ГДБОП – отдел „Киберпрестъпност“
www.cybercrime.bg

Център за безопасен интернет тел. 124 123;
www.safenet.bg

Национална телефонна линия за деца
116 111

ДЪРЖАВНА АГЕНЦИЯ за ЗАКРИЛА на ДЕТЕТО * ДАЗД *

КРАТЪК РЕЧНИК С ПОЛЕЗНА ИНФОРМАЦИЯ

ЗА БЕЗОПАСНОСТ В МРЕЖАТА

ДЪРЖАВНА АГЕНЦИЯ за ЗАКРИЛА на ДЕТЕТО * ДАЗД *

ЗАЩИТА НА КОМПЮТЪРНИТЕ МРЕЖИ ОТ ОПАСНА ЕЛЕКТРОННА ПОЩА

1. Откажете получаване на имейл писма с промоции от интернет страници, които предлагат безплатни или платени услуги и стоки

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.

www.cybercrime.bg

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:

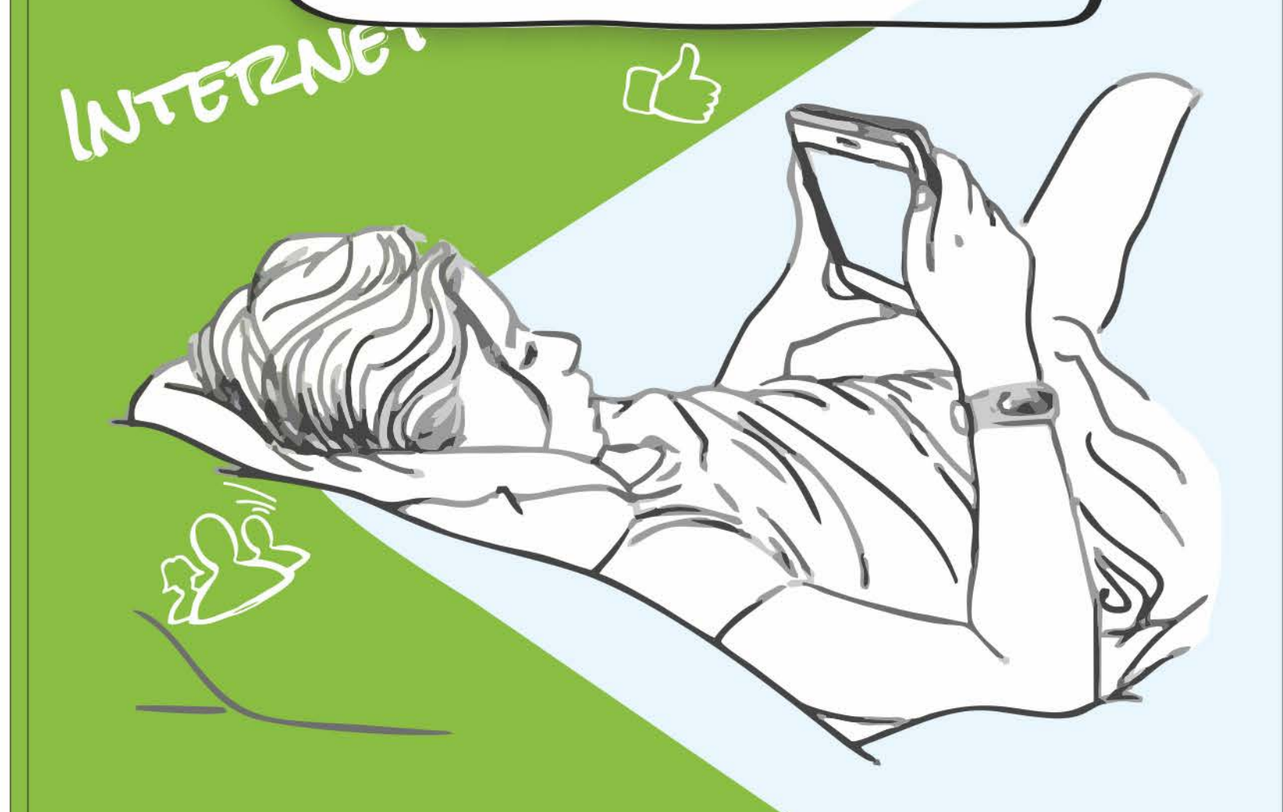
Обръщението е "Dear Customer" или "Dear User", а не Вашето име.

В писмото пише, че акаунтът Ви ще бъде прекратен в случай, че не потвърдите данните си незабавно. 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.

КАЧВАНЕ И СПОДЕЛЯНЕ НА СНИМКИ И ВИДЕО

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 и видеа, 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 и видеа на дете, за които има и най-малкото съмнение, че могат да му навредят и без негово съгласие. Споделянето на снимки и видео материали е често срещано явление в социалните мрежи, затова основна препоръка е те да се споделят само с хората от списъка с приятели на човека, който иска да ги качи, 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 снимки или видео 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 снимки и видеа, които качвате 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.



www.cybercrime.bg

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. Кибертормозът е и 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.

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 се 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 някои от обектите на търговеца, от който 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.

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.

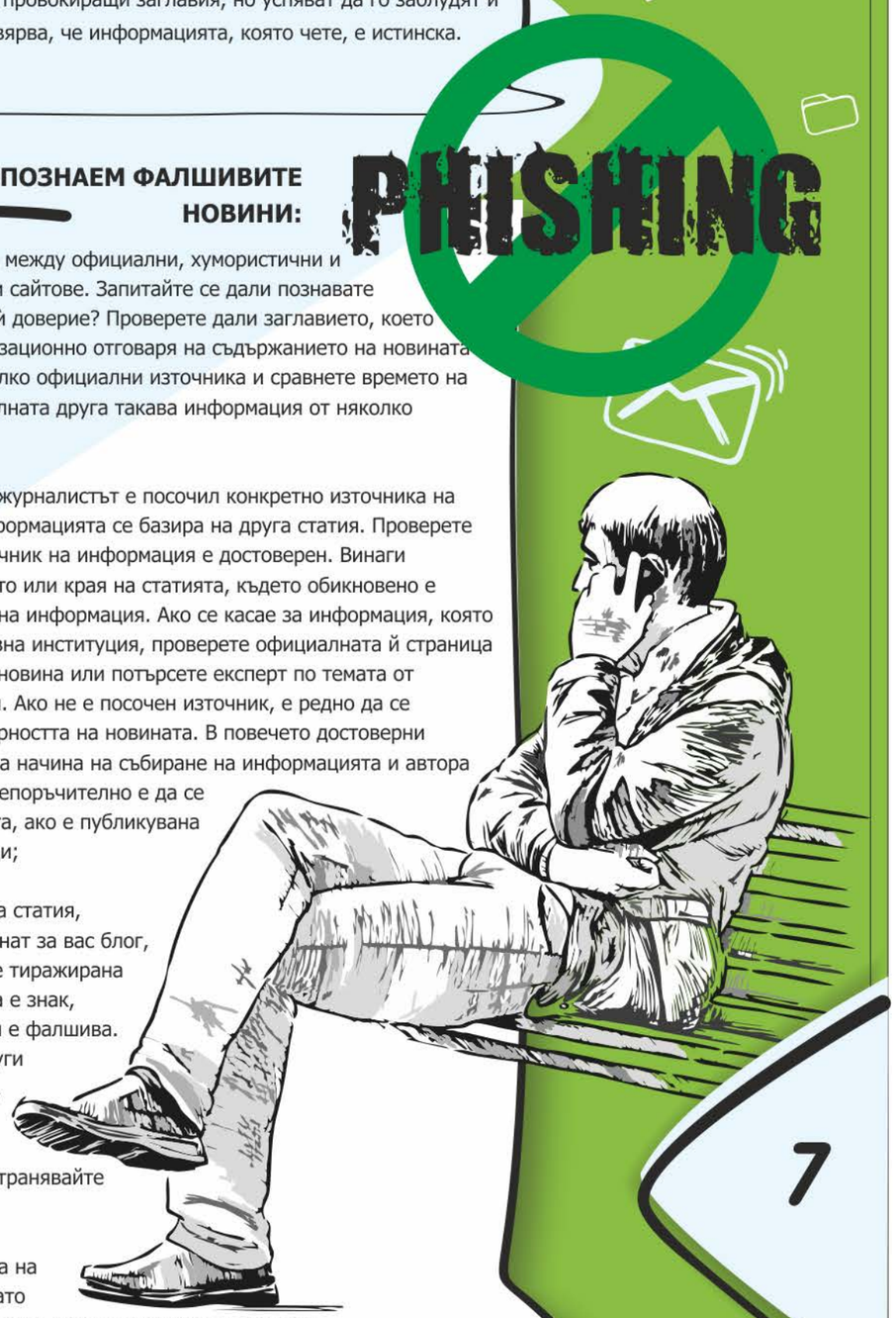
КАК ДА РАЗПОЗНАЕМ ФАЛШИВИТЕ НОВИНИ:

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.



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.

ШЕЙМИНГ – обиди за начина, по който някой изглежда.

Как да постъпим, ако сме притеснени или сме жертва на кибертормоз?

Не се колебайте и реагирайте своевременно!
Може да сигнализирате и да потърсите помощ, консултация или съвет денонощно и безплатно на **Националната телефонна линия за деца 116 111.**
Сигнал за кибертормоз може да подадете и в на отдел „Киберпрестъпност" на ГДБОП **(http://www.cybercrime.bg/bg).**
Може да сигнализирате и на Центъра за безопасен интернет на адрес: www.safenet.bg,
или на техния телефон 124 123,
както и през чат-модула на www.safenet.bg .