БЕЗОПАСНОСТ В МРЕЖАТА

ДЪРЖАВНА АГЕНЦИЯ ЗА ЗАКРИЛА НА ДЕТЕТО • ДАЗД •

„Часовете пред компютъра и в мрежата са полезни и приятни за всички нас. Прекарваме времето си като се забавляваме, научаваме много неща, развиваме въображението и рефлексите си. Участваме във виртуални срещи, създаваме интересни контакти, посещаваме непознати и нови светове. Така времето ни лети неусетно, а и често си спестяваме много усилия като бързо събираме информация и решаваме задачи в ежедневието си. Продължителният престой в онлайн среда обаче съвсем не е безопасен за емоциите, психическия ни комфорт и за физическото ни здраве. Ето защо тук на едно място сме събрали ценни съвети и правила, които ако се спазват, ще предпазят и малки, и големи от неприятности. Лесно е – запомняме ги и се пазим. Може да ги предадем в помощ на своите близки и познати. Ако всички спазваме правилото да не правим на другите това, което не искаме да се случи на нас, ще имаме един чудесен и полезен свят за сърфиране в интернет."

д-р Елеонора Лилова, председател на ДАЗД.

ПРАВИЛА, ЗА ДА СИ В БЕЗОПАСНОСТ В МРЕЖАТА

1. Пази и не давай на други хора в интернет личната си информация: име, адрес, парола от електронна поща, профил в социална мрежа, личен телефонен номер, училището, в което учиш.

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

3. Пази и не изпращай и/или не качвай онлайн свои снимки и видеа, без преди това да е обсъдено и взето решение с родителите ти или хората, които се грижат за теб.

4. Не изпращай и не качвай 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 твои приятели и съученици, да е съгласувано от тяхна страна и с родителите им/учители.

5. Не отговаряй и не отваряй прикачени файлове на електронната ти поща, получена от непознат подател. Тя може да съдържа вирус или друга зловредна програма, която да увреди компютъра/телефона/таблета/устройството ти или да го направи уязвимо/недостъпно за външен достъп.

6. Посъветвай се с родителите си /учител/възрастен, на когото имаш доверие, преди да свалиш или инсталираш нова програма/приложение на компютър, телефон, таблет, както и не прави нищо, което може да увреди компютъра или чрез дадено действие да се разкрият данни за теб и семейството ти.

ИЗПОЛЗВАЙ ТРУДНИ И РАЗЛИЧНИ ЗА ВСЕКИ САЙТ
ПАРОЛИ
MYCLOUDRAIN672
7

8

7. Нещата, които правиш в интернет, не трябва да вредят на други хора или да противоречат на установените правила (част от тях са уредени в закони, които възрастните познават и могат да ти обяснят).

8. Трябва да знаеш, че е забранено да се използва чуждо потребителско име, парола и електронна поща.

9. Не пиши и не качвай нищо, което може да е обидно или унизително за теб, близките ти или за други хора. Всичко в интернет рано или късно се хваща и се разбира кой е причинил вреда на друг човек или група хора

9
WWW.SAFENET.BG

10

10. Незабавно информирай възрастен (родител, учител, директор, педагогически съветник, друг възрастен, на когото имаш доверие) или информирай службите, когато попаднеш на материали, които те карат да се чувстваш 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 отговаряй на съобщения, които са обидни, заплашителни, неприлични или те карат да се чувстваш неудобно. Информирай родителите си /класния ръководител, учител, директор, педагогически съветник или службите за такива съобщения.

11
Wood
MARVY
edd

12

12. Ако някой те обижда или тормози онлайн, не отговаряй. Това може да ти навреди повече, отколкото ако замълчиш и събереш сили да докладваш на отговорен възрастен (родител, учител, директор, педагогически съветник) или службите. Ако си достатъчно отговорен, можеш и сам да докладваш, като подадеш 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 да го блокираш. Добре е да направиш веднага екранна снимка (скрийншот) на съответния разговор/снимка/видеосъобщение или съдържание като електронно доказателство.

13

13. Внимавай, когато разговаряш в чат. Помни!

Правило №1

хората онлайн не винаги са тези, за които се представят и могат да търсят определена информация, с която да злоупотребят с теб, близките ти или с другите хора.

Правило №2

не прави нищо на друг човек в интернет, което не искаш да ти се случи и на теб самия.

14. Ако се случи да попаднеш на информация или друго съдържание в мрежата, което не ти харесва или те плаши по някакъв начин, можеш да подадеш сигнал на денонощната и безплатна Национална телефонна линия за деца 116 111 към Държавната агенция за закрила на детето, на отдел „Киберпрестъпност" на ГДБОП към МВР (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 приемай срещи с лица, с които си се запознал/а в интернет, освен след съгласието на родителите ти. Помни, че хората, с които се запознаваш онлайн, не винаги са тези, за които се представят. Опитвай се винаги да проверяваш 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 подадеш сигнал или да потърсиш съвет през сайта на Центъра за безопасен интернет www.safenet.bg.

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

17. Използвай функцията за безопасно сърфиране. Не посещавай сайтове в интернет, които са със съдържание, неподходящо за аудитория близка до твоята възраст.

15
WWW.CYBERCRIME

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

19. Използвай антивирусна програма, която следва редовно де се обновява. Заедно с възрастни (родител, учител, директор), поддържай последните актуализирани версии на всички програми и приложения.

20. Ако ползваш общи компютри, винаги проверявай дали си излязъл/излязла от профила си, след като свърши часа. В случай, че намериш устройство, на което друг ученик е работил, но не е затворил профила си, веднага излез без да преглеждаш, променяш или добавяш информация в профила му.

21. Трябва да имаш предвид, че когато публикуваш 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.

Важни контакти:

ГДБОП – отдел „Киберпрестъпност“

www.cybercrime.bg

Център за безопасен интернет тел. 124 123

www.safenet.bg

Национална телефонна линия за деца 116 111

към

Държавната агенция за закрила на детето

19

КРАТЪК РЕЧНИК С ПОЛЕЗНА ИНФОРМАЦИЯ 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. Когато се касае за снимки, на 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.

21

ФАЛШИВИ НОВИНИ

Информация с невярно съдържание от неофициални източници. Дезинформация. Манипулация на вярна информация с подмяна на данни, факти, обстоятелства. 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 официални, хумористични и сериозни новинарски сайтове. Запитайте се дали познавате медията и имате ли ѝ доверие? Проверете дали заглавието, което често е гръмко и сензационно отговаря на съдържанието на новината като проверите няколко официални източника и сравнете времето на публикацията, актуалната друга такава информация от няколко източника;
- 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 или **КИБЕРТОРМОЗЪТ** 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 текстове, 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.

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 са 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 някой от обектите на търговеца, от когото 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.

ЗАЩИТА НА КОМПЮТЪРНИТЕ МРЕЖИ ОТ ОПАСНА ЕЛЕКТРОННА ПОЩА

24

1. Не трябва да се проявява инициатива за получаване на имейл писма от 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 и само на проверени лица/организации. 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 отваряйте прикачени файлове в съобщения от непознат изпращач. Ако не се познава името в полето „От", не отваряйте прикачения файл. Внимавайте с обръщенията Mr/Mrs/Dear.

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 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. Внимавайте с измамни съобщения, че сте спечелили от лотарията: 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. Отписвайте се от бюлетин/електронно списание, за които 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.

СЪВЕТИ ЗА ЗДРАВЕТО

За да работите на компютър, без да увредите своето здраве, редувайте онлайн и офлайн дейности и спазвайте следните правила:

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 има прозорец без щори и завеси;
- за да отпочиват очите, от време на време отмествай 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 използващ клавиатура с клавиши, които са под лек наклон.

При работа с мишка:

- мишката трябва да бъде с размера на длан;
- не движи 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.

"Безопасен интернет е, когато мислиш една стъпка напред"
- Диян Калайджиев, Председател на Съвета на децата към председателя на ДАЗД.

"Ти си мислиш, че всичко в интернет е на игра, но внимавай, защото зад монитора може да те дебне врага."
- Ванеса Филипова, член на Съвета на децата към председателя на ДАЗД за София – град.

"Интернетът днес е опасна смес"
- Калина Кръстева, член на Съвета на децата към председателя на ДАЗД за област Хасково

Държавна Агенция за
Закрила на Детето

2020

Текст и съставителство: д-р Елеонора Лилова
и работна група на ДАЗД, ГД ВОП, МОН,
НЦБИ, РУО – София-град, СРСНПБ, СДСОРБ и СБУ.
Художник: Дея Въличева