



Препоръки за безопасна работа в дигитална образователна среда

Комисия за защита на личните данни, Актуални въпроси от обществен интерес

Твоите лични данни и интернет – съвети за деца

Докато работиш в интернет,

1. Не давай лична информация като име, парола, адрес, домашен телефон, месторабота и служебен телефон на родителите си или училището, в което учиш.
 2. Не изпращай свои снимки или снимки на твои близки, без преди това да си обсъдил решението си със своите родители.
 3. Винаги преди да качиш своя снимка и/или да публикуваш своя мобилен номер, помисли добре дали искаш и ще е добре ли за теб тази информация да стане достъпна за един неограничен кръг от хора.
 4. Не приемай среща с някого, с когото си се запознал в интернет, без знанието на твоите родители. Ако те одобрят срещата, нека тя да е на публично и оживено място и задължително да е в присъствие на твои близки или приятели.
 5. Не отговаряй на съобщения, които са обидни, заплашващи, неприлични или те карат да се чувстваш неудобно. Информирай родителите си или друг твой близък възрастен човек за такива съобщения и за техния източник.
 6. Не отваряй приложения на електронна поща, получени от непознат подател. Те могат да съдържат вирус или програма, която да увреди твоя компютър или да черпи неограничено информация от него.
 7. Внимавай, когато някой ти предлага нещо безплатно или те кани да се включиш в дейност, обещаваща лесна, бърза и голяма печалба. В тези случаи, най-вероятно, ще станеш жертва на измама.
 8. Бъди внимателен и наблюдателен при попълване на регистрационните форми при извършване на регистрация в интернет сайтове.
 9. При регистрации винаги проверявай има ли данни на сайта относно администратора/модераторите, които го поддържат, както и възможност за обратна връзка с тях – адрес за контакт.
 10. Чети „Условията за ползване” на сайта, преди да се съгласиш с тях! Там трябва да бъде предоставена информация относно необходимостта и целта на събирането на лични данни на потребителя. В случай че такава информация не е предоставена и не ти е предоставена възможност да се обърнеш към администратора/модераторите на съответния сайт или в тях се съдържа информация, която те притеснява, то тогава сигнализирай на горещите линии, като подадеш оплакване. Трябва да знаеш, че всеки администратор/модератор, който поддържа конкретен сайт, е длъжен да даде информация относно това за какво са му необходими твоите лични данни, за какво ще ги ползва, за какъв срок, какво ще се случи с тях, когато те вече няма да са му необходими за тази цел, за която си му ги предоставил (например регистрация), както и на кого и поради какви причини той ще може да ги даде.
 11. Не чети и не разглеждай сайтове, които съдържат материали с вредно или незаконно съдържание. Единственото нещо, което те биха могли да ти донесат са вреди, неприятности и проблеми. Няма нищо грешно и лошо в това, че от чисто любопитство, случайно или по съвет от „приятел” в нета си достъпил сайт с вредно или незаконно съдържание. Не се притеснявай да споделиш това с родител или друг твой близък възрастен човек. Именно той ще ти даде най-добрия съвет как да постъпиш в тази ситуация.
- Какво означава „сайт с вредно съдържание”?



Това са интернет страници, чието съдържание оказва или би могло да доведе да травмиращо психично въздействие или да подтикне техните ползватели към поведение, водещо до психични и/или физически травми.

Какво означава „сайт с незаконно съдържание“?

Това са интернет страници, на които е публикуван или качен материал, за който в закон е предвидена забрана и се носи съответната отговорност.

12. Използвай на максимум възможностите, които предоставя конкретният сайт за социални контакти за защита на твоя профил и информацията, която си качил на него.

13. Внимавай, когато разговаряш в чат, дискуссионни форуми, социални мрежи и т.н. Помни, че хората онлайн често могат да се представят за такива, каквито не са. Важно е да знаеш, че възможността, която предоставя мрежата на теб да останеш анонимен или да се представиш за друг, се предоставя и на всички други участници в нета!

14. Нещата, които правиш в Интернет, не трябва да вредят на други хора или да противоречат на законите. Бъди вежлив и уважавай правата и достойнството на другите участници в интернет.

15. Консултирай се с родителите си, преди да свалиш или инсталираш нова програма на компютъра си. Не прави нищо, което може да увреди компютъра ти или чрез дадено действие от твоя страна да се разкрият данни за теб и семейството ти.

16. Споделяй с родителите си или с друг възрастен твой близък за начините, чрез които се забавляваш, информираш и научаваш нови неща от Интернет.

17. Бъди разумен и изобретателен при избора си на пароли. Помни: Паролите трябва да се променят периодично. Колкото по-дълго време използваш една и съща парола, толкова по-голям е рискът тя да бъде разкрита.

18. Използвай антивирусен софтуер. Обновявай го редовно и не забравяй да сканираш компютъра периодично.

19. В случай, че попаднеш на информация или други неща в Мрежата, които не ти харесват или те плашат по някакъв начин и нямаш възможност да го споделиш с родител или с друг възрастен твой близък, то тогава ти можеш да подадеш сигнал на адрес: <http://web112.net/>, <http://www.safenet.bg/> или <http://www.cybercrime.bg/bg>

Личните данни и интернет – съвети за родители

Посъветвайте вашето дете:

- Да не дава лична информация като име, парола, адрес, домашен телефон, училището, в което учи, месторабота или служебен телефон на родителите си, както и друга лична информация за себе си, приятелите си, за вас, за братя, сестри или други роднини и близки без вашето или тяхно изрично разрешение.
- Да не приема среща с някого, с когото се е запознал чрез социалните мрежи, сайтовете за запознанства, форумите, чат програмите или по друг начин чрез интернет, без вашето знание и съгласие. Трябва да знае, че един човек може да има няколко регистрирани профила и винаги може да се представи за някой друг. За това е необходимо отделяне на специално внимание към тази категория сайтове с оглед на сигурността на детето.
- Да не отваря и да не отговаря на електронни съобщения/писма, получени от непознат подател, тъй като те могат да съдържат вирус или друга програма, която да увреди софтуера или хардуера на компютъра, както и да позволи безпрепятствен достъп до съдържащата се в него информация.
- Да не отговаря на съобщения, които са обидни, заплашващи, неприлични или го карат да се чувства неудобно и във всички тези случаи да ви информира за такива съобщения.
- Да не изпраща свои снимки или снимки на свои близки, без преди това да е обсъдил решението си с вас. Обърнете му внимание, че публикуването на негови снимки или



качването на видео в социалните мрежи и сайтовете за запознанства прави достъпни тези материали за огромен кръг от хора. Включването на уеб камера в реално време при разговор с непознат в чат програмите води до същия ефект. Лесният достъп до публикувани снимки или видеоматериали може да даде възможност на хора, които искат да му навредят, да ги използват по начин, който да го злепостави.

· Да не се доверява на хора, с които се познава от и общува във виртуалния свят, да не споделя с тях свои или на близките си лични данни, които могат да бъдат от различно естество, но в своята съвкупност да доведат до идентификация на детето или на неговите родители, братя, сестри, приятели и др. Изострете му вниманието върху, това да не предоставя и да не публикува собственото си име или това на близки и приятели, адрес, данни за училището, в което учат, телефон /стационарен или мобилен/.

Предоставянето или публикуването на името и адреса на дома и/или училището, в което учи, в интернет ще даде възможност на всеки, който има за цел да го открие в реалния свят, да го идентифицира и да стигне до него. Опасността, която крие предоставянето на телефонният номер, било стационарен или мобилен, може да доведе до телефонен тормоз от страна на злонамерени хора, както и да бъде използван от тях за злепоставящи действия и публикации в нета и извън него.

· Да се консултира с вас винаги преди да сваля или инсталира нова програма или друг софтуер на компютъра.

· Да внимава и да се съобразява с правилото - нещата, които прави в Интернет, да не вредят на други хора или да противоречат на законите.

· Да внимава, когато създава нови познанства и провежда разговори в чата - хората онлайн често се представят за такива, каквито не са.

· Да споделя с вас начините, чрез които се забавлява, игрите, които харесва, и новите неща, които научава от Интернет.

· Да пази паролите си, да не ги споделя с никого и да ги променя периодично.

· В случай, че попадне на информация, която го плаши или го притесни по един или друг повод, да сподели това с вас или да подаде сигнал на горещата линия за безопасен интернет: <http://web112.net/>, <http://www.safenet.bg/> или <http://www.cybercrime.bg/bg>, чрез предвидения за тази цел паник бутон.

Какво може да направите, за да се погрижите за безопасността на детето в интернет

1. Поемете лична отговорност за безопасността на детето си в Интернет.

2. Наложете правила за безопасно ползване на Интернет и следете за тяхното стриктно спазване.

3. Поставете компютъра в обща стая/помещение. Поставянето на компютъра в общо помещение ще ви даде възможност да станете „страничен” и „недосаждащ” свидетел на посещаваните интернет страници от детето, както и на всички извършени от него посещения, действия, дискусии и т.н. поне за периода от време, през който сте заедно.

4. Провеждайте периодични разговори с детето за опасностите, които крие интернет, и начините, по които то може да се защити. Обяснете му колко е важно да пази личните си данни и тези на своите близки, роднини и приятели и да не ги предоставя на „онлайн приятели”, като говорите с него свободно относно злоупотребите, за които могат да бъдат използвани те.

5. Създайте потребителски профил на детето си на компютъра в къщи. Децата трябва да имат собствени акаунти на компютъра. Това е много ефикасен начин за контрол на дейностите им в интернет. И още нещо: администратор на домашния компютър трябва



СУ "НАЗЕМ ХИКМЕТ" с. МЕДОВЕЦ, общ. ДЪЛГОПОЛ, обл. ВАРНА

ул.Първа№22, tel.0517-52-081

e-mail:medovets_sou@abv.bg, www.su-nhikmet.com

задължително да бъде възрастен човек. Акаунта на детето задължително трябва да бъде без или с ограничени администраторски права.

6. Инсталирайте програма за родителски контрол - програмата за родителски контрол ще ви предостави възможност да ограничите достъпа на вашето дете до сайтове с неподходящо за него съдържание, да наложите времеви рестрикции за ползване на компютъра, да блокирате ползването на определени програми и т.н.

7. Прекарвайте повече време със своите деца, като: играете на предпочитаните от тях компютърни игри или разглеждате интересните за тях интернет страници - така ще разберете за навиците им, и за тяхното поведение в мрежата, за желанията и интересите им.

8. Сърфирайте заедно в Интернет и едновременно с това ги учите на безопасно и етично поведение в мрежата.

9. Станете приятел с детето си във виртуалния свят – направете регистрация в ползваните/достъпваните от него електронни дискуссионни групи, социалните мрежи, чат програми, които представляват форум за обмен на знания, информация, видеоклипчета, снимки, дискусии, създаване на нови запознанства и др. Това ще ви даде възможност да имате пряк поглед върху поведението на детето ви в мрежата.