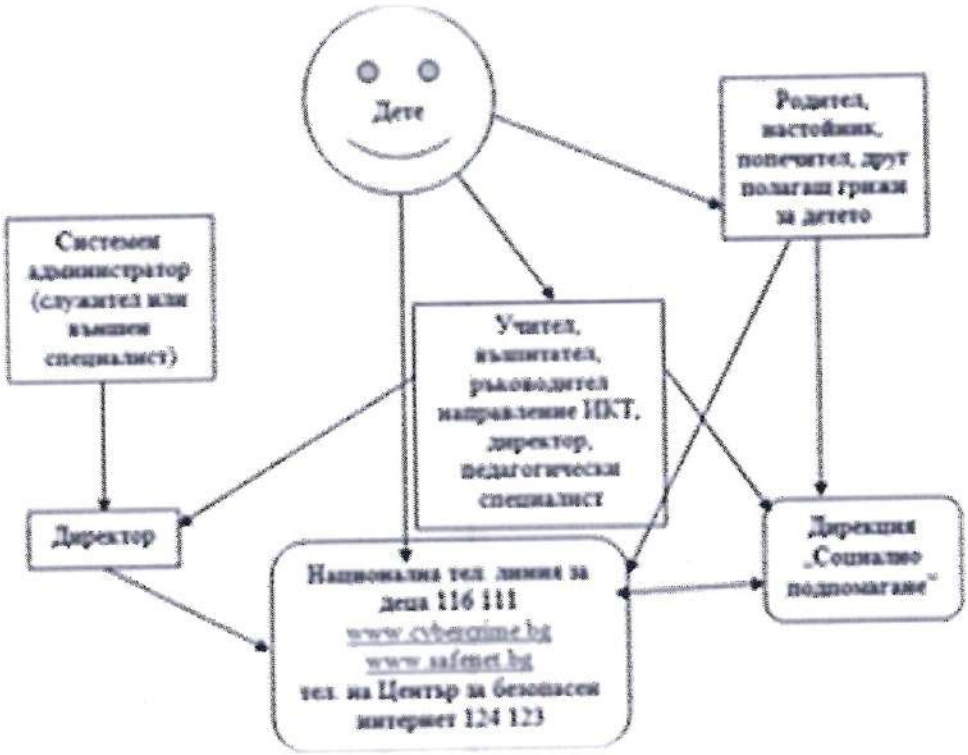
17. Използвам функцията за безопасно сърфиране. Не посещавам сайтове в интернет, които са със съдържание, неподходящо за детска аудитория.

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 де 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.

СХЕМА ЗА УВЕДОМЯВАНЕ В СЛУЧАЙ НА КИБЕРТОРМОЗ



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 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.

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.

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 предлагащи 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. Скритите 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 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 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, 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 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.