ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД

ОПЕРАТИВНА ПРОГРАМА НАУКА И ОБРАЗОВАНИЕ ЗА ИНТЕЛИГЕНТЕН РАСТЕЖ

ПРОЕКТ „ОБРАЗОВАНИЕ ЗА УТРЕШНИЯ ДЕН“

КЛУБ „В СВЕТА НА ДИГИТАЛНИТЕ ТЕХНОЛОГИИ“

ПРИ

ТЕХНИЧЕСКА ПРОФЕСИОНАЛНА ГИМНАЗИЯ

„НИКОЛА ЙОНКОВ ВАПЦАРОВ“ ГРАД РАДОМИР

МОИТЕ ПРАВА И ОТГОВОРНОСТИ В МРЕЖАТА

БЕЗОПАСНО СЪРФИРАНЕ В ИНТЕРНЕТ

ОНЛАЙН ОБЩУВАНЕТО – КАКВИ СА РИСКОВЕТЕ?

ИГРИТЕ В ИНТЕРНЕТ – ЗАБАВЛЕНИЕ И РИСКОВЕ

ХАКЕРЪТ – КРАДЕЦ НА ИНФОРМАЦИЯ ИЛИ ГЕРОЙ НА ДЕНЯ

МОИТЕ ПРАВА И ОТГОВОРНОСТИ В МРЕЖАТА

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

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

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

4. Не трябва да изпращам и да 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 трябва да отговарям и да отварям прикачени файлове на електронната поща, получени от непознат подател. Те могат да съдържат вирус или друга зловредна програма, която да увреди компютъра/ телефона/ таблета или да го направи уязвим за външен достъп.

Децата
безопасно
в Интернет

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.

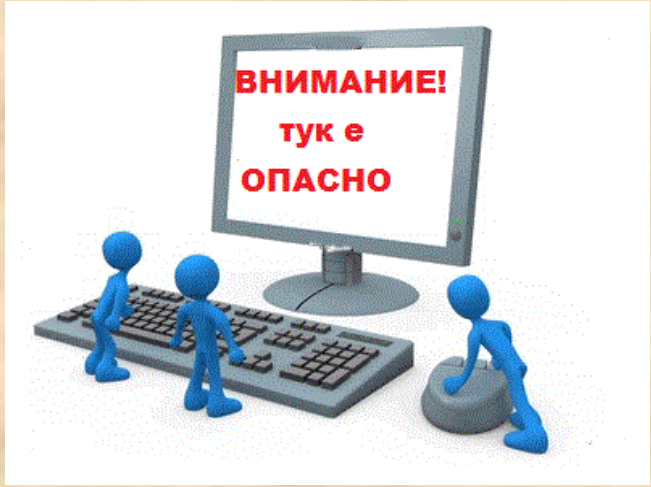
7. Нещата, които правя в интернет, не трябва да вредят на други хора или да противоречат на установените правила (част от тях са уредени в закони).

8. Не трябва да използвам чуждо потребителско име, парола и електронна поща.

9. Не трябва да пиша и качвам неща, които може да са обидни или унизителни за другите 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.



14. 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.**

12. 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 правило №2, е че не правя нищо на друг човек в мрежата, което не искам да ми се случи и на мен.

13. Ако някой ме обижда или тормози онлайн, не отговарям. Споделям с отговорен възрастен (родител, учител, директор, педагогически съветник). Мога и сам да докладвам, като подам сигнал 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).

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

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

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

18. 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.

19. 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.

ОНЛАЙН ОБЩУВАНЕТО – КАКВИ СА РИСКОВЕТЕ?

Интернет е уникална възможност не само за достъп до огромно количество информация, а и като средство за комуникация на младото поколение. Особено примамливи при онлайн общуването са няколко неща:

• много лесно се създават нови контакти, които могат да бъдат прекратени само с едно кликване;

• даване на възможности да бъдеш този, който искаш, или поне да се представиш за него, защото си анонимен;

• в мрежата винаги ще намериш някой, който да има сходни интереси, който е съпричастен към твоите проблеми.

Тези три предимства носят и най-голямата опасност в интернет. Психолозите твърдят, че една връзка укрепва, благодарение на усилията да я поддържаме, а лекотата, с която се свързваме и разделяме с виртуалните си приятели, ни откъсва от реалното пълноценно общуване и ни остава единствено мрежата с нейните краткотрайни и лишени от емоция отношения. Често пъти чрез електронната поща, дискусионните форуми, обявите и различните форми на онлайн общуването подрастващите са податливи на влияние и внушения от страна на непознати партньори в електронната комуникация. Те могат да влязат в киберсексуални, а дори и реални сексуални връзки с партньори от интернет.

ИГРИТЕ В ИНТЕРНЕТ – ЗАБАВЛЕНИЕ И РИСКОВЕ

Със сигурност пристрастяването към игрите е една от най-коментираните теми. Много е трудно да се предупреждават младите хора за дейност, която им носи удоволствие и на пръв поглед не вреди на никого. Родителите обикновено обвиняват игрите, пълни с насилие и агресия, а психолозите казват, че не игрите пристрастяват, а геймърите са податливи на пристрастяване. Зависимостта към интернет те сравняват с всички останали зависимости. Пътят до обсебването е употреба, злоупотреба и зависимост. Времето, прекарано без получена поща, например, е истински кошмар. Облекчението идва при поредното писмо, дори и да е спам.

Съществен е и проблемът с насилието в игрите. Пристрастеното към такива игри детето става агресивно към околните, защото мисълта му е обсебена от бройката на “убитите” виртуални противници. Много често децата са повлияни от интернет - пристрастяването, губят реална представа за света и случващото се около тях. Усещането за време изчезва и те стават неспособни да “съществуват” в реални условия. Човек, пристрастен към комуникацията в чатове и форуми, както и към игрите, губи способността си за нормално общуване. Счита се, че поподатливи на обсебване са хората с лични и емоционални проблеми, но при децата не винаги интернет пристрастяването се свързва с изявени проблеми – просто комуникацията в чата е много по лесна от живия контакт.

Специалистите определят следните основни признаци на интернет-зависимост:

А. Психически:

1. чувствате еуфория, когато сте пред компютъра;
2. прекарвате по-голяма част от деня си в мрежата;
3. пренебрегвате близки и приятели заради виртуални контакти и занимания;
4. чувствате пустота и раздразнение, когато не сте пред компютъра;
5. криете от близките, че прекарвате голяма част от деня в мрежата;
6. имате проблеми с успеха в училище.
7. човек постепенно губи възможността да поддържа отношения с реалните приятели.

Б. Физически:

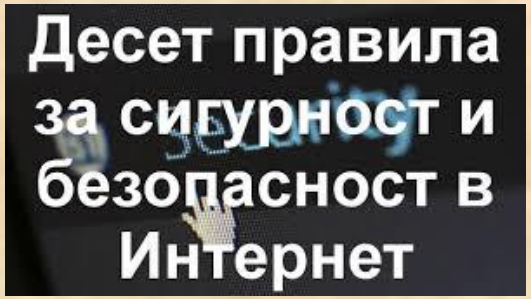
1. често главоболие;
2. сухота в очите;
3. болки в гърба;
4. загуба на апетит, пропускане на хранене заради заниманията с компютъра;
5. пренебрегване на личната хигиена;
6. проблеми със съня и промяна на режима.

ХАКЕРЪТ – КРАДЕЦ НА ИНФОРМАЦИЯ ИЛИ ГЕРОЙ НА ДЕНЯ

Развитието на глобалните комуникации кара някои хора да приемат като предизвикателство преодоляването на компютърни защити и проникване в чужди данни. Техните “умения” са подсъдими, защото реално са посегателство върху чужда интелектуална собственост и причиняват вреда на другите. Хакерите и кракерите се приемат от тийнеджърите като “героите на деня”, които разбиват правилата и не им “пука” от нищо. В същото време хакерите често влизат непозволено в профила, мейла, както и личния компютър.

По този начин те биха могли да използват наличната информация за различни форми на злоупотреба и манипулация, могат да сменят данните в профила, да пускат вируси и т.н. И хакерите (hackers), и кракерите (crackers) се занимават с решаването на една и съща задача – търсене на уязвимостта в информационната система. Разликата е в тяхната гледна точка към проблема. Хакер – изследва информационната система с цел откриване на слабите й места (уязвимостта) и информира потребителите за отстраняването им. Анализира съществуващата сигурност на системата, формулира необходимите изисквания и условия за повишаване нивото й на защита. Кракер – осъществява несанкциониран достъп до системата с цел кражба, подмяна, унищожаване на информация или обявяване факта на достъпа.

БЕЗОПАСНО СЪРФИРАНЕ В ИНТЕРНЕТ



1. Използвай сигурна парола за профилите си.
2. Прави редовно архивно копие на информацията си (backup).
3. Пази се от онлайн вируси.
4. Информирай се за актуалните измами в интернет пространството, за да не станеш жертва на такава
5. Не отваряй съмнителни имейли.
6. Внимавай в кои сайтове влизаш.
7. Използвай само достоверни източници.
8. Внимавай какви приложения си качваш и какъв достъп им даваш.
9. Внимавай какъв дигитален отпечатък оставяш.
10. Внимавай с кого и как общуваш.