
ПАЗИ ДЕТЕТО
В ИНТЕРНЕТ
КАК ДА ЗАЩИТИМ ДЕЦАТА СИ В ДИГИТАЛНИЯ СВЯТ?
ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ
CYBER ONE
Cyber 360
ACADEMY

СЪДЪРЖАНИЕ

ПОЛЕЗНА ИНФОРМАЦИЯ, КОЯТО ЩЕ ОТКРИЕТЕ ТУК

В този наръчник ще получите отговор на въпросите си, свързани с **безопасността на децата в интернет**, под формата на съвети от **експертите на Cyber360 Academy**. Целта на наръчника е да изгради специфични умения у всеки родител, за да може да защити детето си в дигиталното пространство. **Съветите на експертите от Cyber360 Academy в този наръчник обхващат възрастовите групи:**

от 3 до 6 години
от 7 до 10 години
от 11 до 14 години
от 15 до 18 години

ОПАСНОСТИ ЗА ДЕТЕТО В ДИГИТАЛНОТО ПРОСТРАНСТВО

- Технологични
- Социални
- Културни

ТЕХНОЛОГИИ ЗА ЗАЩИТА НА ДЕТЕТО В ДИГИТАЛНОТО ПРОСТРАНСТВО

- Приложения за родителски контрол
- Център по киберсигурност **CyberOne**
- Кибер застраховане **Лев Инс**

ВЪЗРАСТТА НА ДЕЦАТА И СЪВЕТИТЕ НА ЕКСПЕРТИТЕ

Cyber 360 ACADEMY

Децата от 3 до 6 години са много малки и са изложени на рискове в интернет и дигиталното пространство. В тази възраст те обикновено играят на видеоигри или гледат видео и снимки, като най-често използват съдържание, което е предоставено от родителите им. Въпреки че рисковете не са толкова големи, все още има някои **опасности**, които могат да засегнат децата в тази възраст, като:

- **Неподходящо съдържание** (насилие, жестокост, порнография, нецензурен език и др.)
- **Онлайн привличане от странични хора (**чрез онлайн игри, социални мрежи)
- **Вируси и злонамерен софтуер** (при случаен клик върху неподходяща реклама или линк)

Децата на възраст от 7 до 9 години започват да бъдат все по-активни онлайн и да се занимават с различни дигитални дейности, включително онлайн игри с повече играчи, където могат да станат обект на обиди и тормоз. В тази възраст децата започват да проявяват интерес към сексуалността и порнографията. Те може да търсят онлайн информация за теми като сексуално здраве и отношения, но да се сблъскат с неподходящо съдържание.

ЗАТОВА Е ВАЖНО ДЕЦАТА ДА СЕ НАСЪРЧВАТ:

- Да не споделят **лична информация онлайн**
- Да не се свързват с **непознати потребители**

ВЪЗРАСТТА НА ДЕЦАТА

И СЪВЕТИТЕ НА ЕКСПЕРТИТЕ

Децата на възраст между 10 и 12 години са във фазата на развиващо се любопитство и съзнание за социалните мрежи и приложенията за изпращане на съобщения. Те могат да **публикуват лична информация**, която да бъде използвана за нежелани дейности от други хора, ако не знаят как да се защитят в интернет. Неподходящи снимки, видеоклипове или коментари могат да бъдат публикувани на профила на детето без да са осъзнали негативните последствия.

ТЕ МОГАТ ДА СЕ ИЗЛОЖАТ НА РАЗЛИЧНИ ОПАСНОСТИ, КАТО:

- **Неподходяща комуникация с непознати хора**
- **Кибербулинг**
- **Неподходящи за възрастта им съобщения от други потребители**

Във **възрастта от 13 до 15 години** децата търсят **по-активно социални контакти и имат най-силно желание да се приемат от връстниците си.** Това може да ги насочи към участие в онлайн игри и социални мрежи, където да бъдат:

- **Изложени на онлайн тормоз, жестокост и други потенциални опасности**
- **Могат да попаднат на сексуално съдържание**
- **Да публикуват неподходяща информация**

Въпреки че рисковете намаляват във възрастовата група между **16-18 години**, все още има опасности, свързани с онлайн активностите на младите хора. В тази възраст те често споделят лична информация онлайн, като адрес, телефонен номер и друга лична информация, която може да бъде използвана за злоупотреба.

- **Могат да бъдат изложени на онлайн изнудване или сексуална експлоатация**
- **Да станат жертва на онлайн измами или да се присъединят към онлайн групи или общности, които промотират насилие, наркотици и други нежелани поведения.**

ИМЕННО ЗАРАДИ ТЕЗИ РИСКОВЕ Е ВАЖНО РОДИТЕЛИТЕ ДА ПОДДЪРЖАТ ОТВОРЕНА И ЧЕСТА КОМУНИКАЦИЯ С ДЕЦАТА СИ, ДА ГИ НАСЪРЧАВАТ ДА БЪДАТ ВНИМАТЕЛНИ ПРИ СПОДЕЛЯНЕТО НА ЛИЧНА ИНФОРМАЦИЯ И ДА ИМ ПРЕДОСТАВЯТ ЗНАНИЯ И УМЕНИЯ, НЕОБХОДИМИ ЗА БЕЗОПАСНА УПОТРЕБА НА ИНТЕРНЕТ.

ТЕХНОЛОГИЧНИ ОПАСНОСТИ

РАНСЪМУЕР

Ако сте забелязали детето Ви да получава имейли с прикачени файлове, в които има съдържание, подканващо го да отвори тези файлове и имейл **адресът на подателя след кльомбата (@) е напълно непознат**, то това е рансамуер.

Рансъмуерът (ransomware) е вид вреден софтуер, който засича и блокира достъпа до файлове на компютър или мрежа **и изисква от потребителя да заплати определена сума пари (рансом),** за да може да получи отново достъп до тях. Тези програми обикновено криптират файловете на жертвата, с помощта на силна криптография, за да предотвратят достъпа до тях, освен ако не се плати рансомът.

Рансъмуерът може да се **разпространява чрез** надеждни източници като **имейли, социални мрежи, незаконни торенти и други**. За да се предотврати това е важно да наблюдавате какви сайтове посещават децата Ви, какви мейли отварят, какви подскачащи реклами натискат и т.н.

Всички знаем, че в съвременното забързано ежедневие е много трудно човек да съвместява няколко социални роли и постоянно да се адаптира към бързо променящата се среда. Затова препоръките ни са да използвате няколко вида услуги, които могат да предотвратят такъв тип инцидент: това са услуги, предлагани от нашия **център по киберсигурност Cyber One** или още по-надеждно – **кибер застраховането.**

Услугите, които те предлагат, са **специфични филтри на IP адреси и домейн**, което представя възможност за **допълнителна забрана на определени сайтове** по усмотрение на родителя, включително и в социалните мрежи. Също така е добре да поддържате **редовна антивирусна защита** на компютъра, както и да се правят често **резервни копия на важните файлове** и да се избягват съмнителни уебсайтове и имейли. **Към тези услуги „Лев Инс" предлага застрахователни услуги, които осигуряват допълнително финансово покритие при настъпване на инцидент.**

ТЕХНОЛОГИЧНИ ОПАСНОСТИ

ФИШИНГ АТАКИ

Нека разгледаме случка, в която детето има **конзола и акаунт**, с който играе. Той е регистриран **на негово име и с негов имейл**, но за закупуване на играта или разширения за играта е използвана **Вашата кредитна карта**. Детето Ви показва имейл, който е получило от конкретна игра, с искане да се последва посочен линк и да се потвърдят данните на кредитната карта, с която е закупена играта, в противен случай достъпът му ще бъде спрян.

Когато последвате линка, Ви прави впечатление, че **катинарът за сигурност**, който стои в лентата на сайта, **липсва**. Вие го забелязвате и не потвърждавате данните, но едва ли детето Ви ще му обърне внимание.

Тази заплаха е фишинг атака и е най-разпространената форма на измама в интернет. Тя е широко използван похват от компютърни престъпници за получаване на важна информация. Целта им е да подмамят хората, за да предоставят личната си информация, най-вече такава, свързана с подробности по кредитни карти и банкови сметки.

Съветът ни е да не запаметявате данните на кредитната си карта след първото им въвеждане и използване в уеб страницата, защото е възможно отвореният линк да е зловреден и средствата от картата да бъдат откраднати. Бъдете внимателни, когато използвате този метод на плащане в интернет пространството и **обърнете внимание на детето си как да разпознава фишинг атаките** и какво да прави, ако получи фишинг имейл.

ОЩЕ НЯКОИ ПОЛЕЗНИ СЪВЕТИ КАК ДА ПРЕДПАЗИТЕ ДЕТЕТО СИ ОТ ФИШИНГ АТАКИ:

1. ИЗПОЛЗВА ЛЕГАЛНИ, ОБНОВЕНИ ДО ПОСЛЕДНИ ВЕРСИИ ОПЕРАЦИОННИ СИСТЕМИ, АНТИВИРУСНА ЗАЩИТА И БРАУЗЪРИ;
2. ПОДЛАГА ПОД СЪМНЕНИЕ ИМЕЙЛИ ИЛИ САЙТОВЕ, КОИТО ИЗИСКВАТ ЛИЧНА ИНФОРМАЦИЯ ИЛИ ФИНАНСОВА ИНФОРМАЦИЯ;
3. НЕ ПРОСЛЕДЯВА И СЛЕДВА ИНСТРУКЦИИ В ПОДОБНИ НА ПОСОЧЕНИТЕ ИМЕЙЛИ;
4. ПРОВЕРЯВА ИСТИНСКИЯ АДРЕС НА ИЗПРАЩАЧА СПРЯМО ТОЗИ, КОЙТО Е ИЗПИСАН НА ЕКРАНА;
5. ПРОВЕРЯВА ХИПЕРВРЪЗКИТЕ, КЪМ КОИТО ВОДИ ИМЕЙЛЪТ С РЕАЛНИТЕ АДРЕСИ ОТ БРАУЗЪРА;
6. НЕ ЗАПАМЕТЯВА ПОТРЕБИТЕЛСКИ ИМЕНА ИЛИ ПАРОЛИ В БРАУЗЪРИТЕ;
7. ИЗПОЛЗВА РАЗЛИЧНИ ПАРОЛИ ЗА ДОСТЪП ДО РАЗЛИЧНИТЕ АКАУНТИ В ИНТЕРНЕТ.

ПРЕПОРЪЧВАМЕ ВИ СЪЩО ТАКА ДА ИЗПОЛЗВАТЕ УСЛУГИТЕ НА ЦЕНТЪРА ПО КИБЕРСИГУРНОСТ „САЙБЪР УАН" И КИБЕР ЗАСТРАХОВАНЕТО НА „ЛЕВ ИНС".

ТЕХНОЛОГИЧНИ ОПАСНОСТИ

Тъмната мрежа (“Deep Web” и „Dark Web” на английски език) е част от интернет, която не може да бъде достъпна чрез обикновени браузъри като Google Chrome, Firefox и т.н. **Тъй като тъмната мрежа е криптирана и анонимна, това я прави трудна за проследяване**.

Тъмната мрежа е място, където може да се намерят много опасни съдържания, които не са достъпни за обикновените търсачки в интернет. Това включва наркотици, оръжия, уязвимости на компютърни системи, устройства за хакване, незаконни услуги, порно съдържание с деца и т.н. **Една от големите опасности е, че тъмната мрежа може да бъде достъпна само чрез специален софтуер**, който улеснява скриването на идентичността на потребителя.

ДАРК НЕТ

Това прави трудно откриването на престъпления, които се извършват в тъмната мрежа. **За децата опасностите са най-големи, тъй като те лесно могат да бъдат изложени на незаконни съдържания**. Възможно е да се започне общуване с потенциални злоумишленици, да бъде привлечен в терористични групировки и други изключителни опасни за детето влияния.

МОЖЕТЕ ДА ПРЕДПАЗИТЕ ДЕТЕТО СИ ОТ ТЪМНАТА МРЕЖА, КАТО:

1. ГОВОРЕТЕ ПОСТОЯННО С НЕГО ЗА ОПАСНОСТИТЕ В ИНТЕРНЕТ.
2. ИНСТАЛИРАТЕ ДОБРА АНТИВИРУСНА ПРОГРАМА И РОДИТЕЛСКИ КОНТРОЛ В КОМПЮТЪРА, КОЙТО ПОЛЗВА ДЕТЕТО ВИ.
3. ОГРАНИЧЕТЕ ДОСТЪПА ДО КОМПЮТЪРА И ИНТЕРНЕТ - НЕ ПОЗВОЛЯВАЙТЕ НА ДЕТЕТО ВИ ДА ПОЛЗВА КОМПЮТЪР ИЛИ ИНТЕРНЕТ БЕЗ ВАШЕ РАЗРЕШЕНИЕ.
4. СЛЕДЕТЕ КАКВО ПРАВИ ДЕТЕТО ВИ ОНЛАЙН - ПРОВЕРЯВАЙТЕ ИСТОРИЯТА НА НЕГОВИЯ БРАУЗЪР, СОЦИАЛНИТЕ МУ МРЕЖИ И ДРУГИ ПРИЛОЖЕНИЯ.
5. НЕ ПОЗВОЛЯВАЙТЕ НА ДЕТЕТО СИ ДА СПОДЕЛЯ ЛИЧНА ИНФОРМАЦИЯ КАТО ИМЕ, АДРЕС ИЛИ ТЕЛЕФОНЕН НОМЕР НА НЕПОЗНАТИ ХОРА ОНЛАЙН.
6. ГОВОРЕТЕ С ДЕТЕТО СИ ЗА ТОВА КАКВО ДА ПРАВИ, АКО СЛУЧАЙНО СЕ НАТЪКНЕ НА НЕЩО НЕЗАКОННО ИЛИ ОПАСНО ЗА НЕГО ОНЛАЙН.

ИЗПОЛЗВАЙТЕ СЪЩО ТАКА УСЛУГИТЕ НА ЦЕНТЪРА ПО КИБЕРСИГУРНОСТ „САЙБЪР УАН" И КИБЕР ЗАСТРАХОВАНЕТО НА „ЛЕВ ИНС".

СОЦИАЛНИ ОПАСНОСТИ

Кибертормозът е съвкупно понятие за действия, които могат да навредят на даден индивид в интернет и включват **заплахи, злоупотреби, следене или друго агресивно поведение, което е продължително във времето**.

Кибертормозът може да включва обидни реплики, публикуване на снимки в интернет без разрешението на притежателя им, споделяне на видеоклипове, които могат по някакъв начин да накърнят достойнството и доброто име.

ОБИДИ И НАПАДКИ В ИНТЕРНЕТ

Противодействието срещу тази заплаха е особено трудно, тъй като извършителят остава неизвестен, а често използва идентичността на своята жертва и извършва кибертормоз от нейно име. Кибертормозът може да има ***дълбоки последици върху психическото състояние на детето или тийнейджъра***.

НЯКОЛКО СЪВЕТА ОТ НАС:

1. **ОБСЪДЕТЕ С ДЕТЕТО СИ РИСКОВЕТЕ НА ОНЛАЙН ОБЩУВАНЕ - ОБЯСНЕТЕ МУ, ЧЕ В ИНТЕРНЕТ ИМА ХОРА, КОИТО МОГАТ ДА БЪДАТ ГРУБИ. ПООЩРЕТЕ ГО ДА ВИ РАЗКАЗВА ЗА ТАКИВА СЛУЧАИ, ЗА ДА МОЖЕТЕ ДА МУ ПОМОГНЕТЕ.**
2. **НАУЧЕТЕ ДЕТЕТО СИ ДА СЕ ЗАЩИТАВА - ДА НЕ ОТГОВАРЯ НА ГРУБИ КОМЕНТАРИ И ДА НЕ АГРЕСИРА. НАУЧЕТЕ ГО ДА БЛОКИРА ИЛИ ДОКЛАДВА НЕЖЕЛАНИ СЪОБЩЕНИЯ И ДА ИЗТРИВА НЕПОДХОДЯЩИ КОМЕНТАРИ.**
3. **ОГРАНИЧЕТЕ ДОСТЪПА НА ДЕТЕТО СИ ДО СОЦИАЛНИТЕ МРЕЖИ И ВРЕМЕТО, КОЕТО ДЕТЕТО ВИ ПРЕКАРВА ОНЛАЙН И КОНТРОЛИРАЙТЕ СОЦИАЛНИТЕ МРЕЖИ, ДО КОИТО ИМА ДОСТЪП.**
4. **РАЗГОВАРЯЙТЕ С УЧИТЕЛИТЕ НА ДЕТЕТО СИ, АКО ТО ИМА ПРОБЛЕМИ С НЕГАТИВНОТО ПОВЕДЕНИЕ НА СЪУЧЕНИЦИ В СОЦИАЛНИТЕ МРЕЖИ.**
5. **БЪДЕТЕ ПРИМЕР ЗА ДОБРО ОНЛАЙН ПОВЕДЕНИЕ - ПОКАЖЕТЕ НА ДЕТЕТО СИ ДОБРИЯ ПРИМЕР В СВОЯ ОНЛАЙН ЖИВОТ, КАТО СЕ ОТНАСЯТЕ С УВАЖЕНИЕ КЪМ ДРУГИТЕ ХОРА И НЕ ПОЗВОЛЯВАТЕ НА ОНЛАЙН ОБЩУВАНЕТО ДА СЕ ПРЕВРЪЩА В КОНФЛИКТ.**

АКО НЯМАТЕ ВЪЗМОЖНОСТТА ДА ГО ПРАВИТЕ ВСЕКИ ДЕН, ИЗПОЛЗВАЙТЕ ПРОДУКТИТЕ НА CYBERONE И „ЛЕВ ИНС".

Ако имате някакви съмнения за негативни събития в интернет, свържете се с органите на реда.

Важно е да бъдете внимателни и да следите онлайн дейностите на детето си.

СОЦИАЛНИ ОПАСНОСТИ

За всички е ясно, че **социалните мрежи са най-разпространените места, където тийнейджърите споделят всичко** – от баналните неща като времето навън, до потенциално опасни като точното си местонахождение. Именно това е едно от местата, където децата ни срещат нови виртуални „приятели“.

ЗАПОЗНАНСТВА С НЕПОЗНАТИ В ИНТЕРНЕТ

Cyber 360
ACADEMY

Опасността тук произтича от неспазването на определени правила, като например да не се споделя незабавно лична информация. Липсва уверение, че насрещната страна е такава, за каквото се представя.

ТЪЙ КАТО НЕ МОЖЕ ДА ЗАБРАНИТЕ ДОСТЪПА НА ДЕТЕТО ДО ВСИЧКИ СОЦИАЛНИ МРЕЖИ И САЙТОВЕ, Е ВАЖНО ДА:

1. **ПОГОВОРИТЕ С НЕГО И ДА ГО ПРЕДУПРЕДИТЕ, ЧЕ РАЗГОВОРИТЕ С НЕПОЗНАТИ В МРЕЖАТА СА МНОГО ОПАСНИ**
2. **ДА МУ РАЗКАЖЕТЕ КАКВИ МОГАТ ДА БЪДАТ ПОСЛЕДСТВИЯТА ОТ ПОДОБНИ РАЗГОВОРИ**

Често обаче децата не искат да разговарят и споделят с родителите си, особено тези, които са в тийнейджърска възраст.

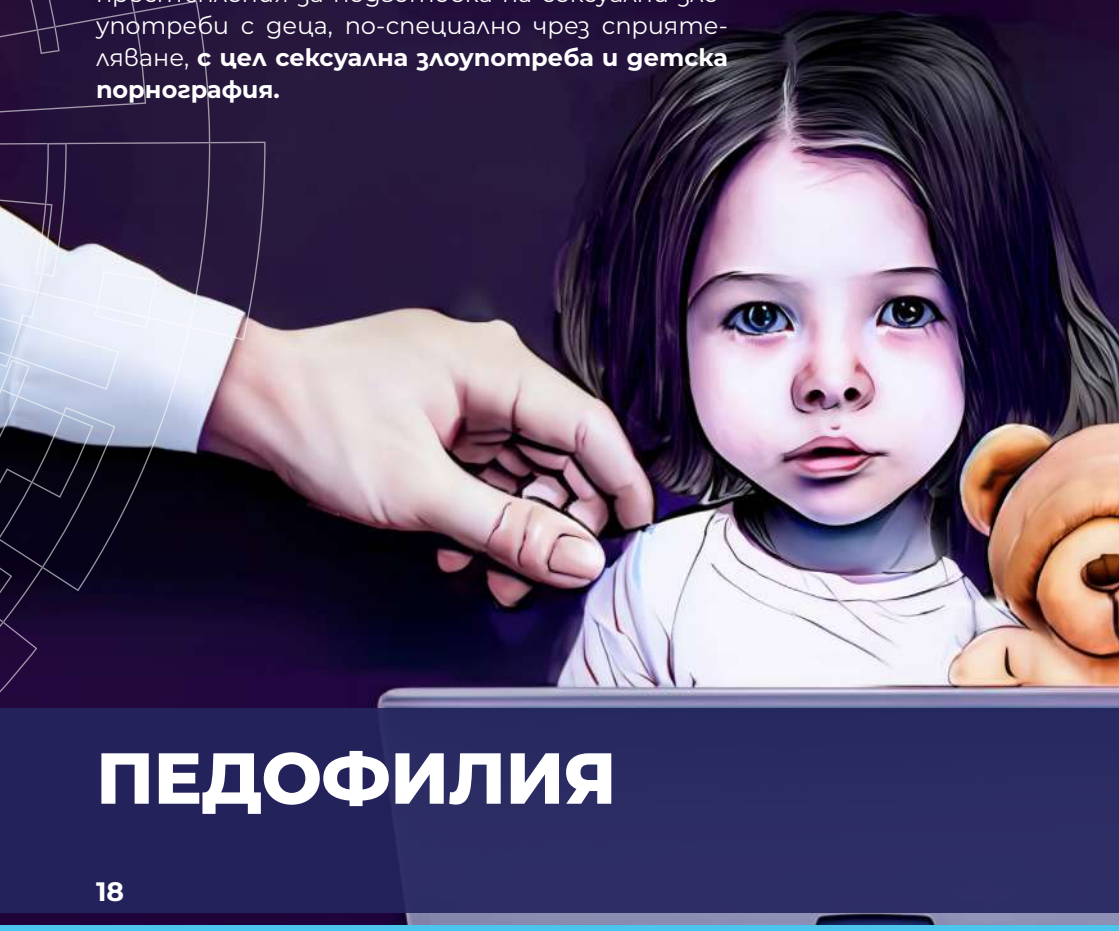
Затова препоръчваме да използвате услугите на Центъра по киберсигурност CyberOne и кибер застраховането на „Лев Инс".

СОЦИАЛНИ ОПАСНОСТИ

Нека поговорим и за най-големите страхове на един родител – **педофилията и порнографското съдържание в интернет.**

КАК ДА ПРЕДПАЗИТЕ ДЕТЕТО СИ ОТ ТЯХ?

Интернет все по-често се използва от потенциални и реални извършители на сексуални престъпления за подготовка на сексуални злоупотреби с деца, по-специално чрез сприятеляване, **с цел сексуална злоупотреба и детска порнография.**

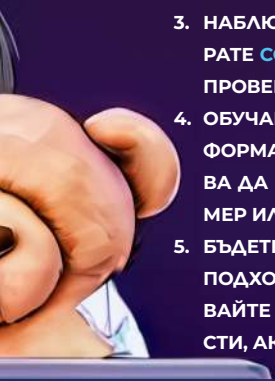


ПЕДОФИЛИЯ

Младите хора могат да станат жертва на т.нар. сексуални хищници, които в днешно време се насочват към социалните мрежи и примамват младежи, демонстрирайки привиден интерес към техните хобита, любими изпълнители, предавания и пр. Така например педофили лесно могат да се доберат до лична информация - адрес, имена, профили, след което изпращат изображения и видео, които имат сексуално съдържание. **Освен пряката негативна въздействие върху психиката и развитието на младите хора**, сайтове с порнографско съдържание, **често крият зловреден софтуер, който атакува компютрите при разглеждането им.**

НАШИТЕ СЪВЕТИ КЪМ ВАС СА:

1. РАЗГОВАРЯЙТЕ ОТКРИТО И ЧЕСТО С ВАШЕТО ДЕТЕ. ОБЯСНЕТЕ МУ ЗА ОПАСНОСТИТЕ НА ИНТЕРНЕТ И КАТО РОДИТЕЛ ТРЯБВА ДА СЪЗДАДЕТЕ ОТКРИТА КОМУНИКАЦИЯ С НЕГО, ЗА ДА МОЖЕТЕ ДА ОТГОВОРИТЕ НА ВЪПРОСИТЕ МУ И ДА РАЗБЕРЕТЕ КАКВИ СА НЕГОВИТЕ НУЖДИ И ПРИТЕСНЕНИЯ.
2. ОГРАНИЧЕТЕ ДОСТЪПА НА ДЕТЕТО СИ ДО ИНТЕРНЕТ. МОЖЕТЕ ДА СЕ ОБЪРНЕТЕ КЪМ УСЛУГИТЕ, КОИТО ПРЕДЛАГА „САЙБЪР УАН" ЗА ИНСТАЛИРАНЕ НА ФИЛТРИ ЗА СЪДЪРЖАНИЕ, КОИТО ДА ОГРАНИЧАТ ДОСТЪПА МУ ДО ПОРНОГРАФИЯ И ДРУГИ НЕЖЕЛАНИ САЙТОВЕ.
3. НАБЛЮДАВАЙТЕ АКТИВНО ОНЛАЙН ДЕЙНОСТТА МУ. МОЖЕТЕ ДА ИНСТАЛИРАТЕ СОФТУЕР ЗА НАБЛЮДЕНИЕ НА НЕГОВОТО И ВАШЕТО УСТРОЙСТВО, ЗА ДА ПРОВЕРЯВАТЕ РЕДОВНО ТЯХНАТА ОНЛАЙН ДЕЙНОСТ.
4. ОБУЧАВАЙТЕ ДЕТЕТО СИ ДА БЪДЕ ВНИМАТЕЛНО И ДА НЕ СПОДЕЛЯ ЛИЧНА ИНФОРМАЦИЯ ОНЛАЙН В НАШАТА АКАДЕМИЯ CYBER 360. ЗНАНИЕТО, ЧЕ НЕ ТРЯБВА ДА РАЗГЛАСЯВА ЛИЧНА ИНФОРМАЦИЯ, КАТО ИМЕ, АДРЕС, ТЕЛЕФОНЕН НОМЕР ИЛИ ДРУГИ ЛИЧНИ ДАННИ, МОЖЕ ДА НАМАЛИ РИСКА ОТ ОПАСНОСТИ.
5. БЪДЕТЕ БДИТЕЛНИ И БЪДЕТЕ ГОТОВИ ДА ДЕЙСТВАТЕ, АКО ОТКРИЕТЕ НЕЩО НЕПОДХОДЯЩО ИЛИ НЕОБИЧАЙНО В ПОВЕДЕНИЕТО НА ДЕТЕТО СИ. НЕ СЕ СТРАХУВАЙТЕ ДА ГОВОРИТЕ С НЕГО ИЛИ ДА ПОТЪРСИТЕ ПОМОЩ ОТ ПРОФЕСИОНАЛИСТИ, АКО СМЯТАТЕ, ЧЕ Е НЕОБХОДИМО.



Важно е да помните, че интернет може да бъде мощен инструмент за образование и развлечение, но е от изключително значение да се знае как да го използваме безопасно и отговорно.

КУЛТУРНИ ОПАСНОСТИ

Много актуално в момента е да се говори за фалшивите новини или т.нар. **Fake news.** Знаем за сайтове, пълни с фалшиви новини, чиято единствена цел е да **събират посещения и да ни подмамват с реклами.** Такива сайтове привличат **вниманието на детето.** То ги посещава, за да се информира. **Получава се обаче обратното, защото съдържанието на тези сайтове е коренно различно от реалността.**

ФАЛШИВИ НОВИНИ

Те се разпространяват в голям мащаб чрез социални медии, таблоидни издания и други медии в интернет пространството. Целта на тези новини е да подмамят и манипулират читателите, като те се използват, за да получат посещения на уеб сайтове. Фалшивите новини са често много убедителни и трудни за разпознаване. Те съдържат заглавия и текстове, които са добре написани и звучат убедително. Също така се използват снимки или видеоклипове, които са манипулирани, за да подкрепят лъжите.

Посланията на фалшивите новини могат да бъдат насочени и към децата и да имат сериозни последици в обществото, тъй като те могат да **повлияят на мненията и действията им.** Характерна черта за фалшивите новини е създаването и лавинообразното им разпространение в интернет. Потребителите рядко проверяват достоверността на информацията, която се разпространява в онлайн пространството.

Друга интересна особеност е характерът на фалшивите новини. Почти всички са с негативно послание и стресиращи факти по актуални теми и проблеми от ежедневието.

Родителите и учителите могат да помогнат на децата да разберат тези принципи и да развият критичното мислене, което е важно за разбирането на новините и информацията, която те четат и получават в социалните мрежи и интернет изобщо. Съществуват програми, с помощта на които може да се провери дали новините са фалшиви.

Тези програми за проверка на данните, наричани също факт-чекинг или факт-проверкинг, **представляват процес на проверка на информация, който се използва за определяне на това дали дадена новина** или твърдение са точни и базирани на факти. Програмите за проверка на данните се използват, както от организации, за да се гарантира, че информацията, която се публикува е базирана на факти и е точна, така и от физически лица, които имат възможността за ръчна проверка на точността на определена информация в интернет.

КУЛТУРНИ ОПАСНОСТИ

Съществуват и други методи и инструменти за справяне с фалшивите новини.

През последните няколко години „популярността“ на фалшивите новини е все по-голяма. Google, Facebook и други големи корпорации инвестират милиони в разработки за улавяне на фалшивите новини. Инструменти за това са специални платформи, които автоматично проверяват и отсяват информацията.

ТАКИВА САЙТОВЕ, В КОИТО МОЖЕТЕ ДА ПРОВЕРИТЕ ДОСТОВЕРНОСТТА НА ИНФОРМАЦИЯТА, КОЯТО ДЕТЕТО ВИ И ВИЕ ЧЕТЕТЕ, СА:

1. Facktcheck.bg
2. BNR , Проверка на факти
3. Reuters
4. BBC

Друг от инструментите за защита от фалшиви новини е изграждане на черен списък с IP адреси на зловредни сайтове по Ваш избор, както и списък, селектиран от специалистите по киберсигуност на Cyber One.

Тези функционалности се представят от центъра по киберсигурност CyberOne и кибер застраховките на „Лев Инс”.

ЗА ДА НАПРАВЯТ ДЕЦАТА РАЗЛИКА МЕЖДУ ФАЛШИВИТЕ И ИСТИНСКИТЕ НОВИНИ, Е ВАЖНО ДА СЕ НАУЧАТ ДА:

1. ПРОВЕРЯВАТ ИЗТОЧНИЦИТЕ, КОИТО ИЗПОЛЗВАТ - ДАЛИ САЙТЪТ И АВТОРЪТ ИМ Е ПОЗНАТ. АКО НЕ МОЖЕ ДА СЕ ПОТВЪРДИ ИЗТОЧНИКЪТ, Е ПО-ДОБРЕ ДА НЕ СПОДЕЛЯ НОВИНАТА.
2. ПРОВЕРЯВАТ ПОВЕЧЕ ОТ ЕДИН ИЗТОЧНИК – ПРОВЕРКА НА НОВИНАТА В РАЗЛИЧНИ МЕДИИ, ЗА ДА СЕ ПОТВЪРДИ, ЧЕ Е ИСТИНСКА И ТОЧНА.
3. ПРОВЕРЯВАТ ФАКТИТЕ - АКО НОВИНАТА СЪДЪРЖА УТВЪРЖДЕНИЯ ИЛИ ФАКТИ, ДА СЕ ПРОВЕРИ ДАЛИ СА ВЕРНИ.
4. БЪДАТ ВНИМАТЕЛНИ СЪС ЗАГЛАВИЯТА - ЗАГЛАВИЯТА МОГАТ ДА БЪДАТ МАНИПУЛИРАНИ, ЗА ДА ИЗГЛЕЖДАТ ПО-ШОКИРАЩИ ИЛИ ИНТЕРЕСНИ, ОТКОЛКОТО РЕАЛНО СА.
5. РАЗБЕРАТ КОЙ ПЕЧЕЛИ ОТ НОВИНАТА - МНОГО ФАЛШИВИ НОВИНИ СЕ ПУБЛИКУВАТ ОТ САЙТОВЕ, КОИТО ИМАТ ФИНАНСОВ ИНТЕРЕС В ПРИВЛИЧАНЕТО НА ПОСЕЩЕНИЯ НА САЙТА.
6. СПОДЕЛЯТ САМО ПРОВЕРЕНИ НОВИНИ - АКО НЕ СА СИГУРНИ ЗА НОВИНАТА, ДА НЕ Я СПОДЕЛЯТ В ПРОФИЛА СИ В СОЦИАЛНИТЕ МРЕЖИ.

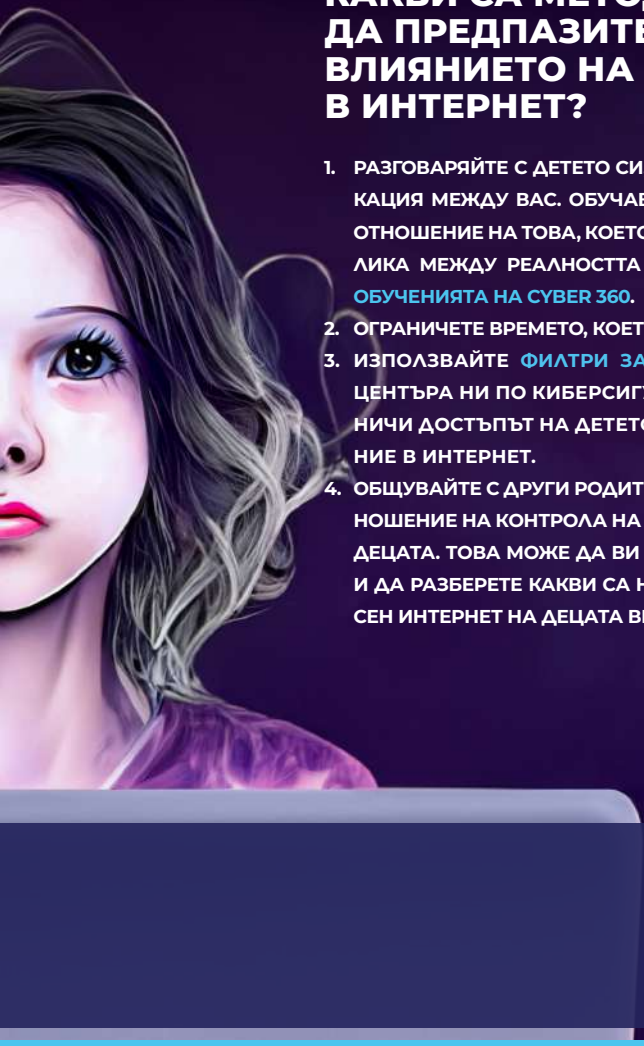
КУЛТУРНИ ОПАСНОСТИ

Инфлуенсърите могат да имат голямо влияние върху нашите деца, особено ако те са почитатели на тези личности. Те могат да оказват натиск върху децата да следват техния пример или да копират техния начин на живот, което може да доведе до нежелани последици.

Една от основните опасности е **влиянието на инфлуенсърите върху самочувствието на децата.** Ако те непрекъснато сравняват себе си с „перфектния“ начин на живот на инфлуенсъра, може да се **почувстват непривлекателни.** Това може да доведе до проблеми като ниско самочувствие, депресия, тревожност и други.

Освен това, инфлуенсърите могат да оказват влияние върху стандартите на децата за красота, мода и стил на живот. Те могат да насърчават или потискат консуматорството на определени храни, както и да оказват натиск върху децата за закупуването на определени продукти и марки, които може да не са подходящи за нуждите или възрастовата им група. Това може да доведе до финансови проблеми и прекомерна консумация.

ИНФЛУЕНСЪРИ



КАКВИ СА МЕТОДИТЕ, ЧРЕЗ КОИТО ДА ПРЕДПАЗИТЕ ДЕТЕТО СИ ОТ ВЛИЯНИЕТО НА ИНФЛУЕНСЪРИТЕ В ИНТЕРНЕТ?

1. РАЗГОВАРЯЙТЕ С ДЕТЕТО СИ, ЗА ДА СЕ УСТАНОВИ ЯСНА КОМУНИКАЦИЯ МЕЖДУ ВАС. ОБУЧАВАЙТЕ ГО ГО ДА БЪДЕ КРИТИЧНО ПО ОТНОШЕНИЕ НА ТОВА, КОЕТО ГЛЕДА В ИНТЕРНЕТ И ДА ПРАВИ РАЗЛИКА МЕЖДУ РЕАЛНОСТТА И ДИГИТАЛНОТО ПРОСТРАНСТВО С ОБУЧЕНИЯТА НА CYBER 360.
2. ОГРАНИЧЕТЕ ВРЕМЕТО, КОЕТО ДЕТЕТО ВИ ПРЕКАРВА В ИНТЕРНЕТ.
3. ИЗПОЛЗВАЙТЕ ФИЛТРИ ЗА СЪДЪРЖАНИЕ, КОИТО ПРЕДЛАГА ЦЕНТЪРА НИ ПО КИБЕРСИГУРНОСТ CYBER ONE, ЗА ДА СЕ ОГРАНИЧИ ДОСТЪПЪТ НА ДЕТЕТО ВИ ДО НЕПОДХОДЯЩО СЪДЪРЖАНИЕ В ИНТЕРНЕТ.
4. ОБЩУВАЙТЕ С ДРУГИ РОДИТЕЛИ И СПОДЕЛЯЙТЕ ОПИТА СИ ПО ОТНОШЕНИЕ НА КОНТРОЛА НА МЕДИИТЕ И СОЦИАЛНИТЕ МРЕЖИ НА ДЕЦАТА. ТОВА МОЖЕ ДА ВИ ПОМОГНЕ ДА ПОЛУЧИТЕ НОВИ ИДЕИ И ДА РАЗБЕРЕТЕ КАКВИ СА НАЙ-ДОБРИТЕ ПРАКТИКИ ЗА БЕЗОПАСЕН ИНТЕРНЕТ НА ДЕЦАТА ВИ.

КУЛТУРНИ ОПАСНОСТИ

В днешно време децата ни могат да избират сред хиляди онлайн или видео игри в зависимост от интересите си. **Едни от най-популярните игри са виртуалните светове,** в които детето си създава аватар, печели някаква виртуална валута и/или изпълнява мисии. **Обикновено в тези игри присъства някакъв елемент на социална мрежа, а в много от тях има и насилие.**

ЧАТЪТ И КОМУНИКАЦИЯТА В ОНЛАЙН ИГРИ

Комуникацията във видео игрите може да бъде предизвикателство, тъй като играчите имат възможност да комуникират по време на играта чрез чат, гласова комуникация или дори видеоконференции. Това може да представлява опасност за децата, особено ако комуникацията се осъществява с непознати хора.

Докато детето Ви играе, може би сте виждали да изскачат реклами. В някои от игрите те са доста натрапчиви. Възможно ли е те да го подтикват към някаква друга опасност?

Рекламите в игрите могат да бъдат натрапчиви, но обикновено те не представляват опасност за детето Ви, освен ако не се кликне върху тях.Все пак, има някои рискове, свързани с рекламите в игрите, които може да бъдат потенциално вредни за детето Ви.

ВИДЕО И ОНЛАЙН ИГРИ

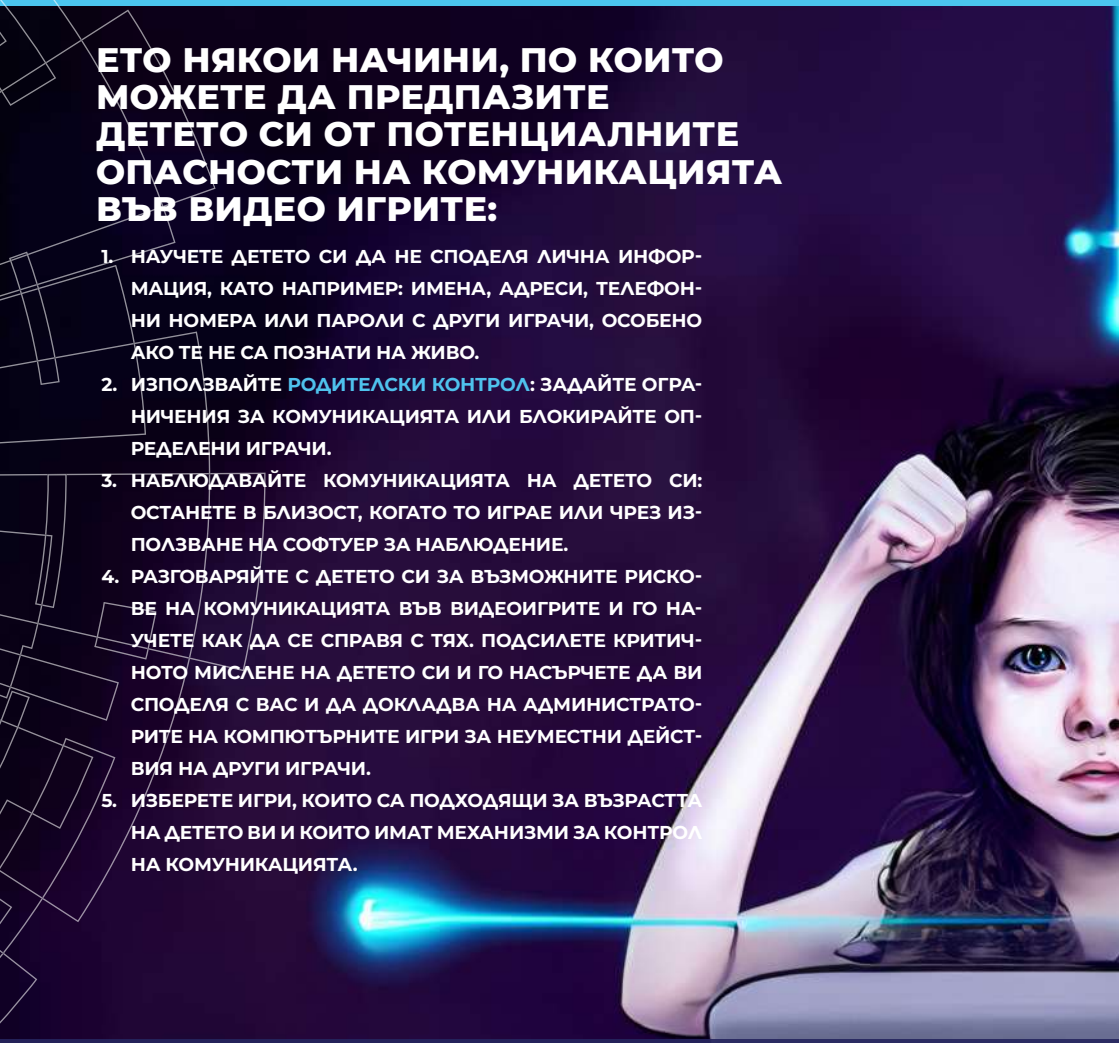
КАКВИ ОПАСНОСТИ И РИСКОВЕ КРИЕ ТОВА ЗА ДЕЦАТА НИ?

1. ОНЛАЙН ИЗМАМИ: ВИДЕО ИГРИТЕ МОГАТ ДА БЪДАТ ПОЛЕ ЗА ОНЛАЙН ИЗМАМИ, КАТО НАПРИМЕР ИЗМАМИ С ФАЛШИВИ АКАУНТИ ИЛИ ВИРТУАЛНИ ПРЕДМЕТИ. ДЕЦАТА МОГАТ ДА СЕ ОКАЖАТ ЖЕРТВА НА ИЗМАМА, ДА БЪДАТ ПОДТИКНАТИ ОТ АНОНИМНИ УЧАСТНИЦИ В ИГРАТА ДА ПРОДАВАТ РЕАЛНИ ПАРИ ЗА ВИРТУАЛНИ ВАЛУТИ ИЛИ ПРЕДМЕТИ, КОИТО НИКОГА НЕ ПОЛУЧАВАТ.
2. ЗЛОУПОТРЕБА С ЛИЧНА ИНФОРМАЦИЯ: АНОНИМНИ ЗЛОУМИШЛЕНИ ИГРАЧИ МОГАТ ДА ИЗИСКВАТ ОТ ДЕЦАТА ДА ПРЕДОСТАВЯТ ЛИЧНА ИНФОРМАЦИЯ (ИМЕНА, АДРЕСИ, ТЕЛЕФОННИ НОМЕРА И ДР.). ТАЗИ ИНФОРМАЦИЯ МОЖЕ ДА БЪДЕ ИЗПОЛЗВАНА ОТ ТЯХ, ЗА ДА МАМЯТ ИЛИ ДА ЗЛОУПОТРЕБЯТ С ДЕТЕТО.
3. НАСИЛИЕ: МНОГО ВИДЕО ИГРИ ВКЛЮЧВАТ ЕЛЕМЕНТИ НА НАСИЛИЕ, КАТО БИТКИ, СРАЖЕНИЯ ИЛИ ОРЪЖИЯ. ТОВА МОЖЕ ДА НАСЪРЧИ ДЕЦАТА ДА ПРИЕМАТ НАСИЛИЕТО КАТО НОРМАЛНА ЧАСТ ОТ ЖИВОТА.
4. ЗАВИСИМОСТ: ВИДЕО ИГРИТЕ МОГАТ ДА БЪДАТ МНОГО ЗАБАВНИ И УВЛЕКАТЕЛНИ ЗА ДЕЦАТА, НО МОГАТ ДА ДОВЕДАТ ДО ЗАВИСИМОСТ КЪМ ТЯХ, КАКТО И КЪМ КОМПЮТЪРА. ТОВА МОЖЕ ДА НАВРЕДИ НА СОЦИАЛНИТЕ И АКАДЕМИЧНИ УМЕНИЯ НА ДЕЦАТА.
5. НЕСЪОТВЕТСТВИЕ С ВЪЗРАСТТА: МНОГО ВИРТУАЛНИ СВЕТОВЕ МОГАТ ДА ИМАТ НЕСЪОТВЕТСТВАЩО С ВЪЗРАСТТА НА ДЕТЕТО СЪДЪРЖАНИЕ (НАСИЛИЕ, СЕКСУАЛНИ СЦЕНИ ИЛИ ОБИДНИ ДУМИ).

КУЛТУРНИ ОПАСНОСТИ

ЕТО НЯКОИ НАЧИНИ, ПО КОИТО МОЖЕТЕ ДА ПРЕДПАЗИТЕ ДЕТЕТО СИ ОТ ПОТЕНЦИАЛНИТЕ ОПАСНОСТИ НА КОМУНИКАЦИЯТА ВЪВ ВИДЕО ИГРИТЕ:

1. НАУЧЕТЕ ДЕТЕТО СИ ДА НЕ СПОДЕЛЯ ЛИЧНА ИНФОРМАЦИЯ, КАТО НАПРИМЕР: ИМЕНА, АДРЕСИ, ТЕЛЕФОННИ НОМЕРА ИЛИ ПАРОЛИ С ДРУГИ ИГРАЧИ, ОСОБЕНО АКО ТЕ НЕ СА ПОЗНАТИ НА ЖИВО.
2. ИЗПОЛЗВАЙТЕ **РОДИТЕЛСКИ КОНТРОЛ**: ЗАДАЙТЕ ОГРАНИЧЕНИЯ ЗА КОМУНИКАЦИЯТА ИЛИ БЛОКИРАЙТЕ ОПРЕДЕЛЕНИ ИГРАЧИ.
3. НАБЛЮДАВАЙТЕ КОМУНИКАЦИЯТА НА ДЕТЕТО СИ: ОСТАНЕТЕ В БЛИЗОСТ, КОГАТО ТО ИГРАЕ ИЛИ ЧРЕЗ ИЗПОЛЗВАНЕ НА СОФТУЕР ЗА НАБЛЮДЕНИЕ.
4. РАЗГОВАРЯЙТЕ С ДЕТЕТО СИ ЗА ВЪЗМОЖНИТЕ РИСКОВЕ НА КОМУНИКАЦИЯТА ВЪВ ВИДЕОИГРИТЕ И ГО НАУЧЕТЕ КАК ДА СЕ СПРАВЯ С ТЯХ. ПОДСИЛЕТЕ КРИТИЧНОТО МИСЛЕНЕ НА ДЕТЕТО СИ И ГО НАСЪРЧЕТЕ ДА ВИ СПОДЕЛЯ С ВАС И ДА ДОКЛАДВА НА АДМИНИСТРАТОРИТЕ НА КОМПЮТЪРНИТЕ ИГРИ ЗА НЕУМЕСТНИ ДЕЙСТВИЯ НА ДРУГИ ИГРАЧИ.
5. ИЗБЕРЕТЕ ИГРИ, КОИТО СА ПОДХОДЯЩИ ЗА ВЪЗРАСТТА НА ДЕТЕТО ВИ И КОИТО ИМАТ МЕХАНИЗМИ ЗА КОНТРОЛ НА КОМУНИКАЦИЯТА.



ВИДЕО И ОНЛАЙН ИГРИ

ЕТО НЯКОИ ОТ ТЕЗИ РИСКОВЕ:

1. **РЕКЛАМИТЕ В ИГРИТЕ МОГАТ ДА НАСЪРЧАВАТ ДЕТЕТО ВИ ДА КОНСУМИРА/ИЗПОЛЗВА ОПРЕДЕЛЕНИ ПРОДУКТИ ИЛИ УСЛУГИ.**
2. **НЯКОИ РЕКЛАМИ МОГАТ ДА НАСЪРЧАВАТ КЪМ ПОСТИГАНЕ НА НЕРЕАЛИСТИЧНИ ИДЕАЛИ, КАТО НАПРИМЕР ПЕРФЕКТНО ТЯЛО ИЛИ УСПЕХ В ЖИВОТА, КОЕТО МОЖЕ ДА ДОВЕДЕ ДО СТРЕС И НЕУВЕРЕНОСТ.**
3. **РЕКЛАМИТЕ В ИГРИТЕ МОГАТ ДА НАСЪРЧАВАТ ДЕТЕТО ВИ ДА ИГРАЕ ПОВЕЧЕ И ДА СЕ ВКЛЮЧВА В ИГРАЛНИ ДЕЙНОСТИ, КОИТО МОГАТ ДА ДОВЕДАТ ДО ЗАВИСИМОСТ.**
4. **РЕКЛАМИТЕ В ИГРИТЕ МОГАТ ДА ИЗЛАГАТ ДЕТЕТО НА ВРЕДНИ СЪДЪРЖАНИЯ, КАТО НАСИЛИЕ ИЛИ СЕКСУАЛНИ ОБРАЗИ, КОЕТО МОЖЕ ДА ИМА НЕГАТИВНО ВЪЗДЕЙСТВИЕ ВЪРХУ ПСИХОЛОГИЧЕСКОТО ЗДРАВЕ.**

Именно заради тези рискове е важно да наблюдавате рекламите, които се появяват по време на играта на Вашето дете и да говорите с него за тях.

Ако нямате възможност да контролирате детето си през цялото време, то може да използва услугите на центъра по киберсигурност CyberOne и кибер застрахователните услуги на „Лев Инс".

Те могат да предложат едно още по-ефективно решение, а именно – защита от зловредни реклами. Тяхната функционалност е да блокират нежелани реклами, като по този начин децата няма да бъдат подведени и да натискат върху тях.

КУЛТУРНИ ОПАСНОСТИ

ВИДЕО И ОНЛАЙН ИГРИ

ПОП ЪП КАРТИНКИ (ПАДАЩИ КАРТИНКИ)

Докато детето Ви играе, може би сте виждали да изскачат реклами. В някои от игрите те са доста натрапчиви. Възможно ли е те да го подтикват към някаква друга опасност?

Рекламите в игрите могат да бъдат натрапчиви, но обикновено те не представляват опасност за детето Ви, освен ако не се кликне върху тях.

Все пак, има някои рискове, свързани с рекламите в игрите, които може да бъдат потенциално вредни за детето Ви.

ЕТО НЯКОИ ОТ ТЕЗИ РИСКОВЕ:

1. **РЕКЛАМИТЕ В ИГРИТЕ МОГАТ ДА НАСЪРЧАВАТ ДЕТЕТО ВИ ДА КОНСУМИРА/ИЗПОЛЗВА ОПРЕДЕЛЕНИ ПРОДУКТИ ИЛИ УСЛУГИ.**
2. **НЯКОИ РЕКЛАМИ МОГАТ ДА НАСЪРЧАВАТ КЪМ ПОСТИГАНЕ НА НЕРЕАЛИСТИЧНИ ИДЕАЛИ, КАТО НАПРИМЕР ПЕРФЕКТНО ТЯЛО ИЛИ УСПЕХ В ЖИВОТА, КОЕТО МОЖЕ ДА ДОВЕДЕ ДО СТРЕС И НЕУВЕРЕНОСТ.**
3. **РЕКЛАМИТЕ В ИГРИТЕ МОГАТ ДА НАСЪРЧАВАТ ДЕТЕТО ВИ ДА ИГРАЕ ПОВЕЧЕ И ДА СЕ ВКЛЮЧВА В ИГРАЛНИ ДЕЙНОСТИ, КОИТО МОГАТ ДА ДОВЕДАТ ДО ЗАВИСИМОСТ.**
4. **РЕКЛАМИТЕ В ИГРИТЕ МОГАТ ДА ИЗЛАГАТ ДЕТЕТО НА ВРЕДНИ СЪДЪРЖАНИЯ, КАТО НАСИЛИЕ ИЛИ СЕКСУАЛНИ ОБРАЗИ, КОЕТО МОЖЕ ДА ИМА НЕГАТИВНО ВЪЗДЕЙСТВИЕ ВЪРХУ ПСИХОЛОГИЧЕСКОТО ЗДРАВЕ.**

ИМЕННО ЗАРАДИ ТЕЗИ РИСКОВЕ Е ВАЖНО ДА НАБЛЮДАВАТЕ РЕКЛАМИТЕ, КОИТО СЕ ПОЯВЯВАТ ПО ВРЕМЕ НА ИГРАТА НА ВАШЕТО ДЕТЕ И ДА ГОВОРИТЕ С НЕГО ЗА ТЯХ.

Ако нямате възможност да контролирате детето си през цялото време, то може да използва услугите на центъра по киберсигурност **CyberOne** *и кибер застрахователните услуги на* **„Лев Инс”.** *Те могат да предложат едно още по-ефективно решение, а именно – защита от зловредни реклами. Тяхната функционалност е да блокират нежелани реклами, като по този начин децата няма да бъдат подведени и да натискат върху тях.*

ТЕХНОЛОГИИ ЗА ЗАЩИТА НА ДЕТЕТО В ДИГИТАЛНОТО ПРОСТРАНСТВО

ПРИЛОЖЕНИЯ ЗА РОДИТЕЛСКИ КОНТРОЛ

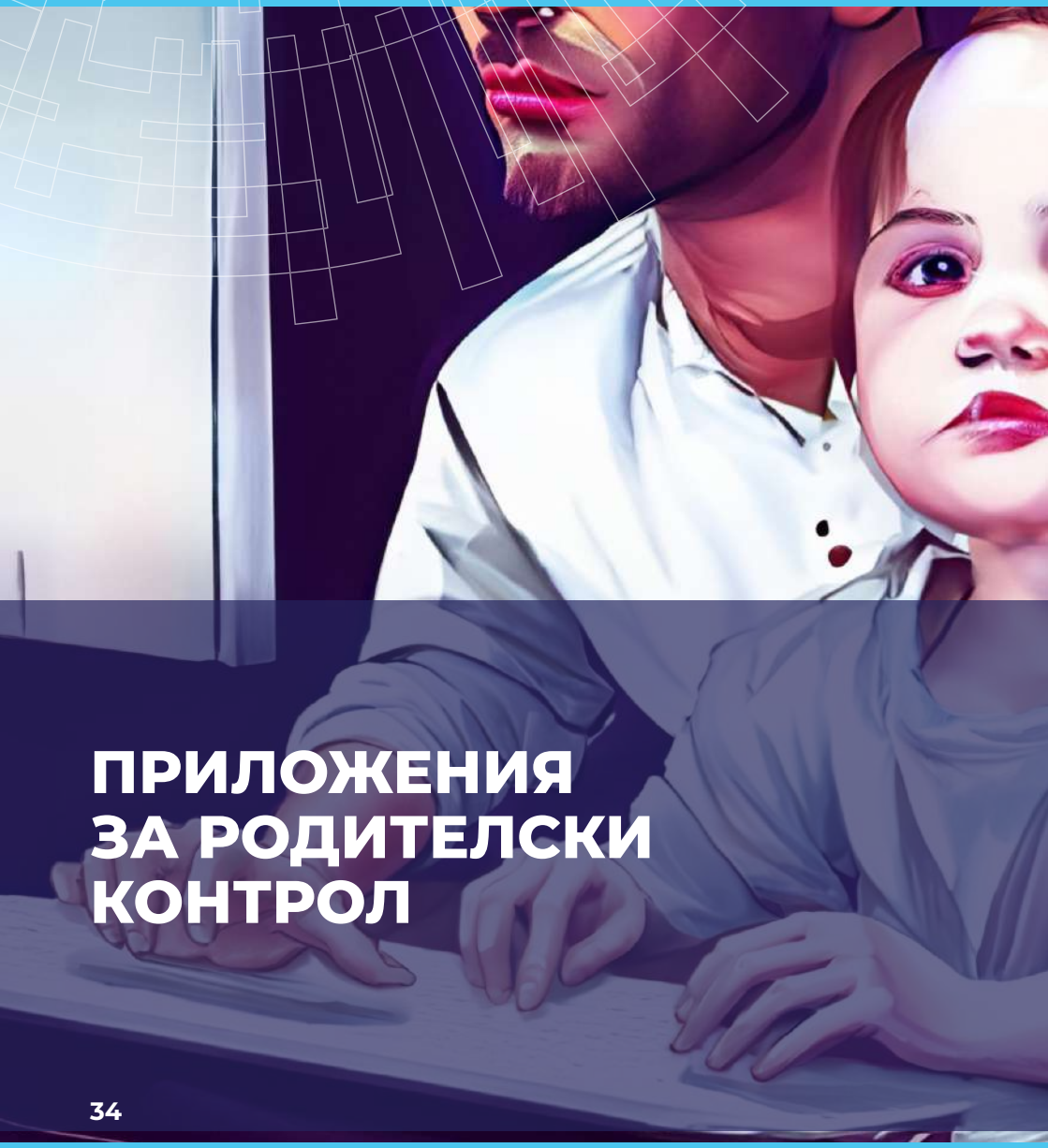
Приложенията за **родителски контрол са софтуерни инструменти, които позволяват на родителите да контролират и ограничават достъпа на техните деца до определени уеб сайтове, игри и други онлайн ресурси.** Те са предназначени да помогнат на родителите да защитят децата си от нежелани контакти, онлайн измамници, порнография и други.

Тези приложения обикновено предлагат функции като блокиране на уеб сайтове, филтриране на съдържанието, ограничаване на времето, което децата могат да прекарват на компютъра или мобилното устройство, следене на активността на децата в интернет и уведомяване на родителите, когато децата им се опитват да достъпят забранени сайтове или приложения.

Такива приложения са полезни инструменти за контрол върху дигиталното съдържание до което да имат достъп децата, но не могат да заменят активното наблюдение и комуникация между тях и родителите.

Има много приложения за родителски контрол на пазара, някои от които са платени, а други са безплатни. Това са някои от най-популярните приложения за родителски контрол: **Qustodio, Net Nanny, Norton Family, Google Family Link, Microsoft Family Safety.**

ТЕХНОЛОГИИ ЗА ЗАЩИТА НА ДЕТЕТО В ДИГИТАЛНОТО ПРОСТРАНСТВО



ПРИЛОЖЕНИЯ ЗА РОДИТЕЛСКИ КОНТРОЛ

ЕТО НЯКОЛКО СТЪПКИ, КОИТО МОГАТ ДА ВИ ПОМОГНАТ ДА СЕ НАУЧИТЕ ДА РАБОТИТЕ С РОДИТЕЛСКИ КОНТРОЛНИ ПРИЛОЖЕНИЯ:

1. ИЗСЛЕДВАЙТЕ РАЗЛИЧНИТЕ ПРИЛОЖЕНИЯ ЗА РОДИТЕЛСКИ КОНТРОЛ И ИЗБЕРЕТЕ ТОВА, КОЕТО НАЙ-ДОБРЕ ОТГОВАРЯ НА ВАШИТЕ НУЖДИ.
2. ИНСТАЛИРАЙТЕ ПРИЛОЖЕНИЕТО НА УСТРОЙСТВОТО НА ВАШЕТО ДЕТЕ И ГО НАСТРОЙТЕ СПОРЕД ПРЕДПОЧИТАНИЯТА ВИ.
3. ПРОВЕРЯВАЙТЕ РЕДОВНО НАСТРОЙКИТЕ И РЕЗУЛТАТИТЕ ОТ ПРИЛОЖЕНИЕТО ЗА РОДИТЕЛСКИ КОНТРОЛ. ПРОДЪЛЖАВАЙТЕ ДА СЛЕДИТЕ ДЕЙНОСТТА НА СВОЕТО ДЕТЕ И АНАЛИЗИРАЙТЕ ДАННИТЕ, КОИТО ПРЕДОСТАВЯ ПРИЛОЖЕНИЕТО, ЗА ДА УСТАНОВИТЕ КАКВО Е НЕОБХОДИМО ДА СЕ ПРОМЕНИ.
4. БЪДЕТЕ ОТВОРЕНИ И ОБЩУВАЙТЕ СЪС СВОЕТО ДЕТЕ ОТНОСНО ИЗПОЛЗВАНЕТО НА РОДИТЕЛСКИ КОНТРОЛ. ОБЯСНЕТЕ НА ДЕТЕТО СИ ЗАЩО ИЗПОЛЗВАТЕ ПРИЛОЖЕНИЕТО ЗА РОДИТЕЛСКИ КОНТРОЛ И КАК ТОВА ПОМАГА ЗА ЗАЩИТАТА МУ ОНЛАЙН.

ЦЕНТЪР ПО КИБЕРСИГУРНОСТ CYBERONE

С разбиране, че цялата тази информация е много сложна за усвояване от детето Ви, а дори от Вас самите, Ви напомняме, че има и други начини за защита, а именно тези, които се предлагат от нашия **център по киберсигурност CyberOne, както и се включват в услугите, предлагани от кибер застраховките на ЗК „Лев Инс" АД.**

Връзката между дете и родител не винаги е толкова близка. В много случаи децата прикриват информация от родителите си.

Ако често не можете да контролирате действията и постъпките на детето си и то е толкова непредвидимо, че каквото и да му говорите, прави каквото си реши или се разстройва и не иска да контактува с Вас на тези теми, то има и технологични начини да спрете това.

Центърът по киберсигурност CyberOne Ви предлага услуги, с помощта на които можете да реализирате контрол на детето си в дигиталното пространство. Центърът по киберсигурност на CyberOne осигурява киберсигурността на Вас и Вашето семейство.

Чрез услугата **"Филтриране на интернет трафик"** можете да забраните достъпа на децата си до определени зловредни сайтове, приложения и програми.

Повече информация може да откриете тук.

CYBERONE

Нашият център по киберсигурност може да обезпечи защитата на устройствата в дома Ви от вируси. Заразяването от вируси може да е следствие от грешка на Вашето дете, както и на Вас самите. За да бъдат предотвратени възможни инциденти на детето Ви в интернет, **центърът по киберсигурност CyberOne има академия – Cyber360 Academy, която предлага обучения за родители и деца.**

Друга услуга, която ще Ви бъде много полезна, са денонощните консултации от експерти на CyberOne на телефонната линия на компанията. Те оказват помощ във всеки момент и по този начин могат да предотвратят инциденти в кибер пространството.

Повече информация може да получите тук.

КИБЕР ЗАСТРАХОВАНЕ ЗК „ЛЕВ ИНС” АД

Не е достатъчно да се уповаваме само на родителските си инстинкти, а трябва да се замислим дали да не се възползваме от специализирани услуги като тези на **центъра по киберсигурност CyberOne, както и застрахователните решения на „Лев Инс”.**

Можете да осигурите защита на семейството и детето си чрез сключване на киберзастраховка в ЗК „Лев Инс”. „Лев Инс” е единствената застрахователна компания в България, която предлага застрахователни услуги в дигитална среда.

При сключване на застраховката „Безопасен интернет” клиентите могат да използват следните услуги:

- **Сигурно сърфиране в мрежата**
- **Блокиране на реклами**
- **Защита на поверителността**
- **Защита на информацията**
- **Родителски контрол**

КАК МОЖЕ ДА СКЛЮЧИТЕ ПОДОБЕН ТИП ЗАСТРАХОВКА?

Във всеки офис на ЗК „Лев Инс",както и тук.

Важно е да се отбележи също така, че всички клиенти на ЗК „Лев Инс" имат включена безплатна връзка към телефон: **0800 10 200**, на който могат да задават своите въпроси свързани с киберсигурността им.

За решението на по-специфични въпроси и пренасочването Ви към експерт ще се реализира след закупуване на **услугата „Кибер помощ".**

За тази услуга можете да получите повече информация тук.

Застраховката "Безопасен интернет" ще бъде полезна за Вас, Вашето семейство, както и за близките Ви в няколко аспекта. За разлика от центъра по киберсигурност, който се занимава единствено със защитата на Вашата дигитална сигурност, то **киберзастраховката осигурява и покритие с лимит на отговорност до 1000 лв., и едновременно с това е превантивна мярка, ограничаваща множество зловредни въздействия,** които могат да достигнат до клиента чрез интернет.

КИБЕР ЗАСТРАХОВАНЕ ЗК „ЛЕВ ИНС” АД

С тази застраховка, застрахованият предпазва и своите приятели, клиенти или контрагенти, в случай че неговият компютър неволно разпространява вредно съдържание.

Покритието „Безопасен интернет” може да бъде добавено към всяка една полица от ЗК „Лев Инс”, независимо от нейния вид.

Застрахованите лица получават също така достъп до клиентски портал, в който имат възможност допълнително да управляват настройките си за сигурност.

По този начин се прекъсват връзките с опасни сайтове, защитават се сайтове с незаконно съдържание, блокират се реклами, премахва се възможността за проследяване чрез злонамерени програми.

ПРИ НУЖДА ОТ ПОМОЩ И СЪДЕЙСТВИЕ

Ако имате въпроси или съмнения относно това, какво прави детето Ви онлайн, обърнете се за помощ към специалистите на CyberOne, Cyber360 Academy и „Лев Инс“, на телефон: 0800 10 200

Можете също така да се свържете и с организации на реда като например Дирекция Киберпрестъпност при Главна дирекция Борба с организираната престъпност към Министерството на вътрешните работи **(ГДБОП-МВР)**, които работят по проблемите свързани с безопасността в интернет. С тях можете да се свържете и да докладвате за киберпрестъпление на телефон **0885 525 545** и електронна поща: report@cybercrime.bg.