CLICK SMART

SAFER.BG
Дигитално читалище

ПРОГРАМА ЕВРОПА
СТОЛИЧНА ОБЩИНА

СЪДЪРЖАНИЕ

ЗДРАВЕЙ! ТИ ДЪРЖИШ В РЪЦЕТЕ СИ CLICKSMART

Здравей!

Това, което държиш в ръцете си, е справочник, създаден специално за теб и твоето семейство. Нарекохме го „ClickSmart – Една крачка пред киберзаплахите“, защото нашата цел е да ти помогнем да разбираш по-добре какво се случва онлайн и как да се предпазиш.

Интернет е мястото, където се срещаш с приятели, учиш нови неща, забавляваш се, следваш хора, които харесваш, и дори откриваш нови възможности за бъдещето си. Но освен свобода и удобство, той носи и предизвикателства. Само през последната година в България са подадени близо триста хиляди сигнала за кибертормоз. Повече от половината деца у нас са ставали жертва на подигравки, заплахи или обиди онлайн.

Едно момиче на 14 години споделя: „Публикувах снимка, която ми харесваше, но няколко съученици започнаха да ми пишат подигравки. В началото мислех, че е шега, но после ми беше трудно дори да вляза в училище.“

Момче на 16 години разказва: „Получих съобщение от непознат, който ми предложи да изпратя лична снимка. Когато отказах, започна да ме заплашва, че ще напише лъжи за мен. Страхувах се да кажа на родителите си.“

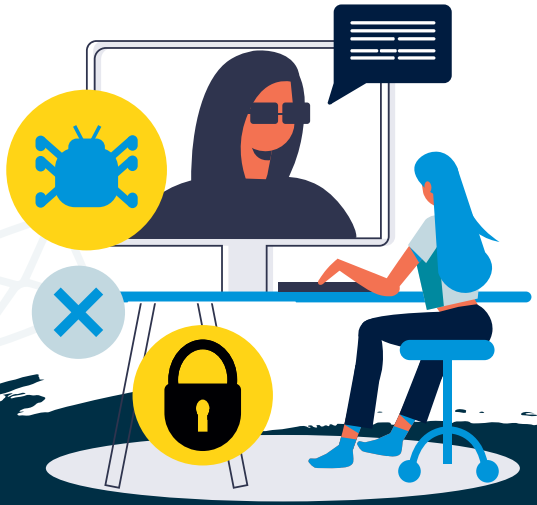
Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Такива истории са истински и често остават скрити. Много деца и младежи не споделят за проблемите си, защото се срамуват или се страхуват от реакцията на възрастните. Точно затова тази книжка е написана така, че да бъде разбираема за всеки – за ученици, студенти, родители и учители.

Ако си млад човек, тук ще откриеш съвети, които да ти помогнат да разпознаваш опасностите и да реагираш уверено. Ще видиш, че не си сам и че има кой да ти помогне. Ако си родител, ще получиш насоки как да бъдеш до детето си, без да го контролираш, а като партньор и подкрепа. А ако си учител, ще намериш идеи как да разговаряш с учениците за тези теми и как да създаваш среда, в която те се чувстват защитени.

Тази книжка е покана за разговор – разговор в семейството, в класната стая и сред приятели. В нея има истории, които може би ще ти напомнят за твои преживявания, игри и тестове, които ще те накарат да се замислиш, и конкретни стъпки как да действаш, ако нещо се случи.

Най-важното, което искаме да запомниш още сега, е, че онлайн светът може да бъде безопасен, ако знаеш правилата и ги използваш всеки ден. А когато мислиш една крачка напред, ти вече си на пътя на дигиталния супергерой – човек, който не се плаши от предизвикателства, а знае как да ги преодолее.



РАЗДЕЛ I – КИБЕРЗАПЛАХИТЕ, КОИТО ТРЯБВА ДА ПОЗНАВАШ

КАКВО Е КИБЕРЗАПЛАХА?

Киберзаплахата е всичко, което може да застраши теб, твоите данни и устройствата ти, когато си в дигиталния свят. Това може да е фалшив профил, опит за измама, вреден софтуер или целенасочена атака. В киберсигурността често казваме, че заплахата е основен елемент при определянето на риска от успешни кибератаки. За да можем да се предпазим, първо трябва да познаваме заплахите – само така можем да предвиждаме рисковете, на които сме изложени.

Важно е да помним, че не самата заплаха е „хитра", а хакерите зад нея. Те постоянно измислят нови начини да ни подведат. Ако разберем как действат, можем да сме една крачка пред тях.

Много често младите хора срещат киберзаплахи там, където прекарват най-много време – в игрите. Представи си, че играеш любимата си онлайн игра и получаваш съобщение: „Ако въведеш този код, ще отключиш специални предмети безплатно". На пръв поглед звучи примамливо, но кодът всъщност води към фалшив сайт, който иска данните на акаунта ти. Едно момче на 14 години разказва: ***„Исках нов скин в играта и кликнах на линк, който изглеждаше официален. Въведох паролата си и след час вече не можех да вляза. Някой беше взел профила ми."*** Решението е винаги да проверяваш източника и да не въвеждаш пароли извън официалния сайт или приложение.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Друг пример е свързан с плащанията. Някои измамници използват игрите, за да подмамят деца и младежи да въведат данните на картите на родителите си. ***„Получих предложение да купя монети с голяма отстъпка, само трябваше да въведа картата на мама. Казаха, че промоцията изтича след минути. За щастие попитах и разбрах, че това е измама.“*** Подобни ситуации показват, че една от най-важните стъпки за защита е разговорът с родителите и никога да не се въвеждат финансови данни без тяхното знание и съгласие.

Киберзаплахите могат да се проявят и в по-незабележими форми – например когато непознат ти пише с молба да му изпратиш лична снимка или ти предлага „приятелство“, за да извлече информация. Това също е заплаха, макар да изглежда невинно. Ако нещо те кара да се чувстваш неудобно или съмнително, това вече е сигнал, че може да има риск.

За родителите и учителите е важно да знаят, че киберзаплахите са не само технически проблем, а и социален. Децата често се сблъскват с измами, фалшиви обещания или натиск от връстници онлайн. В много случаи те не споделят, защото се страхуват от наказание или недоверие. Затова най-сигурният начин за защита е отворен разговор и подкрепа.

Когато познаваме заплахите и ги разбираме, вече сме направили първата крачка към сигурността. В следващите раздели ще разгледаме най-често срещаните киберзаплахи и ще ти покажем как да ги разпознаваш и как да реагираш, за да останеш защитен.

НАЙ-ЧЕСТИТЕ ОПАСНОСТИ, ПРЕД КОИТО СЕ ИЗПРАВЯТ МЛАДЕЖИТЕ

След като вече разбрахме какво представлява киберзаплахата, време е да се вгледаме по-внимателно в най-честите опасности, пред които се изправят младите хора онлайн. Заплахата е като предупредителен знак – ако я познаваш, можеш да предвидиш риска и да се подготвиш. Колкото по-добре разбираме тези рискове, толкова по-малка е вероятността да станем жертви на атака.

Днес младежите са едни от най-активните участници в дигиталния свят – социални мрежи, онлайн игри, видеоплатформи, чат приложения. Точно там обаче се появяват и най-много капани. Хакерите използват фалшиви профили, измислени истории, натиск или примамливи обещания, за да извлекат лична информация, да откраднат акаунт или да накарат някой да направи нещо против волята си.

Младите хора споделят, че често не разбират веднага, че става дума за измама.„Добави ме профил, който имаше снимка на мой съученик. Първо ми написа приятелски, а после започна да иска лични неща. Когато проверих, се оказа, че съучениктът изобщо няма такъв профил.“ Такива ситуации са част от реалността, в която живеем.

В тази глава ще разгледаме стъпка по стъпка кои са основните киберзаплахи за младежите днес, как да ги разпознаем и какво да правим, ако попаднем в тях. Ще видим и реални случаи от България и света, за да стане ясно, че това не са далечни истории, а проблеми,

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

които се случват тук и сега. Ще говорим за фалшиви профили, кибертормоз, измами в игрите и социалните мрежи, изтичане на лични данни и хакване на акаунти. Ще обясним какво означават тези ситуации, какво е тяхното въздействие и какви конкретни стъпки можеш да предприемеш, за да останеш защитен.

За родителите и учителите това е възможност да влязат в света на младите и да разберат по-добре какво ги тревожи онлайн. Когато знаеш как изглеждат заплахите, можеш по-лесно да разговаряш за тях, да подкрепиш и да помогнеш на детето или ученика си да се справи.

Това знание е първата бариера срещу атаките. А когато имаме информация, имаме и сила – силата да изберем правилното действие, вместо да бъдем изненадани.

Започваме с конкретните киберзаплахи

Киберзаплахата е като сигнал за предстояща буря – ако я забележиш навреме, можеш да се скриеш и да останеш в безопасност. След като вече знаем какво означава този термин, е време да разгледаме кои са най-важните заплахи за младите хора днес. Те не са една или две, а цял спектър от рискове, които се променят заедно с технологиите и начина, по който общуваме онлайн.

За да бъде по-ясно, ще разгледаме всяка заплаха отделно. Ще видим как изглежда, как може да бъде разпозната, кои са „червените флагове“, какви са последствията и най-важното – какво можем да направим, за да се защитим. Ще включим и реални примери от България и света, защото когато историята е истинска, посланието е по-силно.

Фалшиви профили и измами в социалните мрежи

Социалните мрежи са като огромно училищно междучасие – всеки иска да се покаже, да общува, да намери приятели. Но сред множеството лица винаги има и такива, които носят маска. Фалшивите профили са една от най-честите заплахи за младите хора онлайн. Те могат да изглеждат безобидни, но зад тях често стои някой, който иска да вземе лични данни, да подведе или дори да навреди.

Пример е и историята която разказахме по-горе: ***„Получих покана за приятелство от профил със снимка на мое съученичка. Приемам, защото мислех, че е тя. След няколко дни започна да ми пише съобщения с въпроси за личния ми живот, които ми се сториха странни. После разбрах, че истинската ми съученичка няма такъв профил.“***

Как да разпознаеш фалшивия профил

Има няколко ясни предупредителни знака. Ако профилът е създаден скоро, има много малко снимки или всички снимки изглеждат еднакво „перфектни“, това е първи сигнал. Ако човекът бърза да задава лични въпроси, настоява за снимки или избягва да се виждате на живо, това също е „червен флаг“.

Какво да правиш

Най-добрият подход е да не споделяш лични данни с непознати, колкото и убедителни да изглеждат. Ако имаш съмнение, провери с общи приятели или директно попитай истинския човек дали има такъв профил. А ако вече си споделил информация и чувстваш, че

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансова подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

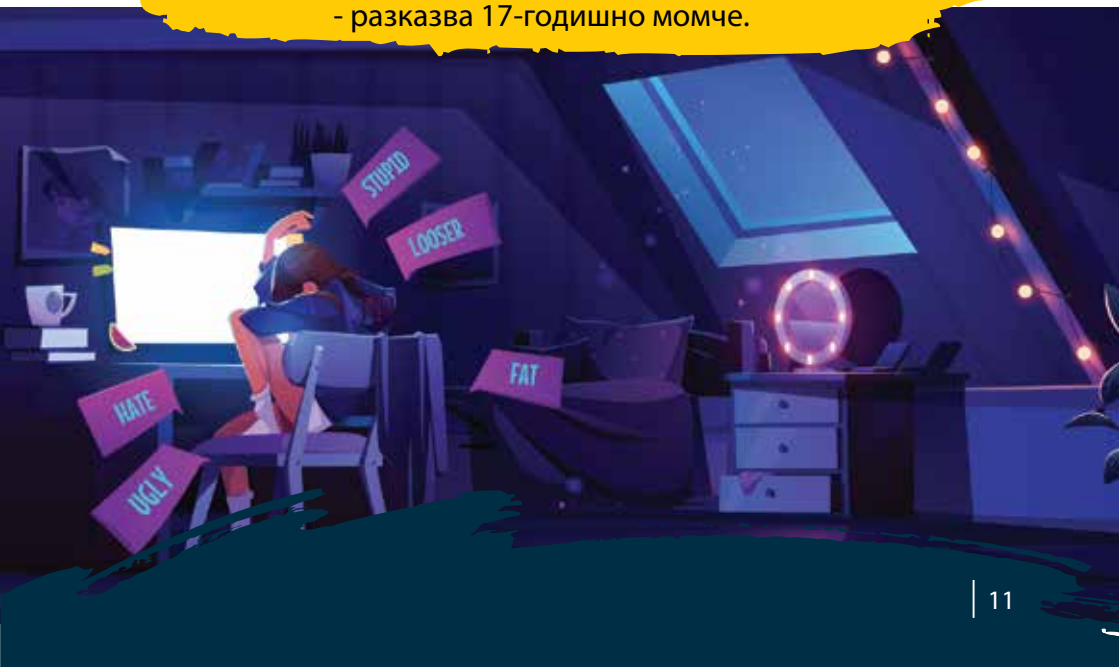
си подведен, важно е да кажеш на родител, учител или доверен приятел. Социалните мрежи също имат функция за докладване и блокиране – използвай я.

Реални случаи и въздействие

През последните години ГДБОП съобщава за множество измами, при които младежи са били подведени да предоставят лични данни чрез фалшиви профили. На форуми като BGMama родители разказват как децата им са били манипулирани от „приятел“ в социалните мрежи, който всъщност се оказва непознат възрастен. В международни общности като Reddit има десетки истории на млади хора, които губят достъп до профилите си или биват изнудвани, след като са повярвали на фалшив профил.

Последиците невинаги са само технически. Често жертвата изпитва срам, вина или страх. Това показва, че измамата не отнема само акаунти, а и увереността на младия човек.

„Чувствах се глупаво, че съм се хванал, и дълго време не исках да влизам в социалните мрежи“
- разказва 17-годишно момче.



Фишинг и неговите разновидности

Фишингът е като примамка – нещо, което изглежда истинско, но всъщност цели да те подведе. Хакерите използват съобщения, имейли, телефонни обаждания или дори фалшиви QR кодове, за да получат достъп до личните ти данни. Важно е да знаеш, че формите на фишинг са различни, но целта винаги е една и съща – да те измамят, за да им дадеш информация.

Имейл фишинг

Това е най-разпространеният вариант. Получаваш имейл, който прилича на съобщение от банка, куриерска фирма или университет. Изглежда спешно: ***„Акаунтът ви ще бъде блокиран, ако не потвърдите данните си.“*** Много хора кликват върху линка и въвеждат паролите си.
Червени флагове: граматически грешки, необичайни линкове, твърде голямо чувство за спешност.
Какво да правиш: никога не въвеждай пароли чрез линкове в имейли; винаги проверявай чрез официалния сайт.

Фишинг в чат и социални мрежи

Тук примамката идва като лично съобщение. Може да изглежда като молба от приятел или като оферта в група. В български форум родител разказва как дете получило линк в Messenger с обещание за безплатни стикери. След въвеждане на парола акаунтът му бил поет от измамник.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Червени флагове: непознат изпращач, странни линкове, молба за лични данни.
Какво да правиш: блокирай и докладвай; ако вече си кликнал, смени паролата веднага.

Вишинг (voice phishing)

Тук измамата идва по телефона. Получаваш обаждане от „служител на банка“ или „техническа поддръжка“. Гласът звучи убедително и често използва спешност: ***„Вашата карта е компрометирана, трябва веднага да потвърдите ПИН кода.“*** В Reddit много млади хора споделят, че са получили такива обаждания, като някои дори са чули клониран глас с помощта на изкуствен интелект.
Червени флагове: настояване за лични данни, използване на страх или паника.
Какво да правиш: прекъсни разговора и сам се обади на официалния номер на институцията.

Смишинг (SMS phishing)

Това са измамни текстови съобщения. Пример от България: ГДБОП предупреждава за SMS-и с текст ***„Пратката ви е задържана, потвърдете тук“.*** Линкът води до фалшив сайт, който краде данни.
Червени флагове: линкове в SMS, които изглеждат странно или идват от непознат номер.
Какво да правиш: не кликвай; провери информацията през официалното приложение или сайт.

QR фишинг (quishing)

По-нова разновидност. Хакерите поставят фалшиви QR кодове върху афиши, постери или дори в заведения. При сканиране се отваря сайт, който изглежда легитимен, но иска данни. През 2023 г. полицията в няколко европейски държави съобщи за подобни случаи на измамени студенти, които мислели, че сканират QR код за безплатен Wi-Fi.

Червени флагове: QR кодове на съмнителни места или такива, които прикриват оригинален стикер.

Какво да правиш: използвай QR кодове само от доверени източници; провери линка преди да отвориш.

Въздействие и реални истории

Фишингът може да изглежда „просто“ като имейл или SMS, но последствията са тежки. Изгубени акаунти, достъп до лични снимки, източени средства от карти. ***„Татко кликна на линк за пратка и въведе картата си. След час бяха изтеглени пари. Беше голям стрес за всички ни.“*** – споделя ученик в дискусия в BGMama.

Загубата е не само финансова, но и емоционална. Жертвата често се чувства засрамена или измамена. Важно е да се помни, че измамата е дело на хакерите, а не вина на потърпевшия.

Сексторшън – изнудване с интимни снимки и клипове

Сексторшън е дума, която съчетава ***„секс“*** и ***„изнудване“***. Това е форма на киберпрестъпление, при което някой успява да получи твои лични или интимни снимки и след това те изнудва: ***„Ако не***

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

ми платиш“ или ***„ако не ми изпратиш още материали, ще ги покажа на всички.“***

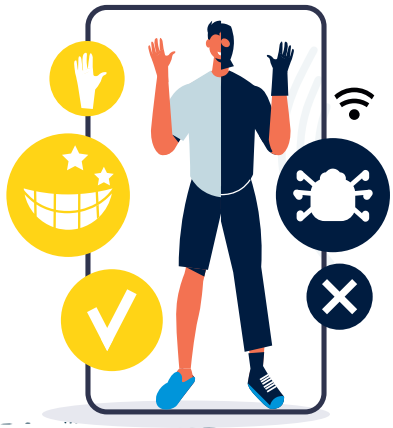
Това не засяга само момичетата. Все повече случаи показват, че и момчета стават жертви – често дори по-често от момичета, защото изнудвачите използват психологически натиск и обещават бърза „връзка“ или флирт.

„Запознах се с момиче в Instagram. След два дни тя поиска да си пуснем видео чат. Малко след това получих съобщение, че ако не изпратя пари, ще качат записа в интернет.“
– споделя 17-годишен ученик.

Трагичното е, че жертви могат да бъдат и родители, ако децата им попаднат в подобна схема. ***„Дъщеря ми беше заплашена, че лични снимки ще бъдат пуснати в училищната група. Аз бях този, който получи съобщение за пари.“*** – разказва баща от форум за родители. Това показва, че проблемът не е индивидуален – той засяга цели семейства.

Как да разпознаеш заплахата

Първият ***„червен флаг“*** е, когато нов познат онлайн бързо премине към интимни теми и настоява за снимки или видео. Друг знак е, ако съобщенията идват от профили с малко съдържание, със съмнителни снимки или с твърде бърза ескалация към ***„лично общуване“.*** Често веднага след изпращането на снимка се появява заплахата.



Какво да правиш

Най-важното правило е: ***никога не изпращай интимни материали, дори ако човекът изглежда доверен.*** Ако вече си жертва, първата реакция е да ***спреш комуникацията*** и ***да не изпращаш повече съдържание или пари***. След това:

- Запази съобщенията и снимките като доказателство.
- Сподели веднага с родител или доверен възрастен.
- Подай сигнал в платформата (Instagram, TikTok, Snapchat) и, ако е нужно, в ГДБОП или Центъра за безопасен интернет.

Реални случаи и въздействие

През 2023 и 2024 г. службите в Европа отчитат рязък ръст на сексторшън, особено спрямо момчета между 13 и 18 години. В България Центърът за безопасен интернет също съобщава за увеличен брой сигнали. В Reddit и други международни общности жертвите споделят, че основното чувство е паника и срам.

„Първата ми мисъл беше, че животът ми е свършен. Но когато казах на родителите си, разбрах, че не съм сам и има какво да се направи."

Последиците могат да бъдат тежки – тревожност, изолация, дори мисли за самонараняване. Затова е важно да подчертаем: вината никога не е у жертвата, а у извършителя.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Послание към родители и учители

Ако дете или ученик попадне в подобна ситуация, първата реакция трябва да бъде подкрепа, а не обвинение. Думите ***„Как можа да си толкова наивен?“*** могат да нанесат повече щети от самата заплаха. Правилното послание е: ***„Добре, че ми каза. Заедно ще намерим решение.“*** Важно е да се подаде сигнал и да се търси професионална помощ – не само техническа, но и психологическа.

Киберзаплахи за кражба и изтичане на лични данни

Личните данни са повече от име и адрес. Това е всяка информация, която може да те идентифицира – телефонен номер, снимка, имейл, профил в Instagram, здравни данни, дори геолокацията на телефона ти. В Европа тяхната защита е гарантирана от ***Общия регламент за защита на личните данни (GDPR)***, а новият ***Акт за данните (Data Act)*** въвежда още по-ясни правила кой и при какви условия може да използва информацията, която генерираме чрез устройства и приложения.

И все пак, въпреки законите, данните продължават да изтичат. Причината е проста – не само хакерите ги крадат, често ние самите ги даваме без да се замислим. Попълваме анкети и викторини в социалните мрежи, инсталираме приложения, които искат достъп до галерията и контактите ни, или качваме документи в сайтове за изкуствен интелект, без да четем условията. В тези случаи информацията ни не е „откраднатa“ – ние сами я подаряваме.

Как да разпознаеш заплахата

Червените флагове са навсякъде: приложение, което иска повече права, отколкото има нужда; сайт, който обещава „безплатни награди“ срещу данни; непознат линк в SMS, който иска да въведеш картата на родителите си. Ако се замислиш „Защо им е нужно това?“ и не получаваш добър отговор – значи е заплаха.

Какво да правиш

- Чети внимателно условията и настройките за поверителност.
- Давай достъп до камера, микрофон или галерия само на приложения, на които имаш доверие.
- Използвай различни имейли за регистрация в игри, социални мрежи и учене.
- Ако данните вече са изтекли, смени паролите си и включи двуфакторна защита. Ако става дума за карта – веднага уведоми банката. При сериозни пробиви подай сигнал до ***Комисията за защита на личните данни*** или ***ГДБОП***.

Реални случаи и въздействие

През последните години има пробиви в големи платформи, които са засегнали милиони потребители по света. В България родители споделят в BGMama как децата им са получили обаждания от „банки“, след като телефонните им номера са изтекли в мрежата. В Reddit млади хора разказват как са загубили достъп до акаунти в Instagram, след като са въвели паролата си в „официална форма“ за проверка на възраст.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Въздействието не е само техническо. Загубата на контрол върху личната информация води до тревожност, недоверие и страх да бъдеш отново открит.

„Чувствах се, сякаш някой е влязъл в стаята ми без да питам. Всички лични неща вече не бяха само мои."
– споделя 16-годишна ученичка.

Кражба чрез хак и кражба чрез доверие

Важно е да разберем, че киберзаплахите за данните действат по два начина. Понякога хакерите пробиват системи и крадат информация масово. Но много по-често те просто използват нашето доверие – ние сами кликваме, въвеждаме и даваме ключовете. Това е като да оставиш входната врата отключена – няма нужда някой да разбива.

Какво означава „хакване" на акаунт

За да разберем какво е „хакване", първо трябва да уточним какво е акаунт. Акаунтът е твоето лично пространство в интернет – профилът ти в Instagram, TikTok, Facebook, Discord, любимата ти онлайн игра, дори училищната платформа за уроци. Той съдържа твоята история: приятели, снимки, постижения, съобщения, контакти. Затова акаунтът е като ключ към дигиталния ти живот.

Когато някой „хакне" акаунта ти, това означава, че е взел този ключ без разрешение и вече може да влиза на твое място. Често това се случва чрез комбинация от техники – не е само един метод.

- ***Фишинг*** – получаваш съобщение или имейл, който те подлъгва да въведеш паролата си.
- ***Социално инженерство*** – някой се представя за твой приятел или администратор и те убеждава да му дадеш достъп.
- ***Слаба парола*** – ако паролата ти е „123456“ или името на любимия ти отбор, хакер може да я отгатне за секунди. Повторна употреба на пароли – ако използваш една и съща парола навсякъде и тя изтече от някой сайт, автоматично излагаш на риск и другите си акаунти.
- ***Повторна употреба на пароли*** – ако използваш една и съща парола навсякъде и тя изтече от някой сайт, автоматично излагаш на риск и другите си акаунти.

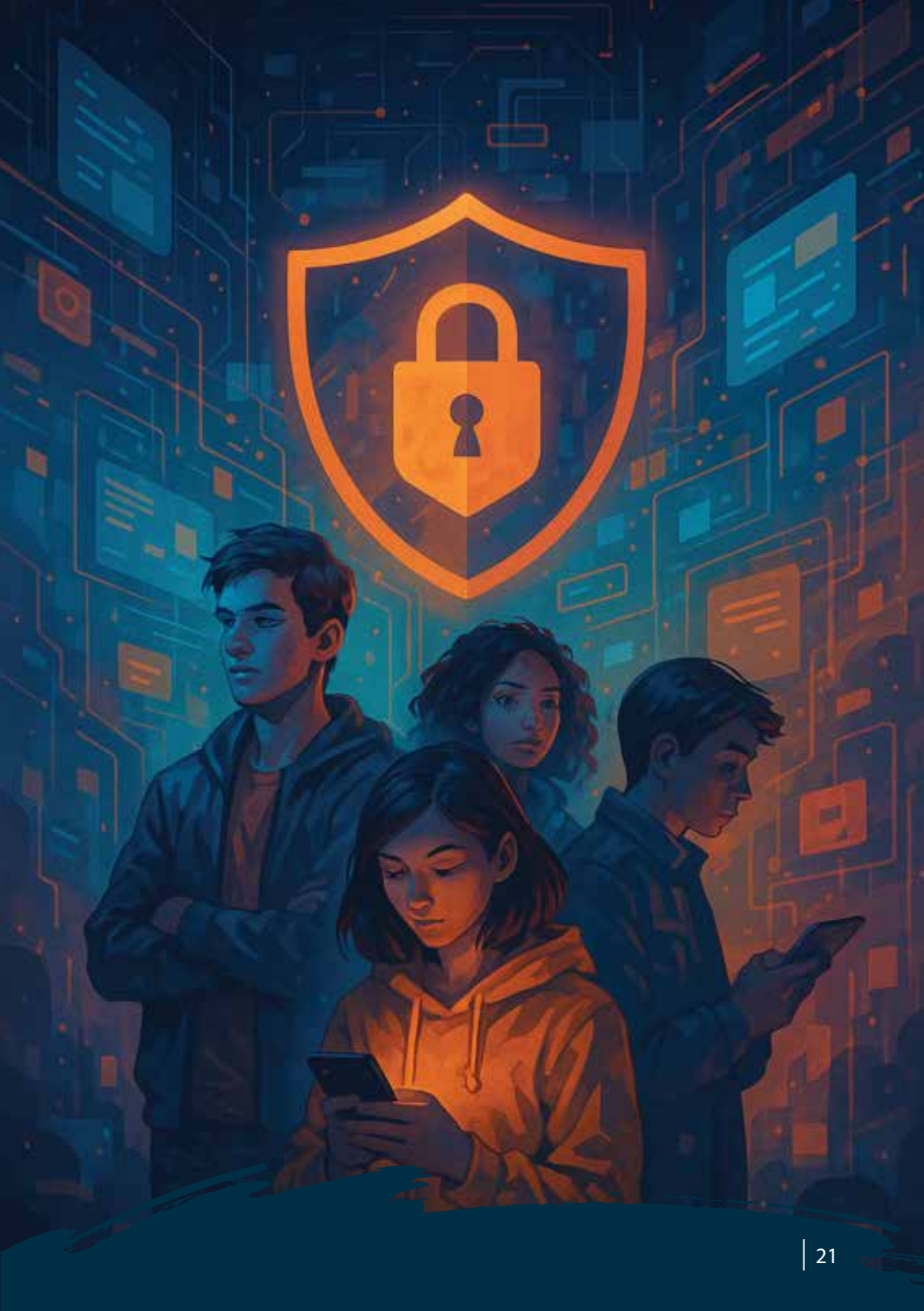
Как да разпознаеш, че акаунтът ти е хакнат

Първите признаци често са промени, които не си правил:

- не можеш да влезеш в профила си, защото паролата е сменена;
- приятелите ти получават странни съобщения от твое име;
- виждаш публикации, които не си качвал;
- получаваш имейли за нов вход от непознато място.

„Събудих се и не можех да вляза в Instagram. Оказа се, че акаунтът ми изпраща реклами за криптовалути на всички приятели. Чувствах се сякаш някой друг живее живота ми онлайн.“
– споделя 16-годишен ученик от София.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА



Какво да правиш

Първо, опитай да възстановиш достъпа чрез функцията „Forgot password". Ако това не помогне, използвай инструкциите на самата платформа за „компрометиран акаунт". Уведоми приятелите си, за да не бъдат подведени. Ако има риск финансови данни да са свързани (например акаунт за игри с вързана карта), веднага уведоми родителите и банката.

След възстановяване – смени паролата с по-силна и включи двуфакторна автентикация (код по SMS или приложение). Това е най-сигурният начин да защитиш профилите си занапред.

Реални случаи и въздействие

В България често се съобщава за хакнати акаунти във Facebook, Instagram и игри. ГДБОП предупреждава, че тези профили се използват за разпространение на измами и вируси. В международни форуми като Reddit младежи разказват как губят достъп до акаунтите си в Roblox или Fortnite и заедно с това губят години труд и постижения.

Въздействието е не само техническо, но и емоционално. Загубата на акаунт е като загуба на личностна карта – тя отнема част от идентичността и връзките ти.

„Изведнъж загубих контакт с приятелите си, защото всички разговори бяха в Messenger. Чувствах се откъснат от света."

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Дийпфейкове и AI-имитации – новата вълна от измами

Преди години можеше да познаеш измамата по тромавия имейл с правописни грешки. Днес обаче киберзаплахите изглеждат съвсем различно. Благодарение на изкуствения интелект вече е възможно да се създават видеа и гласови съобщения, които изглеждат и звучат напълно истински. Тези технологии се наричат ***дийпфейкове*** (фалшиви видеа, в които някой „прави" неща, които всъщност никога не е правил) и ***AI-имитации на глас*** (клониране на нечий глас само от няколко секунди запис).

На пръв поглед това може да изглежда като безобидна забава – да сложиш лицето на известен актьор върху видеоклип или да чуеш как любимият ти певец „изпълнява" нова песен, която никога не е записвал. Но в ръцете на измамници тези технологии се превръщат в мощно оръжие. Представи си, че получаваш обаждане от гласа на майка си, която ти казва, че е в беда и има нужда от помощ. Или видео, в което приятел ти моли за пари. В първия момент реакцията е паника, защото изглежда и звучи истински. Именно това използват хакерите – човешките емоции и доверие.

В Европа вече има реални случаи на родители, които са били измамени, защото са чули „гласа" на своето дете по телефона. В България също има предупреждения от ГДБОП за първи опити за телефонни измами с клонирани гласове. В международни форуми като Reddit младежи разказват как са били подведени от видеообаждания, които изглеждат автентични, но се оказват дийпфейкове.

Как можеш да разпознаеш подобна заплаха?

Понякога в гласа има дребни странности – неестествена пауза, прекалено равен тон, повторение на думи. Видеото може да изглежда леко „странно“ около устата или очите. Но най-силният сигнал е съдържанието: когато съобщението е прекалено спешно или необичайно. „Веднага ми прати парите!“, „Изпрати ми кода сега!“ – това са класически примери за изнудване чрез емоции.

Какво да правиш в подобна ситуация?

Най-важното е да не действаш веднага. Вместо това провери по друг канал – обади се лично на човека или използвай предварително уговорена кодова дума в семейството. Много семейства вече имат проста уговорка: ако някой звъни в беда, казва предварително избрана дума или израз, който е трудно да бъде отгатнат.

Реални случаи и въздействие

Въздействието от подобна измама е силно емоционално. „Бях убедена, че чувам сина си. Когато разбрах, че съм измамена, се чувствах виновна и предадена“ – споделя майка в медийно интервю. Това показва, че тук не става дума само за загуба на пари, а за разклащане на доверие и чувство за сигурност.

За младите хора опасността също е реална. Публичните им видеа и гласови съобщения в социалните мрежи могат да бъдат използвани, за да се създадат убедителни копия. Тези копия после се прилагат в сценарии на измами или изнудване. Колкото повече съдържание качваме без да мислим, толкова по-лесно е да бъдем манипулирани.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Затова основното послание е ясно: дийпфейковете и AI-имитациите са новата вълна от киберзаплахи, която не можем да игнорираме. Но когато знаем за тяхното съществуване, когато подхождаме с внимание и проверяваме, вместо да реагираме моментално, вече сме направили най-важната крачка към защита.

Дезинформация – заплаха за мисленето и избора ни

Не всяка киберзаплаха идва като вирус или хак. Понякога заплахата е в думите, снимките или видеата, които виждаме онлайн. Това е дезинформацията – съдържание, което умишлено подвежда, за да ни накара да вярваме в нещо невярно или да правим избори, които не бихме направили иначе.

Дезинформацията има различни лица. Понякога е фалшива новина, която разпалва страх или омраза. Друг път е „ревю" на продукт, който никой не е ползвал, но което те убеждава да купиш. Тя може да се използва и за по-сериозни цели – да въвлече младежи в крайни групи, да ги изолира от приятели или да ги подтикне към поведение, което е опасно за тях.

„Споделиха ми линк, в който пишеше, че ако купя определени хапчета, ще изглеждам по-добре за две седмици. Оказа се измама, но в началото бях убеден, защото всички в TikTok говореха за тях."
– разказва 15-годишно момче.

В други случаи дезинформацията може да бъде политическа или идеологическа. В интернет лесно можеш да попаднеш на групи, които те убеждават, че „само те казват истината" и че трябва да се отделиш от приятелите или семейството си. Постепенно младият човек започва да вярва в конспирации и да губи връзка с реалността.

Как можем да разпознаем дезинформацията?

Обикновено тя се стреми да предизвика силна емоция – страх, гняв, желание за бързо действие. В новините липсват ясни източници или пък се използват сензационни заглавия. В рекламите се обещава прекалено бърз резултат. А в социалните мрежи често се споделят едни и същи постове от различни профили, които изглеждат подозрително сходни.

Какво да правим, когато срещнем подобно съдържание?

Най-важното е да не бързаме да вярваме и да споделяме. Проверка на източника, сравнение с други медии и въпросът „Кой печели, ако аз повярвам на това?“ са първи стъпки. Ако се съмняваш в даден сайт, по-добре не споделяй съдържанието му. В разговори с приятели или родители сподели своите съмнения – често различна гледна точка помага да видиш манипулацията.

Реални случаи и въздействие

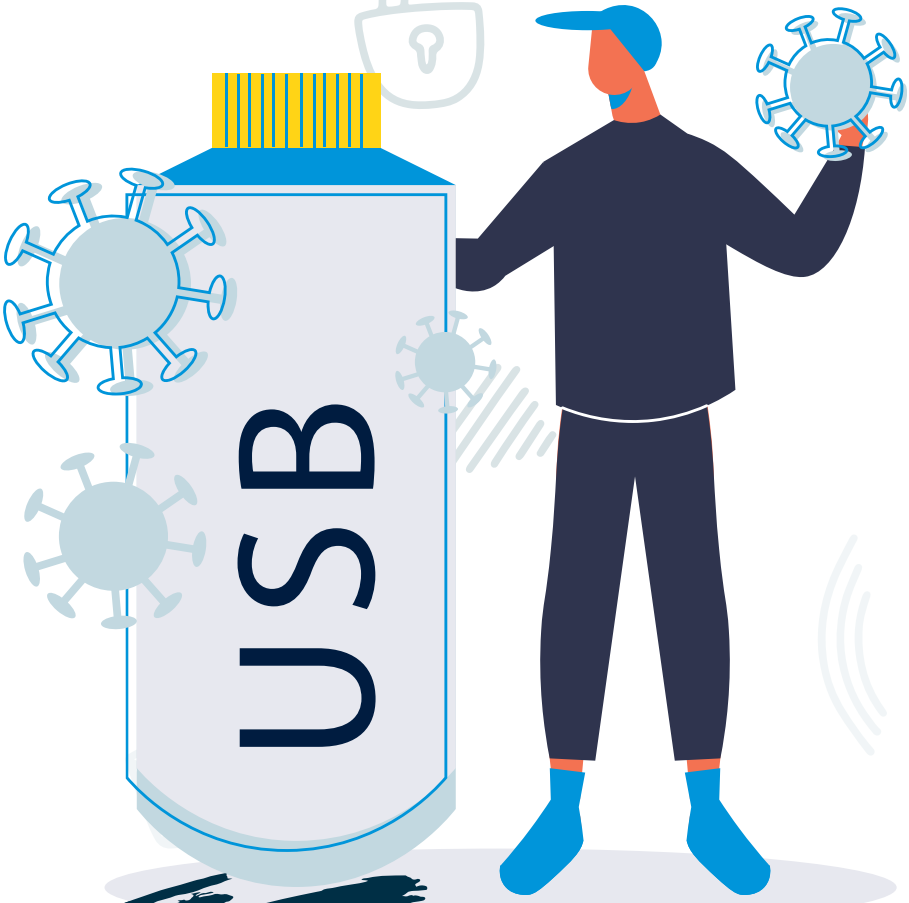
В България имаше кампании, които показват как дезинформацията се използва, за да се насърчават покупки на фалшиви лекарства или хранителни добавки. В международен план има примери как чрез TikTok или Reddit млади хора са привличани в групи, които пропагандират крайни идеи. Във всички случаи резултатът е един и същ – човек губи контрол върху собствения си избор.

Въздействието на дезинформацията е по-малко видимо, но също толкова разрушително. Тя не ти отнема паролата, но може да ти

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

отнеме увереността кое е вярно и кое не е. Може да те накара да похарчиш пари за нещо безсмислено, да се изолираш от приятели или да се въвлечеш в крайни идеи.

Затова е важно да развиваме „цифров имунитет“ – навика да питаме, да проверяваме и да се съмняваме в твърде хубавите обещания. Защото киберзаплахите не винаги идват като хак – понякога идват като дума, образ или история, която изглежда прекалено убедителна, за да е истина.



КИБЕРТОРМОЗ – КОГАТО АГРЕСИЯТА ПРЕМИНАВА В ДИГИТАЛНИЯ СВЯТ

Кибертормозът е съвременната форма на стария проблем с училищното насилие, но усилен многократно от силата на интернет. Той представлява умишлено и повтарящо се използване на електронни средства – социални мрежи, чатове, имейли, форуми – за да се нарани, унижи или изолира даден човек. Терминът включва широк спектър от действия: обидни съобщения, подигравателни коментари, публикуване на засрамващи снимки, създаване на фалшиви профили, изключване от онлайн групи или дори директни заплахи.

За разлика от традиционния тормоз, който често остава в училищния двор, кибертормозът няма граници. Той следва жертвата навсякъде – в стаята ѝ, в телефона, дори посред нощ. Затова въздействието е по-силно и дълготрайно.

Защо се случва? Мотивите на киберхулиганите

Причините един млад човек да се превърне в „киберхулиган“ са много и често се преплитат. Анонимността на интернет създава усещане за безнаказаност – когато няма директен очен контакт, е по-лесно да обидиш. Желанието за признание и влияние също играе роля: някои младежи тормозят онлайн, за да се почувстват по-силни, да получат внимание или да изглеждат „смешни“ пред групата.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Има и случаи, когато мотивацията е отмъщение – ученик, който се чувства обиден или унизен, използва дигиталната среда, за да „върне удара“. Други действат от скука или под влияние на връстници, без да осъзнават напълно последиците. А понякога кибертормозът се използва и като средство за печалба – изнудване за пари или лични снимки, които след това да се използват за финансов натиск.

„Не исках да бъда незабелязан в класа. Когато направих група с подигравателни снимки на един съученик, всички започнаха да ми пишат и да се смеят. Чувствах се важен.“
– споделя анонимен ученик в проучване.

Това изречение показва колко често причината е търсенето на внимание и фалшиво чувство за власт.

Кои са жертвите

Може да бъде всеки. Често жертвите са младежи, които се различават по нещо – външен вид, произход, интереси, социален статус. Но има и популярни ученици, които стават обект на завист. Понякога просто „да бъдеш на грешното място в грешното време“ е достатъчно – един спор в игра или социална мрежа може да прерасне в постоянен тормоз.

Жертвите обикновено изпитват срам и изолация. Много от тях не споделят с родители или учители, защото се страхуват от подигравки или наказание.

„Всеки ден се будех с мисълта какво ново ще напишат за мен в чата. Спрях да излизам навън, защото мислех, че всички ще ме гледат.“
– разказва 13-годишна ученичка.

Какво цели кибертормозът

Основната цел е да се унижи или да се подчини жертвата. Това може да е заради желание за доминация – извършителят иска да се почувства по-силен и значим. Друг път се цели изолация – жертвата да бъде изключена от група, за да се засили чувството ѝ на самота. В някои случаи целта е конкретна изгода: да се получат интимни снимки, достъп до акаунт или пари чрез изнудване.

Печалбата за киберхулиганите е краткотрайна – внимание, „слава“ в групата, усещане за контрол. Но последствията за жертвата често са тежки и дългосрочни – от загуба на самочувствие и доверие, до депресия и отказ от училище.

Какво печелят извършителите

Въпросът „какво печелят“ е ключов, защото показва защо феноменът не изчезва. Някои печелят внимание – лайкове, последователи, признание сред връстници. Други печелят усещането за власт. Трети печелят директна материална облага – чрез изнудване или разпространение на данни. Но всъщност всички губят – защото онлайн агресията разрушава доверието и общността.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)

Как да разпознаеш кибертормоза

- Получаваш многократни обидни съобщения или коментари.
- Създават се фалшиви профили на твое име с цел подигравки.
- Разпространяват се снимки или клипове без твое съгласие.
- Умишлено те изключват от онлайн групи и те унижават публично.

Причини за разпространението на кибертормоза

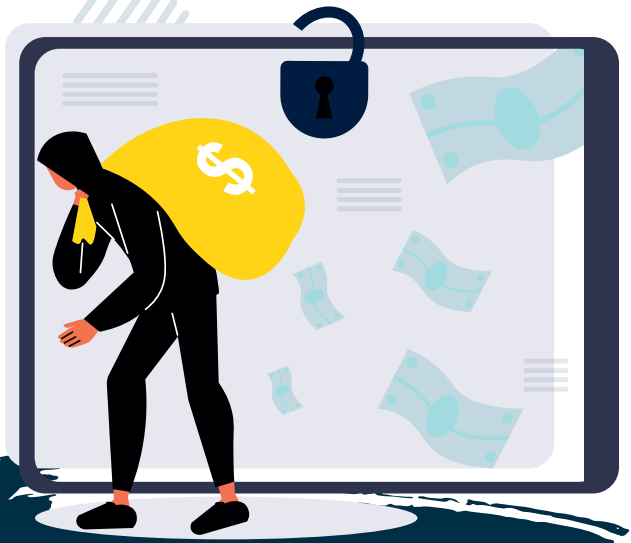
1. Анонимността – възможността да действаш скрито дава смелост на иначе несигурни хора.

2. Липсата на ясни граници – дигиталният свят е 24/7, което прави тормоза постоянен и изтощителен.

3. Груповото поведение – когато няколко души участват, отговорността се размива и никой не се чувства виновен.

4. Липсата на дигитална грамотност – и жертвите, и извършителите често не осъзнават последствията от действията си.

5. Слаб контрол от институциите – много случаи остават без реакция, защото не се докладват или се смятат за „детски проблем".



Въздействието върху жертвите

Последиците от кибертормоза не са само онлайн. Те проникват в живота на младите хора и могат да доведат до тревожност, депресия, проблеми с доверието, отказ от училище, а в крайни случаи – до саморазрушително поведение.

„Чувствах се, сякаш цял свят е срещу мен. Всеки лайк на подигравателна снимка беше като шамар."
– споделя 15-годишно момче.

Размисъл: защо трябва да говорим за това

Кибертормозът не е „шега" или „моментна прищявка". Това е феномен, който се корени в социалната среда, в културата на общуване и в начина, по който младите хора търсят признание. За да бъде намален, не е достатъчно само да блокираме профил или да сменим парола. Нужно е възпитание в уважение, емпатия и дигитална грамотност. Нужно е родители и учители да бъдат част от разговора – не като съдии, а като партньори.

Когато разберем причините – нуждата от внимание, отмъщението, скуката, чувството за безнаказаност – можем да мислим и за решения. А решението винаги започва с разговор: да чуем, да разберем и да подкрепим.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Какво казва законът

В България кибертормозът не е самостоятелно престъпление, но много от действията, които го съставят – обида, заплаха, изнудване, разпространение на лични данни или интимни снимки – попадат под Наказателния кодекс. Съществува и национална стратегия за борба с насилието над деца онлайн, а Комисията за защита на личните данни и ГДБОП приемат сигнали за сериозни нарушения. Училищата са длъжни да реагират при сигнали за тормоз и да осигурят подкрепа.

КАК ЕДНА АТАКА СЕ РАЗГРЪЩА (КИБЕРЗАПЛАХИТЕ В ДЕЙСТВИЕ) – ДВЕ ИСТОРИИ, ЕДНА ПОУКА

История първа: играта, която отне повече от точки

Владо е на 15 години и обича да играе онлайн с приятели. Една вечер получава съобщение в Discord: „Специална промоция – нови скинове безплатно! Само за ограничено време." Линкът изглежда истински – логото на играта, познат дизайн, таймер с обратно броене. Владо кликва и въвежда паролата си.

Това е началото на Cyber Kill Chain. Хакерите вече са минали през ***разузнаване*** (знаят, че Владо е фен на играта), ***подготовка*** (създават фалшивия сайт), и ***доставка*** (съобщението в Discord). Когато той въвежда данните си, идва ***експлоатацията*** – акаунтът му вече е компрометиран. След минути започват да се купуват предмети с вързаната към акаунта карта на баща му.

Владо разбира, че нещо не е наред, когато не може да влезе в профила си. Това е ***инсталацията*** – хакерите са сменили паролата и вече имат пълен контрол. После идва и ***контролът*** – профилът му изпраща същите фалшиви линкове към приятелите му. Накрая е ***действието върху целта*** – освен източените пари, Владо губи достъп до акаунт, в който е вложил години труд и постижения.

История втора: „гласът" от телефона

Докато Владо се опитва да възстанови профила си, неговата съученичка Нели преживява друг вид атака. Майка ѝ получава обаждане късно вечерта. На телефона звучи гласът на Нели: „Мамо, помогни ми, случи ми се нещо, прати пари на този номер." Гласът е треперещ, паникьосан – достатъчно, за да разтърси всяка майка.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Това е друг пример за Kill Chain. ***Разузнаване*** – хакерите намират открито видео с гласа на Нели в TikTok. ***Подготовка*** – използват изкуствен интелект, за да клонират гласа ѝ ***Доставка*** – телефонно обаждане към майката. ***Експлоатация*** – емоционалният натиск. За щастие, майката решава да провери – звъни директно на Нели и разбира, че тя е у дома и всичко е наред. Веригата е прекъсната навреме.

Какво ни казват тези истории

И двете ситуации показват, че кибератаката не е един момент, а верига от стъпки. Ако я прекъснеш рано – с малко внимание, с едно обаждане, с малко повече съмнение – можеш да предотвратиш големи щети.

Към децата: Внимавайте. Колкото по-рано забележите, че нещо е съмнително – странен линк, твърде хубава оферта, паникьосващо обаждане – толкова по-бързо можете да спрете атаката. Не е срамно да попитате или да споделите.

Към родителите: Разговаряйте с децата си за техния дигитален живот. Както питате как е минал денят им в училище, попитайте и какво ново са видели онлайн. Вашият опит може да помогне да разпознаете атака, която вече е започнала – странен имейл, подозрителна покупка, необичайно обаждане.

Към учителите: Рисковете вече са и в дигиталната среда. Бъдете до учениците си и там. Потърсете инструменти и обучения, за да можете да разпознавате ранни сигнали – промени в поведението, отказ от използване на акаунт, страх да се включат в чат. Превенцията и ранната реакция винаги намаляват щетите.

Извод

Cyber Kill Chain е като история – започва с дребни следи и завършва с щети. Но най-важното е, че веригата може да бъде прекъсната във всеки момент. Ако сме внимателни, ако разговаряме и ако действаме навреме, няма нужда историята да стига до финала, в който някой губи данни, пари или доверие.

ЗАКОНОДАТЕЛСТВОТО В РЕПУБЛИКА БЪЛГАРИЯ ОТНОСНО КИБЕРПРЕСТЪПЛЕНИЯТА

Какво е киберпрестъпление?

Киберпрестъпление е всяко престъпно деяние, извършено чрез използване на компютърни системи, мрежи или данни. Това включва нерегламентиран достъп до чужди акаунти, кражба на данни, създаване или разпространение на зловреден софтуер, измами чрез интернет, разпространение на дезинформация или детска порнография, както и кибертормоз, когато той прерасне в заплахи, изнудване или унижение с тежки последици.

В българското законодателство понятието е уредено основно в ***Наказателния кодекс*** (НК), като там са разписани различни видове „компютърни престъпления“ (чл. 319а–319ф).

Какво казва българският закон?

- ***Нерегламентиран достъп до компютърни данни (чл. 319а НК):*** Който без право влезе в компютърна система или мрежа, се наказва с ***лишаване от свобода до 3 години*** и глоба.

- ***Кражба, изтриване или промяна на данни (чл. 319б–319г НК):*** Наказанията могат да достигнат ***до 5 години лишаване от свобода***, особено ако е засегнато голямо количество информация или се причинят значителни вреди.

- ***Разпространение на вируси или зловреден софтуер (чл. 319д НК):*** Лишаване от свобода до 3 години и глоба до 3 000 лв.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

- ***Измама чрез използване на компютърни данни (чл. 212а НК):*** Когато някой получи неправомерна облага чрез компютърна измама – наказанието може да стигне ***до 8 години лишаване от свобода.***
- ***Разпространение на порнографски материали с непълнолетни (чл. 159 НК):*** Това е тежко престъпление, наказуемо със затвор до 6 години и високи глоби.

Мерките в закона и превенция

Освен наказания, в България има и институции и механизми за защита:

- ***ГДБОП (Главна дирекция „Борба с организираната престъпност“)*** – приема сигнали за киберпрестъпления.

- ***Комисия за защита на личните данни (КЗЛД)*** – гарантира правата на гражданите, ако техни данни са използвани неправомерно.

- ***Национален център за безопасен интернет*** – предлага консултации и подкрепа на деца и родители.

Защо това е важно за младите хора?

Много често кибертормозът или „невинното любопитство“ – като опит да хакнеш паролата на приятел, да влезеш в чужд акаунт или да споделиш лична информация за някого – се възприемат като игра. Но законът не прави разлика между „на шега“ и „сериозно“. Дори едно действие, извършено с любопитство, може да остави следа в съдимостта и да провали бъдеща кариера.

„Исках само да видя какво ще стане, ако вляза в чуждия акаунт. Не мислех, че е толкова сериозно.“ – това е често срещано оправдание. Но реалността е, че в очите на закона това е престъпление.

Млад човек, който днес е „просто хакнал“ нечий профил, утре може да не успее да учи в чужбина, да работи в голяма фирма или да получи работа, свързана с доверие и отговорност.

Изборът е в твоите ръце – светлата или тъмната страна

Точно както във филмовите истории, всеки млад човек стои пред избор.

- От едната страна е ***Светлината*** – дигитална култура, уважение, умения да защитаваш себе си и другите. Това е пътят на „джедаите на киберсигурността“ – хората, които пазят общността и използват знанията си, за да изграждат доверие и сигурност.

- От другата страна е ***Тъмнината*** – любопитство, превърнато в злоупотреба, кибертормоз, измами, злоупотреба с чужди данни. Това е пътят на „Ситите“ – хора, които използват уменията си, за да манипулират и рушат.

Твоят избор определя не само какъв ще бъдеш онлайн, но и какъв ще бъде твоят живот извън екрана. Законът може да те накаже, но истинската последица е загубеното доверие – на приятели, семейство, бъдещи работодатели.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

ПРАКТИЧЕСКИ СТЪПКИ ЗА ЗАЩИТА

1. Силна и уникална парола

Паролата е като ключа на дома ти – ако е тънка тел, всеки може да влезе. Ако е здрава и уникална, пази всичко вътре. Силната парола съдържа букви (малки и големи), цифри и символи. Колкото е по-дълга – толкова е по-трудна за отгатване. Най-важното е никога да не използваш една и съща парола за всички акаунти. Ако Instagram бъде пробит, не искаш хакерът да получи достъп и до мейла ти.

- ***Предпазва от:*** хакване чрез отгатване или пробив от друг сайт.
- ***Време:*** 5–10 минути.
- ***Нужно:*** идея за фраза („АзОбичамКниги!2024“) или приложение за пароли.

2. Критично кликване

В интернет най-опасното е да кликнеш без да мислиш. Вирусите и измамите рядко влизат сами – ние им отваряме вратата. Затова винаги си задай въпроса: „Кой печели, ако натисна този линк?“ Ако линкът идва от непознат, ако има странен адрес, ако обещава твърде хубаво нещо – вероятно е измама.

- ***Предпазва от:*** фишинг, рансъмуер, кражба на акаунти.
- ***Време:*** 2 секунди размисъл.
- ***Нужно:*** навик да спираш за миг и да проверяваш.

3. Настройки за поверителност

Социалните мрежи са като сцена – ти решаваш кой да гледа. Ако профилът ти е отворен за всички, всеки може да види снимките, местоположението и приятелите ти. Прегледай настройките в TikTok, Instagram, Facebook – ограничи кой може да вижда публикациите ти и кой може да ти пише. Това е малка стъпка, която прави огромна разлика.

- ***Предпазва от:*** кибертормоз, stalk-ване, фалшиви профили.
- ***Време:*** 15–20 минути.
- ***Нужно:*** време да разгледаш настройките.

4. Двуфакторна автентикация (2FA)

Представи си, че дори ако някой вземе ключа от дома ти, трябва да има и втори ключ, за да влезе. Това е 2FA – освен парола, системата иска и код, който идва по SMS или в приложение. Така хакерът няма как да влезе, дори да е откраднал паролата ти.

- ***Предпазва от:*** хакване на акаунти след изтичане на парола.
- ***Време:*** 10–15 минути настройка.
- ***Нужно: с***мартфон и приложение като Google Authenticator.

5. Сподели, ако нещо те тревожи

Най-голямата грешка е да мълчиш. Ако усетиш, че нещо не е наред – странни съобщения, изнудване, обиди – не стой сам в това. Кажи на родител, учител или приятел. Колкото по-рано се говори, толкова по-бързо може да се реагира. Мълчанието е най-добрият съюзник на хакерите и тормозещите.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

- ***Предпазва от:*** задълбочаване на проблема, емоционален стрес.
- ***Време:*** зависи, но помощта идва веднага щом споделиш.
- ***Нужно:*** смелост и доверие към някой близък.

Практически стъпки за защита (средно ниво)

6. Обновявай устройства и приложения

Телефонът или лаптопът ти не е само машина – това е твоята дигитална врата. Когато системата или приложенията имат пропуски, хакерите ги използват. Затова производителите редовно пускат „ъпдейти", които запушват тези дупки. Ако игнорираш известията „Има нова версия", всъщност оставяш вратата си открехната.

- ***Предпазва от:*** нови уязвимости, рансъмуер, зловредни приложения.
- ***Време:*** 10–30 минути (зависи от устройството и връзката).
- ***Нужно:*** да не натискаш „Напомни ми по-късно", а да позволиш актуализацията.

7. Бъди внимателен какво споделяш

Интернет никога не забравя. Снимка, която днес изглежда забавна, утре може да се използва за подигравка или изнудване. Когато качваш съдържание, си задай въпроса: „ОК ли съм това да остане тук завинаги и да го видят и хора, които не познавам?" Локацията, училището, дори снимка на стаята ти са информация, която някой може да използва.

- ***Предпазва от:*** сексторшън, кибертормоз, кражба на самоличност.
- ***Време:*** нула минути – просто мисли преди пост.
- ***Нужно:*** самоконтрол и осъзнатост, че „приятели онлайн" не винаги са истински приятели.

8. Информираност за нови измами

Киберзаплахите се променят толкова бързо, колкото и модните трендове. Днес е фишинг имейл, утре – дийпфейк видео. Ако не знаеш за тях, е по-лесно да се подлъжеш. Затова е полезно веднъж седмично да отделяш малко време да четеш за актуалните измами. Може да е сайтът на ГДБОП, ENISA или Центърът за безопасен интернет.

- ***Предпазва от:*** нови форми на измами, AI-имитации, непознати трикове.
- ***Време:*** 5 минути седмично.
- ***Нужно:*** интерес и любопитство да знаеш как работи светът около теб.

Практически стъпки за защита (експертно ниво)

9. Мениджър на пароли

Представи си кутия със сто ключа – един за всяка врата. Ако се опиташ да ги носиш в джоба си, ще ги изгубиш. Мениджърът на пароли е като сейф – пази всичките ти пароли на едно място и ги отключва с една главна парола. Това ти позволява да използваш различни, силни и уникални пароли за всеки акаунт, без да ги помниш наизуст.

- ***Предпазва от:*** повторно използване на пароли, забравяне, кражба.
- ***Време:*** около 30 минути първоначална настройка, после работи автоматично.
- ***Нужно:*** доверие към избрано приложение (1Password, Bitwarden, KeePass).

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

10. VPN (виртуална частна мрежа)

Когато се свързваш към интернет от кафене, училище или обществен Wi-Fi, твоите данни могат да бъдат прихванати. VPN е като тунел – криптира връзката ти и скрива IP адреса, така че никой да не може да наднича какво правиш. За младежите, които пътуват или учат онлайн, това е допълнителен щит.

- ***Предпазва от:*** проследяване, кражба на данни в публични мрежи.
- ***Време:*** 15 минути за настройка.
- ***Нужно:*** приложение за VPN (платено или внимателно подбрано безплатно).

11. Хардуерен токен за 2FA

Най-високото ниво на защита е да имаш „физически ключ“ за акаунтите си – малко устройство (USB/NFC), което вкарваш или доближаваш до телефона, за да потвърдиш влизането. Това е като дигитален катинар, който почти никой хакер не може да прескочи. Все по-често университети, компании и дори социални мрежи предлагат тази опция.

- ***Предпазва от:*** дори най-усъвършенствани атаки срещу акаунти.
- ***Време:*** 10–15 минути настройка на акаунт.
- ***Нужно:*** закупуване на токен (например YubiKey).

12. Мониторинг за изтичане на данни

Може би вече някъде в интернет циркулират твои пароли – от пробиви в сайтове или игри. Има услуги, които проверяват дали имейлът или паролата ти е „изтекла“. Регистрираш се, и ако твоите данни се появят в публични бази, получаваш известие. Това е като аларма, която ти казва, че трябва веднага да смениш парола.

- ***Предпазва от:*** повторна употреба на вече изтекли пароли.
- ***Време:*** 5 минути за регистрация, после автоматично следене.
- ***Нужно:*** имейл и достъп до услуга като HavelBeenPwned или подобни.

13. Сегментиране на акаунти

Не слагай всички яйца в една кошница. Много младежи използват един имейл за всичко – училище, игри, социални мрежи. Ако този имейл бъде пробит, целият им дигитален живот е изложен на риск. По-добре е да разделяш – един имейл за училище, друг за игри, трети за важни акаунти като онлайн банкиране. Това е като да имаш отделни ключове за дома, колата и училищния шкаф.

- ***Предпазва от:*** масови последствия при пробив в един акаунт.
- ***Време:*** 1–2 часа за създаване и настройка.
- ***Нужно:*** нови имейл адреси и организация.

14. Цифрова хигиена като култура

Най-високото ниво на защита не е конкретна технология, а начин на мислене. Това е съчетание от всички горни стъпки и постоянен навик да подхождаш осъзнато към интернет. Да мислиш преди да постнеш. Да проверяваш източници. Да си спокоен, че имаш резервни копия и защита. Това е като лична култура – част от ежедневието, която се изгражда с време и практика.

- ***Предпазва от:*** почти всички модерни заплахи.
- ***Време:*** постоянен процес.
- ***Нужно:*** навици, подкрепа от родители и учители, желание да учиш и да се пазиш.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

РАЗДЕЛ II – УМНИ ХОДОВЕ ОНЛАЙН

Провери се колко рисков играч си в интернет

Всеки ден правим десетки избори онлайн – коя парола да ползваме, дали да приемем нов приятел, дали да кликнем на линк. Някои от тези решения са безопасни, други ни излагат на сериозен риск. С този тест можеш да се самооцениш и да видиш къде се намираш в скалата на дигиталната сигурност.

Как да попълниш

Отговори честно на въпросите с „Да“ или „Не“. Записвай си точките:

- ***1 точка*** – за по-леките рискове.
- ***3 точки*** – за средните рискове.
- ***5 точки*** – за най-опасните поведения.

В края събери всички точки и виж какъв е твоят дигитален профил.

Въпроси

1. Използваш ли една и съща парола за повече от един акаунт? (5 т.)
2. Имаш ли парола, която е по-къса от 8 символа? (5 т.)
3. Споделял ли си някога паролата си с приятел? (3 т.)
4. Записваш ли пароли на листчета или в бележника на телефона без защита? (3 т.)

5. Натискал ли си линк от непознат човек в социална мрежа? (5 т.)
6. Използваш ли обществен Wi-Fi без VPN? (3 т.)
7. Приемаш ли покани за приятелство от хора, които не познаваш лично? (3 т.)
8. Проверяваш ли настройките си за поверителност поне веднъж годишно? (ако „Не“ – 1 т.)
9. Споделяш ли редовно местоположението си онлайн? (3 т.)
10. Публикувал ли си снимки или лични данни, които по-късно си съжалявал? (3 т.)
11. Проверяваш ли дали сайтът има „https://“ преди да въведеш данни? (ако „Не“ – 1 т.)
12. Имаш ли включена двуфакторна автентикация в социалните мрежи? (ако „Не“ – 5 т.)
13. Обновяваш ли операционната система и приложенията си редовно? (ако „Не“ – 3 т.)
14. Ползваш ли различни имейли за училище, игри и лични акаунти? (ако „Не“ – 3 т.)
15. Имаш ли навика да кликваш „Съгласен съм“ без да четеш условията? (1 т.)
16. Проверяваш ли новините за актуални киберизмами? (ако „Не“ – 1 т.)
17. Свалял ли си приложение от непознат или съмнителен сайт? (5 т.)
18. Разговаряш ли с родител или учител, ако нещо онлайн те тревожи? (ако „Не“ – 3 т.)
19. Имаш ли резервни копия на най-важните си файлове? (ако „Не“ – 3 т.)
20. Използваш ли мениджър на пароли или записваш всичко „на ръка“? (ако второто – 1 т.)

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Скала на резултатите

- ***0–10 точки:*** Ти си „дигитален джедай“ – внимателен, информиран и в повечето ситуации знаеш как да се пазиш.
- ***11–30 точки:*** Имаш добри навици, но и няколко слаби места. Малки промени могат да те направят много по-сигурен.
- ***31–60 точки:*** Рисков играч си. Често пренебрегваш основни правила за сигурност. Нужно е да промениш поведението си.
- ***61+ точки:*** Висок риск – дигиталният ти живот е като врата без ключалка. Започни веднага с лесните стъпки от предишния раздел.

Силните пароли и как да ги измислиш

Паролата е като личния ти ключ към дигиталния свят. Тя пази не само профила ти в Instagram или TikTok, но и спомените в облака, разговорите с приятели, понякога дори парите на родителите ти, ако акаунтите са свързани. И както никой не би оставил дома си отключен, така и в интернет паролата трябва да бъде здрава, сложна и само твоя.

Повечето хора правят една и съща грешка – избират лесни пароли. Нещо като „mimi2008“ или „pesho123“. Лесни са за запомняне, но са и първото, което ще опита хакерът. Такива пароли могат да се отгатнат за секунди.

Силната парола, от друга страна, изглежда сложна и дълга. Но това не означава, че е невъзможна за запомняне. Тайната е да използваш ***фрази***, а не отделни думи. Например, ако обичаш книгите и си роден през 2008, можеш да направиш парола като „AzObichamKnigi!2008“. Изглежда сложна, но в главата ти е лесна: „Аз обичам книги!“

Друг трик е да комбинираш думи, които нямат връзка помежду си. редстави си парола като „Panda!S#umr42Limon“. За всеки друг това е хаос от символи, но за теб може да е „панда, шумър, лимон“ – три произволни образа, които мозъкът запомня по-лесно.

Ако искаш да си още по-сигурен, можеш да използваш ***мениджър на пароли***. Това е приложение, което пази всичките ти пароли на сигурно място и ти позволява да използваш уникална комбинация за всеки акаунт. Така дори ако някой сайт изтече данни, останалите профили ти остават защитени.

Някои онлайн инструменти предлагат генератори на пароли. Те могат да ти създадат случайна комбинация като „F7!xkN2#LmZ8“. На пръв поглед тя изглежда невъзможна за помнене, но мениджърът я пази вместо теб.

Истината е проста: силната парола е бариера, която прави атаката толкова трудна, че хакерите обикновено избират по-лесна жертва. Затова, когато се чудиш каква парола да сложиш, помисли за нещо, което е уникално за теб, но невидимо за останалите – фраза, комбинация от думи, спомен, който само ти разбираш.

Чеклист: Силни пароли

- Паролата е ***поне 12 символа.***
- Съдържа ***букви (главни/малки), цифри и символи.***
- Използвам ***различна парола за всеки акаунт.***
- Мога да измисля парола чрез ***фраза*** („AzObichamKnigi!2024“).
- Не споделям пароли с приятели.
- Ако не мога да запомня – използвам ***мениджър на пароли.***
- Никога не записвам пароли „на листче“.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Мини игра: „Стаята с петте пароли“

Влизаш в дигитална стая. Пет врати, зад всяка стои младеж със своята история. Ако отгатнеш паролата му, вратата се отваря. Но внимавай – лесните пароли ще те върнат в капан, а само най-силните ще ти позволят да излезеш.

1. Историята на Петър

Петър е на 13 години. Всички го наричат Реро, а в отбора по футбол винаги носи фланелка с номер 7. Когато си прави профил в TikTok, не иска да мисли много и просто избира парола, която съчетава прякора му и любимия му номер. Той вярва, че никой няма да се сети – но дали е така?

Как мислиш, каква е неговата парола?

Подсказка: Реро + 7

2. Историята на Мая

Мая е на 15 и обожава своята котка Лили. Толкова много, че почти всички снимки в Instagram са с нея. За парола тя решава да използва името на котката и годината, когато я е взела у дома – 2021. В нейните очи това е уникално, но реално е нещо, което всеки, който я следи онлайн, може да отгатне.

Коя е нейната парола и силна ли е според теб?

3. Историята на Иван

Иван е геймър и прекарва часове в Minecraft. Любимото му е да строи „замъци“. За да не си забрави паролата, решава да използва самото име на играта, а за сигурност добавя „123“ отзад. Той е убеден, че това е „кодиране“ – но в света на киберсигурността подобна комбинация е сред най-лесните за разбиване.

Можеш ли да познаеш паролата му?

4. Историята на Ели

Ели е на 16. Тя е от онези хора, които четат книги нощем, дори когато трябва да учат. За парола решава да използва любимата си фраза: „Обичам да чета нощем“. Но тя е по-креативна – превръща някои букви в цифри („о“ става „0“, „е“ става „3“), добавя удивителна и прави своята комбинация по-трудна за отгатване. Това вече е истинска техника, която наричаме кодиране на символи.

Как мислиш, как изглежда паролата на Ели?

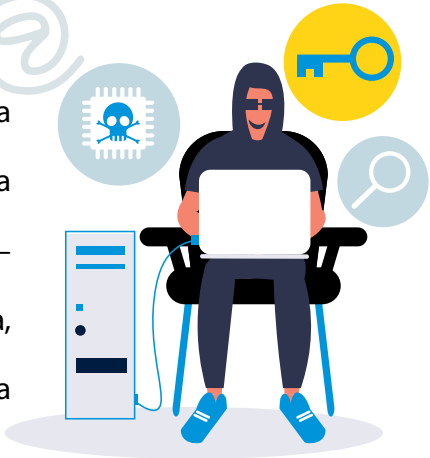
5. Историята на Георги

Георги е на 17 и мечтае да стане програмист. Той вече знае, че дори най-креативните пароли могат да бъдат разбити, ако се използват отново и отново. Затова решава да си инсталира мениджър на пароли. Приложението генерира за него случайна комбинация – дълга, пълна с букви, цифри и символи, която никой не би могъл да познае. Георги няма нужда да я помни – софтуерът я пази вместо него. Това е най-сигурната стратегия.

Как мислиш, защо тази парола е почти невъзможна за разбиване?

Отговори

1. Петър → Pepo7 Слаба – очевидна комбинация.
2. Мая → Lili2021 Слаба – лична информация, видима онлайн.
3. Иван → Minecraft123 Слаба – популярна дума + последователност.
4. Ели → 0bichamCh3ta! Силна – фраза, кодиране на букви, добавен символ.
5. Георги → X!9v%kLp#72n Много силна – генерирана, уникална и случайна.



Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Извод

Паролите са огледало на нашите навици. Колкото повече лични данни влагаме в тях, толкова по-лесно някой може да ги отгатне. Когато използваме креативност, символи, кодиране и мениджъри на пароли, вратата към нашия дигитален живот става почти непробиваема.

Поверителност в социалните мрежи – практическо ръководство

Поверителността онлайн означава ти да решаваш кой, какво и кога вижда за теб. Тя не е „една настройка и готово", а навик: от това какво публикуваш, през това кой може да ти пише, до това как си защитил профила при загубен телефон. Платформите добавят все повече инструменти за тийнейджъри и семейства — важно е да ги включиш и да ги преглеждаш редовно.

TikTok – какво да включиш (за тийн акаунти и семейства)

- ***Family Pairing (родителски контрол):*** позволява на родител/настойник да свърже своя профил с този на тийн и да управлява време на екрана, директни съобщения, думи за филтър на съдържание и др. Активира се от Profile ⟶ Menu ⟶ Settings and privacy ⟶ Family Pairing. Новите опции включват и ***блокиране на конкретни акаунти*** от страна на родителя.
- ***Teen privacy defaults:*** TikTok има отделни страници с указания за поверителност и безопасност за <18 г.; при Family Pairing част от настройките се управляват централно от родителя.
- ***Ако профилът е компрометиран:*** официалните стъпки за разпознаване и възстановяване (смяна на парола, 2FA, преглед на сесии, докладване).

Защо сега? Регулаторни действия срещу TikTok за защита на деца показаха, че настройките им се променят и затягат — стой „в крак" с актуалните опции.

Instagram – „Teen accounts“, Supervision и лична сигурност

- ***Teen Accounts (подразбиращи се по-поверителни профили):*** профилите на тийнейджъри са private by default, с ограничения за кой може да изпраща съобщения/тагва и по-строг филтър на чувствително съдържание. За <16 г. често е нужно родителско одобрение за разхлабване на настройките.
- ***Family Center / Supervision:*** доброволно „супервижън“ между родител и тийн — виждаш време в приложението, можеш да зададеш лимити, да преглеждаш настройките и да ограничиш кой може да контактува. Стартира се през Settings -> Supervision.
- ***Практика:*** включи 2FA (препоръчително чрез приложение, не само SMS) и прегледай „Recognized devices“ в Account Center; махни остарели устройства.

Facebook – бърза проверка на поверителността и сигурността

- ***Privacy Checkup & Security features:*** прегледай кой вижда публикациите ти, активирай ***login alerts*** и t***wo-factor authentication,*** провери активните сесии/устройства и ги излез. Facebook
- ***Съвет:*** прегледай „Recognized devices“ и изключи доверие към стари телефони/компютри (след промени в 2FA логиката някои устройства остават „доверени“ по подразбиране).
- ***Ръководства 2025:*** добри практики и стъпка по стъпка примери за скриване на публичната информация.

YouTube – „Supervised experiences“ и контрол на съдържанието

- ***Supervised experience:*** за деца и по-малки тийн — профили с родителски контрол и ***нива на съдържание*** (Explore/Explore more/ Most of YouTube). Настройва се през профила на родителя; може да се променя по всяко време.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Бърз ориентир: какво да включа (младеж / родител / учител)

- ***Младеж:*** личен профил ***Private,*** 2FA с приложение, филтри за коментари/думи, ограничени съобщения (само от последвани), редовен преглед на активни устройства.
- ***Родител:*** активирай ***Family Pairing*** (TikTok) / ***Supervision*** (Instagram), блокирай конкретни акаунти при нужда, преглеждай известия за нови качвания и лимити за време.
- ***Учител:*** води „проверка на настройките“ като класно упражнение 2–3 пъти в годината; използвай официалните ръководства (UK Safer Internet, Internet Matters) за чеклист и език към тийнейджъри.

Мини ръководства по платформи (само най-важното)

TikTok (за тийн и семейства)
1. Profile → Menu → Settings and privacy → Family Pairing (свързване и управление).
2. Privacy → Suggest your account to others (ограничи), Direct messages (само „No one“/„Friends“), Comment filters (ключови думи), Private account – ON.

Instagram
1. Settings → Privacy → Account Privacy = Private; Messages = само от „people you follow“.
2. Settings → Security → Two-Factor Authentication (приложение).
3. Settings → Supervision (за семейства).
4. Account Center → Password and security → Recognized devices (почисти).

Facebook
1. Privacy Checkup → кой вижда публикации/стара активност/списък с приятели.
2. Settings → Security and login: 2FA, Get alerts about unrecognized logins, преглед на Where you're logged in.

YouTube
1. Настрой Supervised experience и ниво на съдържание; преглеждай „watch & search history“, Restricted Mode на устройствата в училище/дома.

Истории за мотивация: „Преди и след“

Instagram: „Хакнат профил, върнат с помощ и нови настройки“ — потребител споделя как е изгубил достъп (сменена парола и включено 2FA от нападателя), после през поддръжката си връща акаунта и включва свои 2FA, сменя имейла и преглежда доверените устройства. Извод: провери 2FA и „Recognized devices“ веднага.

Facebook: „Хакер включи 2FA вместо мен“ — серия теми в r/facebook описват точно този сценарий; решението е през официалното възстановяване + проверка на устройства и доклади към поддръжката. Извод: активирай 2FA предварително и пази резервни кодове.

Практика от медиите — дори опитни хора се хващат: реален случай с компрометирана FB страница довежда до измама с хиляди долари сред приятели. Извод: сигнализирай близките веднага щом загубиш достъп; не приемай „инвестиционни“ оферти от приятели без проверка.

TikTok: „Как да реагираш при съмнение за хак“ — официалната помощ описва точни стъпки и как да разпознаеш признаци (смени, изтрити клипове, непознати ДМ-и). Извод: имай план: парола -> 2FA -> сесии -> доклад.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Финален съвет

Прави ***сезонна проверка*** на поверителността: есен/пролет. 15 минути на профил са достатъчни да включиш частен профил, 2FA, филтри на съобщенията/коментарите и да изчистиш стари устройства. Тези навици, плюс разговорите у дома и в клас, са най-силната защита — превенцията и ранната реакция винаги намаляват щетите.

Бисквитената къща и дигиталните „cookies“

Помните ли как Хензел и Гретел попадат на къща от бисквити и захар? Всичко изглежда примамливо и вкусно, но зад фасадата се крие капан. В интернет „бисквитките“ работят по сходен начин. Те са малки файлове, които сайтовете записват в браузъра ти. На пръв поглед помагат – запомнят входа, държат продуктите в количката ти, пазят езиковите предпочитания. Но зад тях стои и друга страна – събиране на данни за твоите навици, интереси и поведение онлайн.

Когато натискаш „Съгласен съм“, ти разрешаваш на сайта да постави различни видове бисквитки:

- ***Задължителни*** – нужни, за да работи сайтът (например, за да не излезеш от профила си при всяко кликване).
- ***Статистически*** – следят колко често посещаваш дадена страница, за да може сайтът да се подобрява.
- ***Маркетингови*** – проследяват те от сайт на сайт и изграждат профил на интересите ти, за да ти показват целеви реклами.

Истории за мотивация

Онлайн магазин и „кукичките“: Потребители забелязват, че след като са търсили обувки в един сайт, на следващия ден реклами за същите модели ги следват в YouTube и Facebook. Те разбират, че това е резултат от маркетинговите бисквитки и започват да избират опцията „Reject non-essential cookies“, когато имат възможност.

„Кликнах без да мисля“: Студент споделя, че винаги натиска „Приемам всички“, за да влезе по-бързо в сайтове. След време започва да се притеснява – защо получава реклами за теми, които е обсъждал само в чатове? Тогава научава, че голяма част от поведението му е следено чрез бисквитки и решава да промени настройките на браузъра си, за да блокира трети страни.

Регулаторна намеса: В Европа някои компании бяха глобени, защото улесняваха само приемането, но не и отказа на бисквитки. След обществен натиск и медийни реакции те бяха принудени да включат бутон „Отказвам“ още в банера. Потребителите споделят, че оттогава се чувстват по-свободни да избират.

Какво да запомниш

Бисквитките не са непременно лоши – те улесняват работата на интернет. Но когато приемаш всички без да четеш, отваряш вратата на маркетингови компании и непознати страни, които започват да знаят повече за теб, отколкото си мислиш. Винаги избирай разумно: „Необходими“ – да, „Маркетингови“ – само ако искаш.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

АКО НЕЩО СЕ СЛУЧИ – КАКВО ДА НАПРАВЯ?

Колкото и внимателни да сме, никой не е застрахован от инциденти в интернет. Важното е в труден момент да запазим самообладание и да предприемем правилните стъпки. Ето кратък чеклист с действия, които да следвате, ако станете жертва на кибертормоз, онлайн изнудване или друг опасен инцидент:

1. Не изпадайте в паника и не отговаряйте с агресия. Първата реакция при онлайн нападка или заплаха е много важна. Опитайте се да запазите спокойствие и не пишете веднага гневен отговор. Не се поддавайте на провокацията – ако отвърнете на обидата с обида, ситуацията може да се влоши и конфликтът да ескалира. Например при кибертормоз, грубите ви реплики само „наливат масло в огъня" и радват тормозещия. По-добре не отговаряйте на злонамерени съобщенияsacp.government.bg.

2. Съберете доказателства (направете скрийншоти). Не изтривайте веднага обидните чатове, снимки или имейли. Направете екранни снимки (screenshots) на съответния разговор или съдържание – те ще послужат като електронно доказателство за случилото cesacp.government.bg. Запазете и други потенциални доказателства (например имейли, линкове, логове). Тази информация ще е полезна, когато подадете оплакване или сигнал.

3. Блокирайте нарушителя и прекратете контакта. Изолирайте източника на тормоз или злоупотреба. Ако конкретен потребител ви обижда или заплашва, блокирайте го (чрез функцията

Block/Блокиране в приложението или сайта)sacp.government.bg. Преустановете всякаква директна комуникация с този човек. Ако получавате заплашителни обаждания или SMS-и, добавете и номера в списъка с блокирани на телефона си. Важното е да прекратите контакта възможно най-скоро, след като сте запазили нужните доказателства.

4. Споделете с възрастен, на когото имате доверие. Не оставайте сами с проблема – веднага потърсете съдействие. Разкажете за случилото се на родител, настойник или учител. Те могат да ви помогнат да прецените ситуацията и да предприемете по-нататъшни стъпки. Много деца вече осъзнават колко е важно това – над 65% от учениците у нас биха потърсили помощ точно от родителите си относно онлайн безопасносттаsacp.government.bg. Не се притеснявайте, няма да ви винят – възрастните искат да ви защитят. Ако смятате, че и друг ваш връстник е в опасност, поговорете и с него и го насърчете да сподели с доверен възрастен.

5. Подайте сигнал и потърсете професионална помощ. Не се колебайте да докладвате за инцидента на съответните органи или платформи. Ако проблемът е в социална мрежа или сайт, използвайте вградената функция за "Report/Докладване" – администраторите може да премахнат обидното съдържание или да блокират нарушителя. Можете да подадете сигнал и до Националния център за безопасен интернет, например през онлайн формата на сайта имsacp.government.bg. Ако ситуацията е сериозна (например получавате заплахи, предложение за среща или сексуален тормоз), обърнете се към ГДБОП – отдел "Киберпрестъпност". Изпратете им имейл на с подробно описание на инцидента, приложете скрийншоти/снимки и посочете своите имена и телефон. Може да се обадите и на телефон 0885 525 545 – директна линия за киберпрестъпления към МВРcybersecbg.org. Полицията и специализираните органи са там,

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

за да ви помогнат – не се страхувайте да ги потърсите, ако сте жертва на нещо наистина опасно.

6. Обадете се на телефон за помощ и подкрепа. След неприятен инцидент в интернет е нормално да се чувствате разстроени, уплашени или объркани. Освен на близките си, можете да разчитате и на професионална подкрепа. В България денонощно работи Национална телефонна линия за деца – 116 111, на която можете да споделите анонимно и да получите съвет от психолог. Все повече младежи се доверяват на тази услуга – през 2024 г. делът на децата, които биха потърсили консултантите на 116 111, нараства до 21.6% (в сравнение с 13.4% през 2023 г.)sacp.government.bg. Не се колебайте да се обадите на 116 111 или на друг горещ телефон за помощ, ако имате нужда – разговорът може да ви помогне да преодолеете стреса и да намерите решение на проблема.

Източници: Държавна агенция за закрила на детето (ДАЗД); Национален център за безопасен интернет (Safenet.bg); Главна дирекция „Борба с организираната престъпност“ (ГДБОП-МВР); Комисия за защита на личните данни (КЗЛД); УНИЦЕФ България

НДИГИТАЛНАТА РЕПУТАЦИЯ – ТВОЕТО НОВО CV

Представи си, че в интернет вървиш по снежна пътека. Всеки пост, всяка снимка, всеки коментар е стъпка, която оставя отпечатък. Дори когато се опиташ да се върнеш и да изтриеш следата си, някой вече може да я е снимал. Тази пътека наричаме дигитална следа – тя се състои от всичко, което оставяш след себе си онлайн.

Дигиталната репутация е начинът, по който тази следа се вижда от другите. Ако преди години работодателите или университетите гледаха само хартиено CV, днес те първо ще напишат твоето име в Google. Това, което излезе там – профили, публикации, снимки от игри, коментари в Reddit или форум – става твоето ново CV.

Как се управлява и поддържа дигиталната репутация

1. Направи си самооценка. Потърси името си в търсачки – Google, DuckDuckGo или Bing. Виж какво излиза на първата страница. Ако ти не харесваш как изглежда, значи е време да се погрижиш.

2. Изчисти ненужното. Прегледай старите си постове, снимки или коментари. Понякога това, което е било смешно на 14, изглежда напълно различно на 18.

3. Създай положителен образ. Споделяй постижения, доброволчество, проекти, изкуство, спорт. Така репутацията ти не само ще е „чиста“, но и ще говори добре за теб.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

4. Пази бъдещето. Помисли преди всяка публикация: бих ли искал учителят ми, бъдещият ми работодател или моите родители да видят това?

Какво можеш да провериш онлайн

Твоят дигитален отпечатък не е само във Facebook или TikTok – той се разпростира в Google, Reddit, стари форуми, гейминг профили и още много места. Ето десет безплатни и достъпни ресурса, с които можеш да провериш какво „знае“ светът за теб:

1. Google Search (google.com) – въведи името си и виж какво излиза на първите страници.

2. DuckDuckGo (duckduckgo.com) – търсачка, която не проследява потребителите и показва често различни резултати.

3. Startpage (startpage.com) – извежда резултати от Google, но без да събира лични данни.

4. Ecosia (ecosia.org) – екологична търсачка, която също дава различна перспектива върху твоето име онлайн.

5. Have I Been Pwned (haveibeenpwned.com) – провери дали имейлът ти е бил част от изтичане на данни.

6. Google Alerts (google.com/alerts) – създай известие, за да получаваш имейл, когато името ти се появи някъде ново.

7. Social Searcher (social-searcher.com) – позволява търсене на публични публикации в социални мрежи.

8. Reddit Search (reddit.com/search) – проверка на твои постове или коментари в Reddit.

9. TinEye (tineye.com) – търси твои снимки в интернет, за да разбереш дали се използват на други места.

10. Wayback Machine (archive.org/web) – показва стари версии на сайтове, където може да присъства твоя информация, дори вече да е изтрита.

Правото да бъдем забравени

Важно е да знаеш, че в Европа имаме специална защита: ***правото да бъдеш забравен*** (чл. 17 от GDPR). Това означава, че можеш да поискаш от платформа или сайт да изтрият твои лични данни, които вече не искаш да бъдат публични – например стар профил, снимки или постове. Google дори предлага формуляр, чрез който можеш да поискаш премахване на резултати, свързани с твоето име (линк тук).

Това право не е „магическа гума“, която трие всичко, но е важен инструмент да контролираш следата си.

Пример: как да питаш изкуствен интелект за твоя дигитален отпечатък

Можеш да използваш AI като ChatGPT или Gemini, за да мислиш критично за това как изглеждаш онлайн.

Примерен промпт: „Представи си, че си бъдещ университет. Потърси информация за човек с моето име и ми кажи каква дигитална репутация виждаш – какви рискове и какви позитиви.“

Тези инструменти не могат да претърсят целия интернет вместо теб, но ще ти помогнат да се замислиш и да организираш проверката си.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

CLICK SMART: ДИГИТАЛНИЯТ СУПЕРГЕРОЙ

В дигиталния свят няма нужда от наметало, за да си супергерой. Достатъчно е да знаеш правилата на играта, да ги прилагаш умно и да пазиш не само себе си, но и другите. Това е ролята на Click Smart – нашият дигитален супергерой.

Кой е Click Smart?

Click Smart не е човек, а идея. Това е всеки млад човек, който умее да натиска правилния бутон, да разпознава капаните и да излиза от опасни ситуации. Той е комбинация между стратег от видеоигра, добър приятел в чата и отговорен гражданин онлайн.

Какви сили има?

- ***Щитът на поверителността*** – знае как да пази личните си данни и решава какво да остане лично и какво може да бъде публично.
- ***Мечът на силните пароли*** – въоръжен е с пароли, които не се чупят лесно, и с двуфакторна защита.
- ***Очите на бдителността*** – разпознава фалшиви профили, измами и фишинг.
- ***Гласът на смелостта*** – говори, когато вижда кибертормоз или несправедливост.
- ***Ръката на подкрепата*** – помага на приятелите си да се справят, когато са в беда.

Какво може да прави?

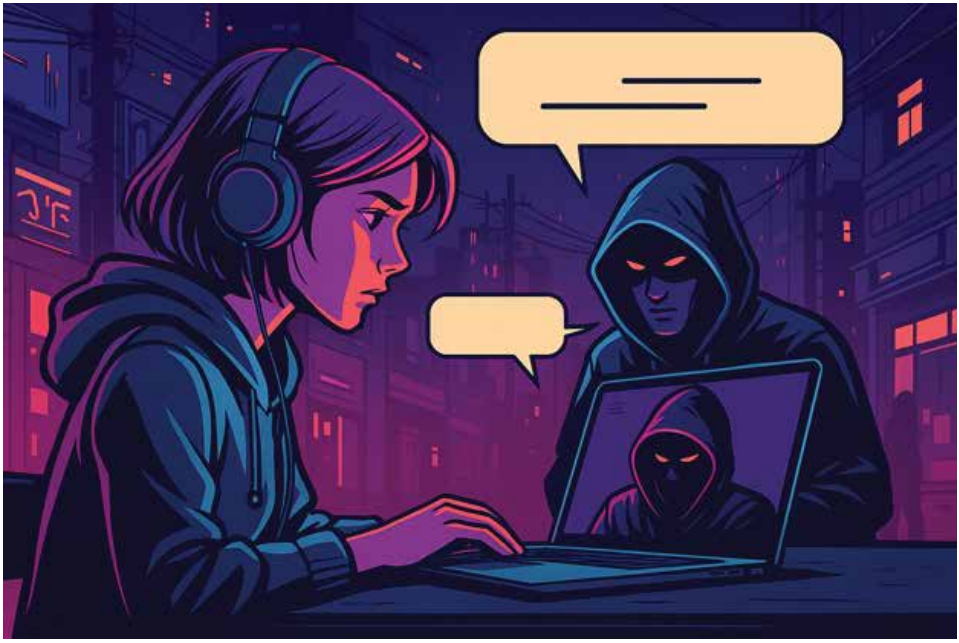
Click Smart не лети, но може да се „прехвърли“ от TikTok към Instagram, от YouTube към гейминга, без да губи фокус. Той умее да спира за секунда и да пита: ***„Ако кликна тук, това ли е най-доброто решение?“*** – и това го прави по-силен от всеки хакер.

Защо е важен?

Защото в дигиталната вселена героите не са измислени – те сме ние. Всеки избор онлайн може да е суперсила или слабо място. Да бъдеш Click Smart значи да си една крачка пред киберзаплахите.

ПРАВИЛА НА ЦИФРОВАТА ХИГИЕНА И ВИЗУАЛИЗАЦИИ:

1. Не разговаряй с непознати



Извод:
В интернет непознатите не винаги са това, за което се представят. Един профил може да изглежда приятелски, но да крие опасност. Ако някой ти пише без причина и настоява за твоята лична информация – спри и не отговаряй.

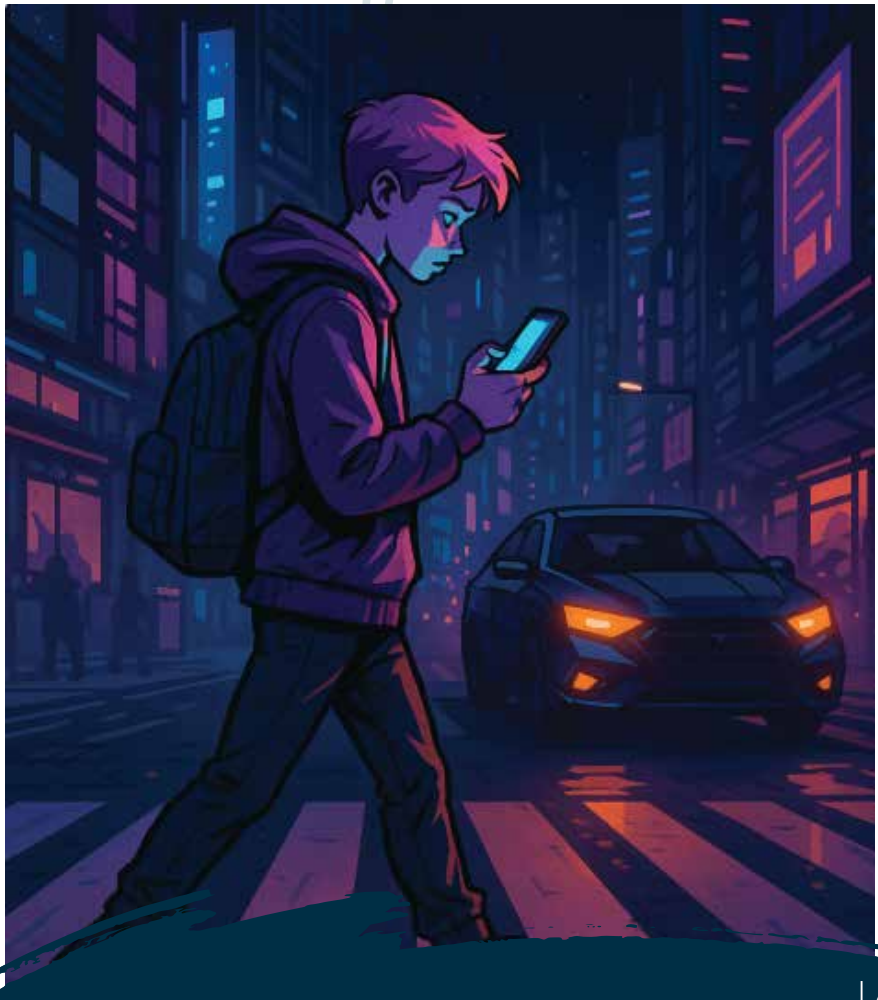
Гатанка
Когато някой те вика от тъмна уличка – ще тръгнеш ли с него?
Ако отговорът е „не“, тогава защо да го правиш онлайн?

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

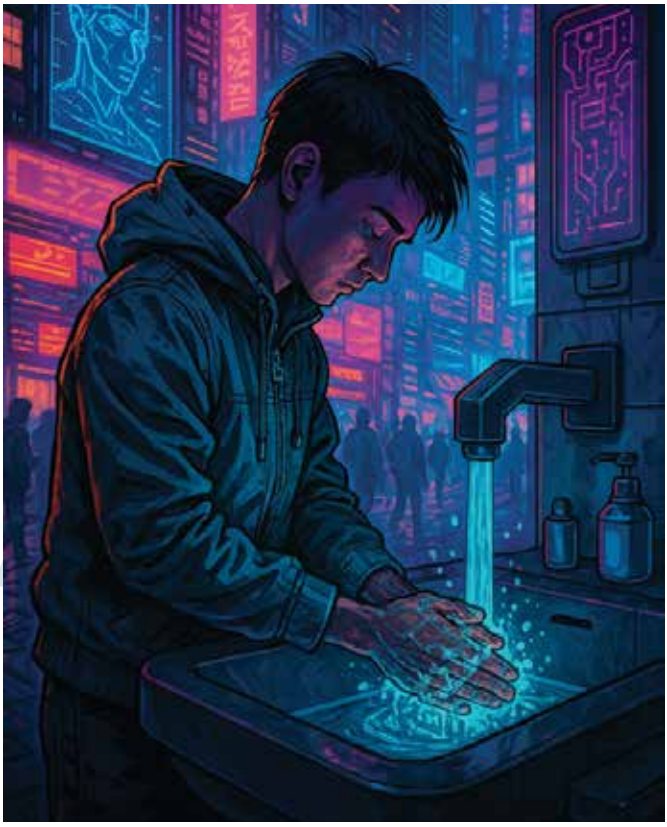
2. Оглеждай се като пресичаши

Извод:
В дигиталния свят опасностите идват бързо – като коли на оживено кръстовище. Преди да кликнеш на линк или да въведеш данни, спри за момент и се огледай. Провери адреса на сайта, подателя на съобщението и дали източникът е надежден.

Гатанка
Когато пресичаш улица, първо се оглеждаш, нали?
Тогава защо да влизаш в сайт или да кликваш на линк, без да го направиш онлайн?



3. Поддържайте лична хигиена



Извод:
Както миеш ръцете си всеки ден, така трябва да поддържаш и своята цифрова хигиена – със силни пароли, актуализации и внимателно подбрани приложения. Чистото устройство е защитено устройство.

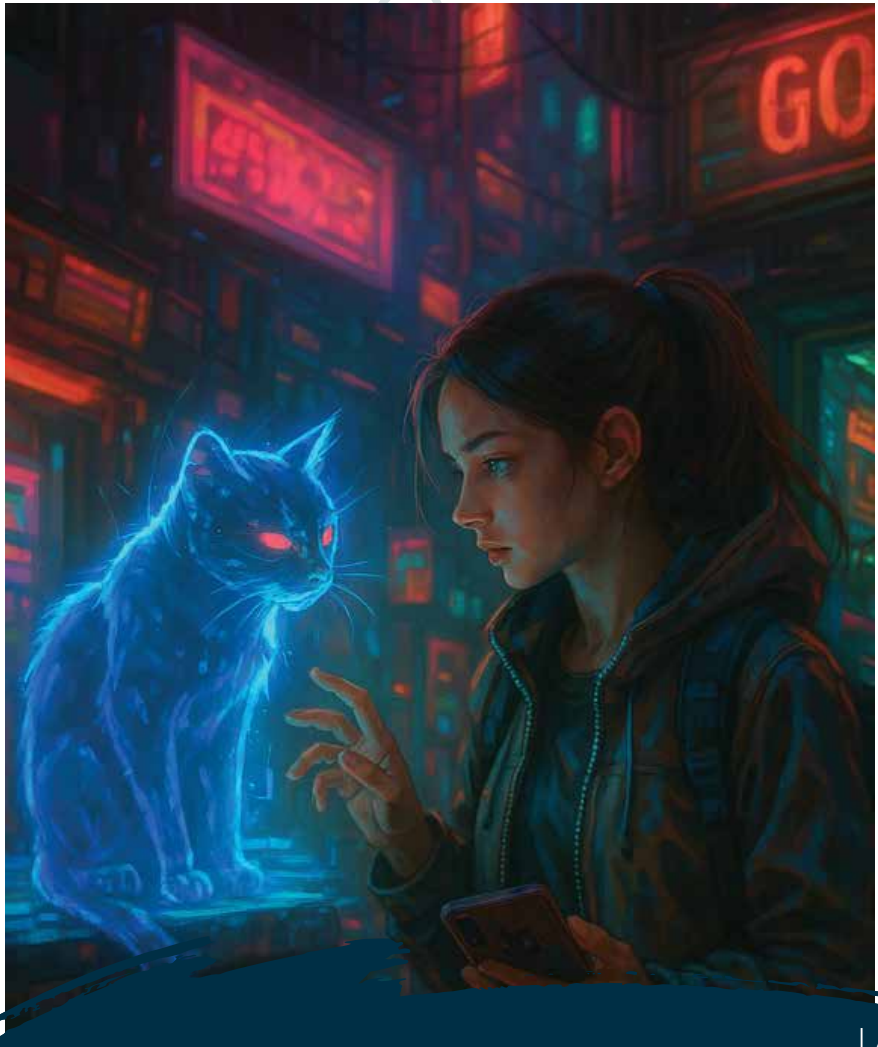
Гатанка
Ако не измиваш чиниите, мухите идват сами.
Ако не поддържаш акаунтите си, кой ще дойде при теб?

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение
" Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на
Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

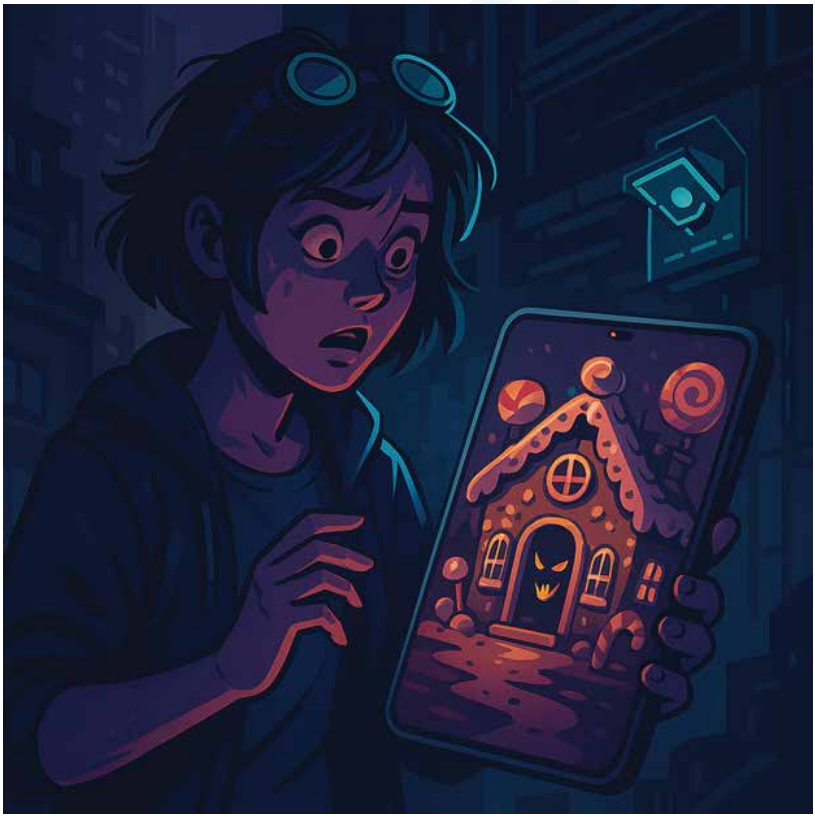
4. Любопитството зарази котката

Извод:
Любопитството е естествено, но в интернет може да отвори врата към капани. Когато видиш странна оферта, подарък или линк, който изглежда твърде добър, за да е истина – вероятно е точно така.

Гатанка
Ако котката се зарази си заради любопитството,
готов ли си ти да рискуваш своя дигитален профил?



5. Къща от захар може да крие проблеми

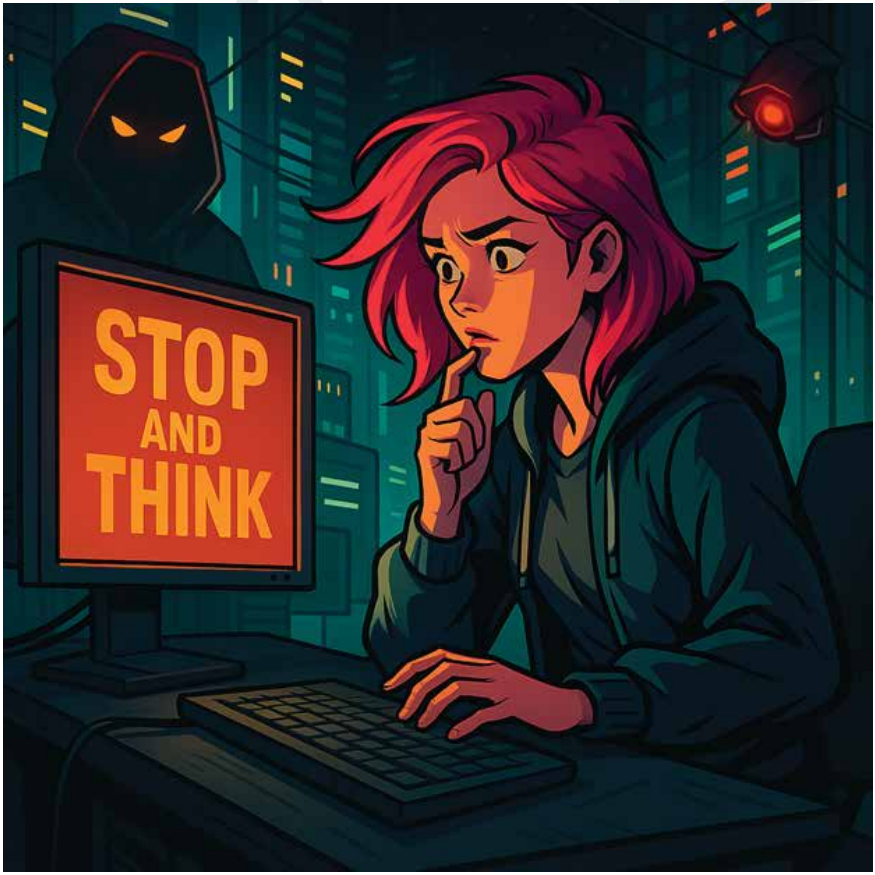


Извод:
Къщата от захар изглежда примамлива, но вътре може да дебне опасност. В интернет това са съмнителните оферти, подаръци и безплатни игри. Не всичко сладко е безопасно.

Гатанка
Ако ти подадат торта от непознат – ще я изядеш ли?
Тогава защо да „хапваш“ всеки дигитален подарък?

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение
" Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на
Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Спри, помисли и после продължи



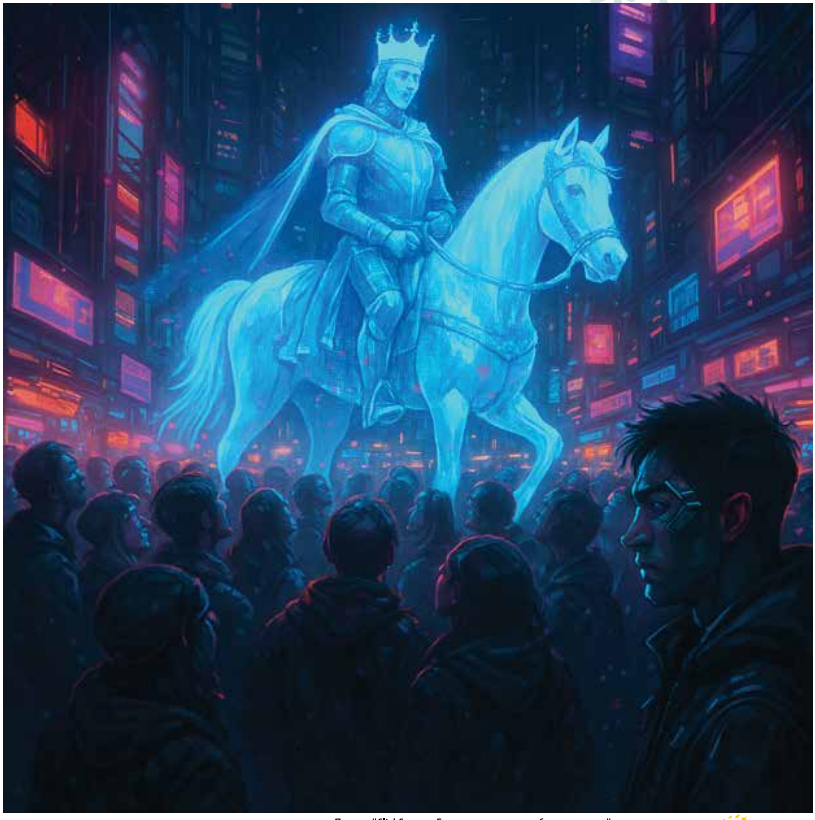
Извод:
Най-опасните решения се вземат прибързано. Ако линк, съобщение или оферта ти изглеждат странни – спри. Дай си време да помислиш и едва след това реши дали да продължиш.

Гатанка
Ако на улицата светофарът светне червено – ще тичаш ли напред? Тогава защо да го правиш онлайн?

Няма принцове на бял кон извън приказките, ако се появи или не е принц или коня не е боядисан или и двете.

Извод:
В дигиталния свят няма спасители от приказките. Ако някой се представя за твой „принц на бял кон“ – замисли се. Или не е принц, или конят е боядисан, а може би и двете.

Гатанка-провокация:
Когато нещо изглежда твърде съвършено, за да е реално – защо да вярваш, че е истинско?



Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

ПРИЛОЖЕНИЕ А: СИМВОЛИ И СТОЙНОСТИ НА ДИГИТАЛНАТА КУЛТУРА

Дигиталната култура е език от навици, правила и негласни сигнали. Символите ни помагат да „видим“ сложното, а ценностите – да изберем правилното действие, когато никой не гледа. Тук събираме общ речник от образи и смисли, за да сме една крачка напред – като Click Smart.

Защо са ни нужни символи

В интернет всичко се случва бързо: нотификации, линкове, предложения, покани. Символът е като светлинен сигнал – включва инстинкт, спира ни за секунда и ни напомня правилото. Когато превърнем символите в навици, дигиталната хигиена става естествена.

Основни стойности на дигиталната култура

- ***Поверителност (Privacy):*** правото да решаваш кой вижда твоите данни и история. Уважение към чуждата поверителност също е част от това.
- ***Съгласие (Consent):*** без ясно „да“ няма споделяне, препращане, тагване и срещи – нито онлайн, нито офлайн.
- ***Автентичност (Authenticity):*** не се крий зад маски за да нараниш; бъди честен към себе си и другите.
- ***Отговорност (Accountability):*** думите онлайн имат последици; поемаме отговорност за постове, коментари, шеги и „предизвикателства“.
- ***Емпатия (Empathy):*** отсреща не е екран, а човек. Питай се: „Как би му прозвучало това лице в лице?“

- ***Сигурност по дизайн (Security by default):*** силни пароли, 2FA, обновления и минимално споделяне по подразбиране.
- ***Критично мислене (Critical thinking):*** проверка на източници, скептицизъм към сензационни твърдения и „твърде добри“ оферти.
- ***Включване (Inclusion):*** уважение към различието, без език на мразата; създаване на безопасни пространства за всички.
- ***Цифрова хигиена (Digital hygiene):*** ежедневни малки действия, които пазят устройства, профили и репутация.
- ***Правото да бъдеш забравен:*** осъзнаване, че имаш механизми да премахнеш данни за себе си и да управляваш следата си.

Символен речник: от образ към действие

Щит
Значение: Поверителност и защита.
Действие: Преглед на настройки, ограничаване на видимост, блокиране при нужда.

Ключ
Значение: Силна парола и 2FA.
Действие: Уникални пароли, мениджър на пароли, активирана двустепенна защита.

Светофар / Пешеходна пътека
Значение: „Спри–помисли–продължи“.
Действие: Проверка на линк/източник преди клик; оглед вляво/вдясно за червени флагове.

Маска
Значение: Фалшиви профили, deepfake, измами.
Действие: Верификация през друг канал, недаване на лични данни, скептицизъм към „съвършени“ аватари.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Холограма
Значение: Илюзия/манипулация (реклама, дезинформация, „принц на бял кон“).
Действие: Сравнение на източници, търсене на детайли, които „проблясват“ фалша.

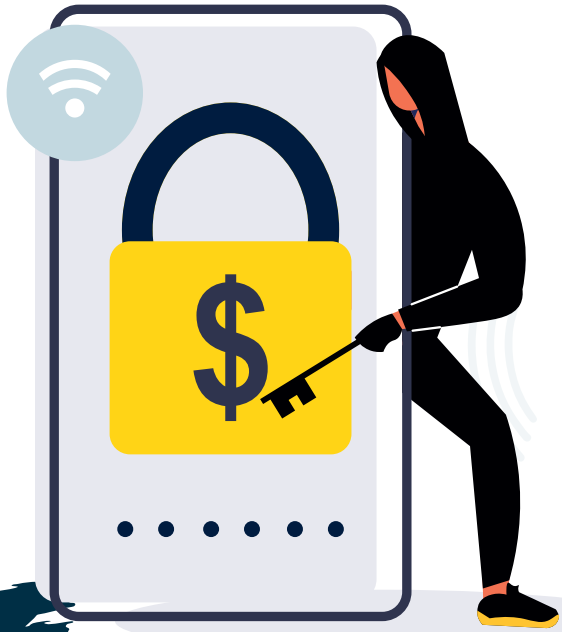
„Захарна къща“ (бисквитки/оферти)
Значение: Примамливото съдържа капани.
Действие: Отказ/персонализиране на бисквитки, избягване на „безплатни“ дарове и пиратски софтуер.

Стъпки/Отпечатъци
Значение: Дигитална следа и репутация.
Действие: Самопроверка в търсачки, чистене на стари постове, изграждане на позитивно портфолио.

Катинар
Значение: Сигурна връзка, https.
Действие: Въвеждане на данни само на защитени страници; избягване на публичен Wi-Fi за чувствителни операции.

QR/Портал
Значение: Вход към непознато.
Действие: Сканиране само от доверени източници; избягване на случайни QR кодове.

Часовник
Значение: Ранна реакция и навременност.
Действие: Смяна на пароли, блокиране, доклад и сигнал веднага, не „утре“.



Приложение на символите в ежедневни ситуации

- ***Чат от непознат:*** виж маската → провери профила през друг канал; не споделяй нищо лично; блокирай при натиск.
- ***Линк с „невероятна оферта“:*** светофар и „захарна къща“ → спри, провери домейна, не въвеждай данни; по-добре потърси официалния сайт.
- ***Групов чат с ескалиращи шеги:*** емпатия и отговорност → прекъсни веригата, не споделяй чуждо съдържание, предложи частен разговор.
- ***Покана за среща от онлайн познат:*** маска и щит → не отивай сам/а; информирай родител/учител; публично място, придружител.
- ***Снимка/клип преди пост:*** отпечатъци → попитай се „би ли стояло в CV-то ми?“; ако не – не го публикувай.

Мини-етичен кодекс „Click Smart“

- Първо човекът, после екрана.
- Без съгласие няма споделяне – чуждо или мое.
- Истината не се обижда от проверка.
- Не всичко сладко е безопасно.
- Ранната реакция намалява щетата.
- Доверие ≠ наивност: проверявам, преди да кликна.
- Не съм сам/а онлайн: разговарям с близък, когато се колебая.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Как да превърнеш символите в навик

- ***Ритуал „60 секунди сигурност“:*** веднъж седмично – проверка на устройства, обновления, 2FA, активни сесии.
- ***Сезонно почистване:*** пролет/есен – преглед на стари постове, тагове, списъци с приятели.
- ***Чек преди клик:*** светофар в главата – източник, домейн, https, „кой печели, ако кликна?“.
- ***Договор у дома и в класа:*** съгласувани правила за споделяне и време онлайн; роли на „партньори, не шпиони“.

Послание към младежи, родители и учители

- ***Младежи:*** символите са твои инструменти – щит, ключ, светофар. Вземи ги със себе си във всяка платформа.
- ***Родители:*** бъдете партньори – градете доверие и общи ритуали за проверка; споделяйте своя опит от „офлайн опасностите“.
- ***Учители:*** пренесете безопасността и в дигиталната среда – кратки класни упражнения с „светофара“ и „маската“, казуси от реалния живот.

Последна мисъл

Дигиталната култура не е списък със забрани, а компас. Символите ни сочат посока, а ценностите – причина ***защо*** да поемем по нея. Когато ги носим със себе си, ставаме именно онзи герой, който интернетът очаква: умен, смел и отговорен. ***Click Smart.***

ПРИЛОЖЕНИЕ Б: КИБЕРБУКВАР – РЕЧНИК НА ВАЖНИТЕ ТЕРМИНИ

Този речник събира ключовите понятия, които използвахме в наръчника. Целта му е да бъде лесен ориентир както за младежи, така и за родители и учители.

А

Акаунт (Account) – твоята дигитална идентичност в дадена платформа (игра, социална мрежа, приложение). Често съдържа лични данни, снимки, контакти и е основа на дигиталната ти репутация.
Анонимен профил – регистрация без истинско име или с измислени данни. Може да бъде използван за безопасност, но и за злоупотреби.

Б

Бисквитки (Cookies) – малки файлове, които сайтовете запазват в браузъра, за да „помнят" предпочитания, вход или активност. Полезни, но често използвани и за проследяване.
Блокиране (Block) – действие, с което спираш достъпа на друг човек до твоето съдържание или комуникация.

В

Вирус (Computer Virus) – зловреден софтуер, който заразява устройство, често чрез прикачени файлове, линкове или пиратски програми.
Войс фишинг (Vishing) – измама чрез телефонно обаждане, при което измамникът се представя за институция или познат и опитва да получи лични данни.

Г

Груминг (Online Grooming) – процес, при който възрастен с лоши намерения изгражда доверие у дете или тийнейджър онлайн, за да го манипулира или изнуди.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Д

Двуфакторна автентикация (2FA) – допълнителен слой защита при влизане в акаунт: освен парола се изисква и втори код (SMS, приложение, токен).

Дигитална репутация – образът ти в интернет, съставен от постове, снимки, коментари и следи в мрежата. Твоето „ново CV".

Дийпфейк (Deepfake) – видео или аудио, създадено с изкуствен интелект, което имитира реален човек (глас, лице). Използва се за измами или дезинформация.

Е

Етика онлайн – съвкупност от правила и поведение, базирани на уважение, отговорност и емпатия в дигиталното пространство.

З

Защита на личните данни (GDPR) – европейски регламент, който ти дава права върху личната информация (например право да бъдеш забравен – да поискаш изтриване на свои данни).

И

Изтичане на данни (Data Breach) – случай, при който лична информация (имейли, пароли, снимки) става достъпна за трети лица без разрешение.

Изнудване онлайн (Sextortion / Cyber extortion) – когато някой изисква пари, снимки или услуги под заплаха, че ще публикува лични материали.

К

Кибератака – умишлено действие за пробив в компютърна система или акаунт.

Кибертормоз (Cyberbullying) – обиди, заплахи или унижения онлайн, които могат да имат сериозни емоционални последствия.

Киберзаплаха – потенциална опасност от атака или измама в дигитална среда.

Л

Лични данни – всяка информация, която може да идентифицира човек: име, ЕГН, адрес, телефон, снимки, глас, IP адрес.

М

Малвер (Malware) – общ термин за зловреден софтуер: вируси, троянци, червеи, шпионски програми.

Манипулация чрез дезинформация – умишлено разпространение на неверни или подвеждащи новини, за да се постигне влияние, печалба или радикализация.

О

Онлайн идентичност – начинът, по който изглеждаш и се представяш в дигитална среда.

П

Парола – тайна комбинация за достъп до акаунт. Силна парола включва букви, цифри и символи.

Фишинг (Phishing) – измамни съобщения или сайтове, които те подмамват да разкриеш лични данни или пароли.

QR фишинг (Quishing) – измама чрез фалшив QR код, който отвежда към зловреден сайт.

Р

Ранна реакция – действията, които предприемаш веднага при инцидент онлайн: смяна на парола, блокиране, сигнализиране.

С

Социално инженерство – техника, при която измамникът манипулира доверието ти, за да получи достъп или информация.

Х

Хакване на акаунт – неоторизиран достъп до чужд профил. Често става чрез откраднатa парола или уязвимост в приложението.

Холограма (в метафората на наръчника) – символ на дигитална илюзия: нещо, което изглежда съвършено, но е фалшиво отвътре.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

ПРИЛОЖЕНИЕ В: ДОСТЪПЕН РЕЧНИК ЗА МЛАДИ ХОРА И РОДИТЕЛИ

1. Акаунт
Това е твоят дигитален „ключ“ към игра или мрежа. Ако някой друг го вземе, може да пише от твое име.

- ***Ученици:*** пази акаунта си като врата към дома.
- ***Родители:*** попитайте децата как защитават профилите си.
- ***Учители:*** насърчавайте създаването на силни пароли в клас.

2. Лични данни
Име, адрес, снимка, училище – всичко, което може да те разкрие.

- ***Ученици:*** не ги споделяй лекомислено.
- ***Родители:*** обяснете, че не всяко приложение има право да ги изисква.
- ***Учители:*** включвайте темата за защита на личните данни в уроците.

3. Парола
Кодът за достъп до профила ти. Колкото е по-силна, толкова си по-защитен.

- ***Ученици:*** не използвай „123456“.
- ***Родители:*** помогнете при създаване на пароли.
- ***Учители:*** правете упражнения „слаба или силна парола“.

4. Двуфакторна защита (2FA)
Втори код освен паролата, който прави акаунта много по-сигурен.

- ***Ученици:*** активирай я навсякъде.
- ***Родители:*** насърчете децата да я използват.
- ***Учители:*** обяснете я с пример – „две ключалки на вратата“.

5. Фишинг
Фалшиво съобщение, което иска да кликнеш линк или да дадеш данни.

- ***Ученици:*** ако те карат да бързаш – спри.
- ***Родители:*** покажете на децата примери за измамни имейли.
- ***Учители:*** разгледайте в час реални примери.

6. QR фишинг (Quishing)
Фалшив QR код, който отвежда към опасен сайт.

- ***Ученици:*** сканирай само от доверени места.
- ***Родители:*** предупреждавайте при разлепени QR кодове навън.
- ***Учители:*** включете това в дигиталната грамотност.

7. Кибертормоз
Когато някой обижда, унижава или заплашва онлайн.

- ***Ученици:*** говорете, ако станете жертва.
- ***Родители:*** слушайте без осъждане.
- ***Учители:*** създавайте безопасни пространства в клас.

8. Хакване на акаунт
Когато някой влезе в профила ти без разрешение.

- ***Ученици:*** смени паролата веднага.
- ***Родители:*** помогнете при възстановяване на достъпа.
- ***Учители:*** обяснете какво значи „сигнализиране“.

9. Дигитална репутация
Всичко, което интернет показва за теб – твоята „визитка“.

- ***Ученици:*** мисли преди да публикуваш.
- ***Родители:*** обсъждайте как постовете изглеждат отвън.
- ***Учители:*** работете с учениците върху „дигиталното CV“.

10. Бисквитки
Малки файлове, които сайтовете ползват, за да те „помнят“.

- ***Ученици:*** научи се да отказваш ненужните.
- ***Родители:*** настройвайте ги заедно с децата.
- ***Учители:*** обяснете чрез примера с „къща от захар“.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

11. Изтичане на данни
Когато лична информация попадне в ръцете на непознати.
- ***Ученици:*** провери имейла си в Have I Been Pwned.
- ***Родители:*** помагайте при смяна на пароли.
- ***Учители:*** покажете сайта за проверка в час.

12. Дийпфейк
Фалшиво видео или аудио, направено с изкуствен интелект.
- ***Ученици:*** не вярвай на всичко, което изглежда „твърде реално".
- ***Родители:*** говорете за опасността от измами с глас/видео.
- ***Учители:*** дискутирайте темата в гражданско образование.

13. Груминг
Когато възрастен се опитва да спечели доверие на дете с лоши намерения.
- ***Ученици:*** ако някой непознат иска твоята тайна – сподели с близък.
- ***Родители:*** обръщайте внимание на новите „онлайн приятели".
- ***Учители:*** обучавайте как да разпознават опасното поведение.

14. Социално инженерство
Измама чрез манипулиране на доверието ти.
- ***Ученици:*** ако някой настоява твърде много – внимавай.
- ***Родители:*** разиграйте заедно сценарии „какво ако".
- ***Учители:*** направете упражнения „разпознай червените флагове".

15. Правото да бъдеш забравен
Можеш да поискаш да изтрият твои данни от интернет.
- ***Ученици:*** знай, че имаш избор.
- ***Родители:*** помогнете на децата да подадат заявки при нужда.
- ***Учители:*** разяснете как работи GDPR.

Цел на този речник:
- Учениците да разберат понятията чрез примери от своя живот.
- Родителите да имат прост език за разговори с децата.
- Учителите да вмъкват темите в час по ИТ, гражданско образование или час на класа.

ТЕСТ: „КОЛКО УМЕН ИГРАЧ СИ В ИНТЕРНЕТ?“

Част I: Основи на киберсигурността

1. (★) Какво е акаунт?
A) Твоят профил в игра или социална мрежа ✓
B) Хардуерно устройство
C) Личната ти карта
D) Папка на компютъра ✓

2. (★) Кое от следните са лични данни?
A) Име ✓
B) Любим цвят
C) Телефонен номер ✓
D) Училището на приятел

3. (★★) Коя е силна парола?
A) 123456
B) Football2024
C) M!raKle*2025 ✓
D) imenofthecat

4. (★★) Двуфакторната защита (2FA):
A) Изисква два кода ✓
B) Е по-сигурна от само парола ✓
C) Работи само в игри
D) Означава два акаунта

5. (★★★) Кога е редно да сменяш парола?
A) Ако мислиш, че е изтекла ✓
B) Ако е една и съща на много места ✓
C) Никога
D) Само когато си купиш нов телефон

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Част II: Киберзаплахи

6. (★) Какво е фишинг?
A) Спорт
B) Фалшиво съобщение, което иска лични данни ✓
C) Сайт за видео игри
D) Публичен чат

7. (★★) Пример за фишинг е:
A) Имейл от банка, в който искат парола ✓
B) Съобщение от непознат в Instagram ✓
C) Влизане през училищния портал
D) Пускане на домашно във Viber

8. (★★) Какво е QR фишинг (Quishing)?
A) Фалшив QR код ✓
B) Безопасен баркод
C) Ново приложение
D) Състезание в игри

9. (★★★) Какво е deepfake?
A) Филтър в TikTok
B) Видео/аудио, създадено с AI ✓
C) Игрова модификация
D) Истински клип

10. (★★★) Пример за кибертормоз е:
A) Подигравки в групов чат ✓
B) Заплашителни съобщения ✓
C) Споделяне на смешно видео с животни
D) Лайк на снимка

Част III: Реални действия при заплаха

11. (★) Ако ти хакнат акаунта, първо трябва:
A) Да смениш паролата ✓
B) Да изтриеш телефона
C) Да се паникьосаш
D) Да блокираш интернет ✓

12. (★★) При онлайн тормоз какво НЕ трябва да правиш?
A) Да запазиш доказателства
B) Да мълчиш и да криеш ✓
C) Да потърсиш доверен възрастен
D) Да блокираш профила

13. (★★) Къде можеш да подадеш сигнал за киберинцидент в България?
A) ГДБОП ✓
B) Център за безопасен интернет ✓
C) Reddit
D) Google

14. (★★★) Ако данните ти изтекат:
A) Провери имейла в Have I Been Pwned ✓
B) Смени паролите ✓
C) Не прави нищо
D) Сподели в TikTok

15. (★★★) Коя е правилната реакция при фалшив „подарък“ онлайн?
A) Да го вземеш веднага
B) Да провериш източника ✓
C) Да игнорираш ✓
D) Да пратиш на всички приятели

Част IV: Дигитална репутация

16. (★) Какво е дигитална репутация?
A) Това, което интернет „разказва“ за теб ✓
B) Мнението на приятелите ти
C) Оценката ти в училище
D) Любимият ти филм

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

17. (★★) Как можеш да провериш какво пише за теб онлайн?
A) Чрез Google ✓
B) Чрез Have I Been Pwned ✓
C) Чрез компютърна игра
D) Чрез Instagram филтри

18. (★★) Какво можеш да направиш, ако намериш неприятна снимка онлайн?
A) Да я изтриеш от акаунта си ✓
B) Да поискаш изтриване по GDPR ✓
C) Да я споделиш още веднъж
D) Да я игнорираш

19. (★★★) Кое НЕ е част от дигиталната репутация?
A) Коментари в YouTube
B) Снимки в Instagram
C) Домашните в училище ✓
D) Постове във форуми

20. (★★★) Какво е правото да бъдеш забравен?
A) Да изтриеш профила си ✓
B) Да поискаш заличаване на данни ✓
C) Да не плащаш интернет
D) Да смениш устройство

Част V: Цифрова хигиена

21. (★) Какво значи „цифрова хигиена“?
A) Редовно да миеш екрана
B) Да поддържаш профилите и устройствата си сигурни ✓
C) Да имаш най-новия телефон
D) Да изтриваш игри

22. (★★) Пример за добра цифрова хигиена е:
A) Редовни обновления ✓
B) Силни пароли ✓
C) Пиратски програми
D) Споделяне на парола с приятел

23. (★★) Какво предпазва двуфакторната защита?
A) Само паролата
B) Достъпа до акаунта ✓
C) Вируси
D) Бисквитките

24. (★★★) Кое е „червен флаг“ в интернет?
A) Имейл с правописни грешки ✓
B) Натиск „отвори веднага“ ✓
C) Писмо от официален източник
D) Линк към познат сайт

25. (★★★) Кое НЕ е добър навик?
A) Да проверяваш линкове
B) Да споделяш пароли ✓
C) Да блокираш непознати
D) Да използваш 2FA

Част VI: Социални мрежи и родители

26. (★) Какво трябва да направиш с настройките за поверителност?
A) Да ги провериш и настроиш ✓
B) Да ги игнорираш
C) Да ги оставиш по подразбиране
D) Да ги споделиш с всички

27. (★★) Кое е вярно за TikTok, Instagram и Facebook?
A) Имат настройки за поверителност ✓
B) Позволяват ти да блокираш ✓
C) Нямат никаква защита
D) Винаги са безопасни

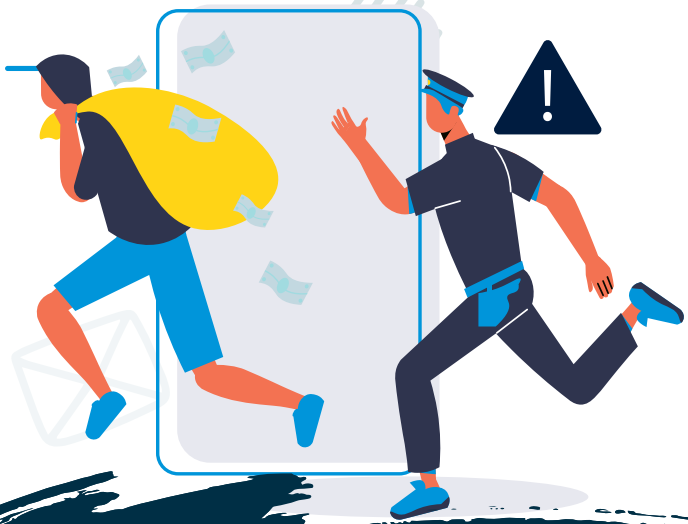
Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение
" Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на
Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

28. (★★) Какво да направят родителите, за да помогнат?
A) Да бъдат партньори ✓
B) Да слушат без осъждане ✓
C) Да четат всички чатове
D) Да наказват

29. (★★★) Как могат учителите да подкрепят учениците?
A) Чрез упражнения за киберсигурност ✓
B) Като създават доверие ✓
C) Като игнорират проблемите
D) Като наказват

30. (★★★) Какво е най-важното при общуването в семейството за онлайн рисковете?
A) Доверие ✓
B) Откритост ✓
C) Строг контрол
D) Мълчание

Инструкция за попълване:
- Отбележи всички верни отговори на всеки въпрос.
- Брой правилни отговори = твоята „киберзрялост".
- Повече от 25 точки ⟶ истински **Click Smart.**



Семейно споразумение за използване на устройства

Ние, членовете на нашето семейство (и училищната общност), се съгласяваме да използваме дигиталните устройства отговорно, с уважение и грижа един към друг. Това споразумение е наша обща „карта“ за безопасно и здравословно онлайн поведение.

1. Поверителност и лични данни

- Учениците обещават да не споделят лични данни (адрес, училище, пароли) без съгласие.
- Родителите обещават да уважават личното пространство на децата онлайн и да не влизат в акаунти без знание.
- Учителите ще насърчават безопасното споделяне в клас и ще помагат при инциденти.

2. Пароли и акаунти

- Всеки използва собствени пароли и ги пази в тайна.
- Ако парола бъде споделена случайно, тя се сменя веднага.
- Родителите и децата заедно настройват двуфакторна защита.

3. Онлайн време

- Устройствата се използват в разумни граници: време за учене, игра и почивка.
- Вечер, преди сън, устройствата остават на общо място.
- Уикендите включват и „офлайн“ занимания заедно.

4. Кибертормоз и онлайн поведение

- Учениците се съгласяват да не обиждат, унижават или изолират други онлайн.
- Родителите обещават да подкрепят, ако децата са жертви или свидетели на тормоз, без упреци.
- Учителите поемат ангажимент да реагират на сигнали за кибертормоз.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

5. Доверие и разговор

- Ако нещо притесни ученика онлайн, той се обръща към родител или учител.
- Родителите обещават да изслушват без да наказват, първо да разберат ситуацията.
- Учителите създават атмосфера в клас, в която децата могат да споделят.

6. Сваляне на приложения и игри

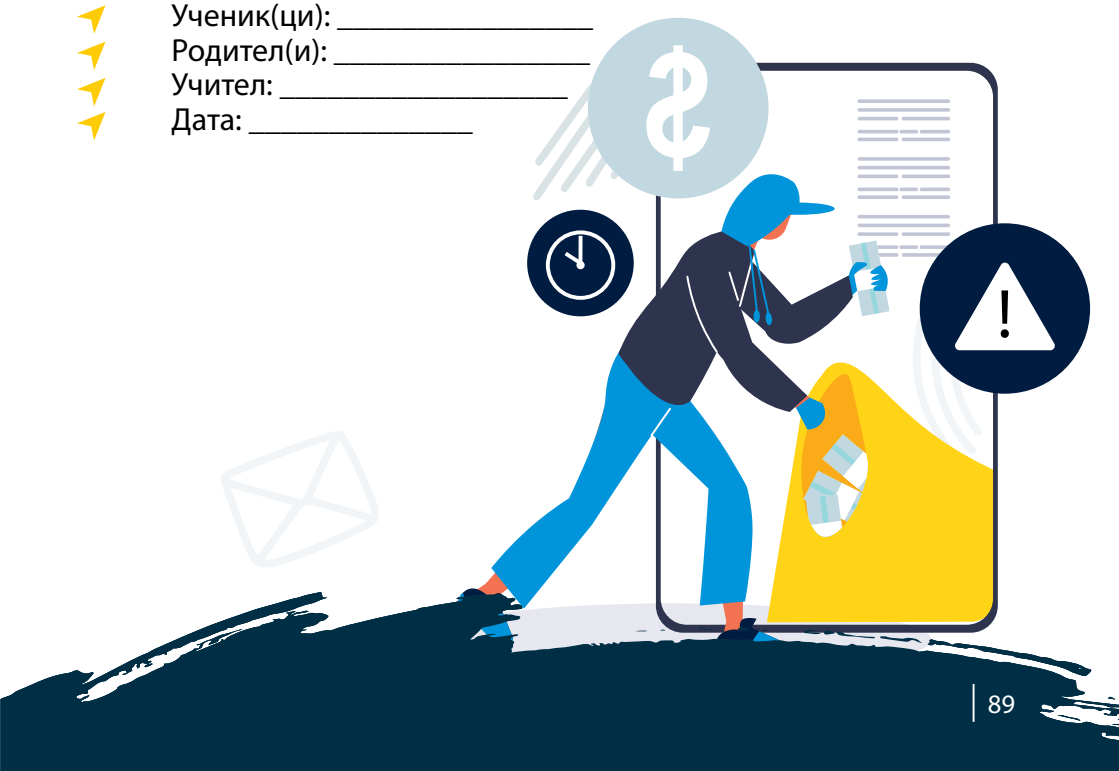
- Нови приложения или игри се обсъждат заедно с родител.
- Проверява се възрастовата граница и безопасността.
- Учителите дават препоръки за образователни ресурси.

7. Семейна и училищна подкрепа

- Всички се съгласяваме, че подкрепата не е слабост.
- При проблем се обръщаме първо един към друг, а след това – към институции като ГДБОП или Център за безопасен интернет.

Подписваме това споразумение като знак за доверие и сътрудничество:

- Ученик(ци): _____
- Родител(и): _____
- Учител: _____
- Дата: _____



Финални думи

Този наръчник е резултат от месеци работа, проучвания и диалог. Изследвахме съвременните киберзаплахи, предизвикателствата пред младите хора и начина, по който семействата и училищата могат да изградят по-безопасна и осъзната дигитална култура. Уникалното в него е, че комбинира практични знания, реални истории и съвети с ясен и достъпен стил, насочен едновременно към ученици, родители и учители.

В процеса на разработка използвах и ***изкуствен интелект*** – не като заместител на човешката експертиза, а като партньор за диалог. AI ми помогна да изследвам темите по-широко, да проверя различни гледни точки и да прецизирам посланията. Това е още едно доказателство, че технологиите могат да бъдат ценен инструмент, ако ги използваме осъзнато и отговорно.

Надявам се този наръчник да се превърне в практическо помагало, което не просто се чете, а се използва – в класните стаи, у дома, в разговорите между родители и деца. Целта ни е проста, но изключително важна: да дадем знания, увереност и инструменти, за да сме винаги ***една крачка пред киберзаплахите.***

Екипът на ***Safer.bg*** е готов да надгради това съдържание и да го превърне в ***дигитален асистент***, който да се обновява редовно и да бъде винаги актуален. Ние вярваме, че знанието не трябва да остава заключено в книга – то трябва да живее, да се адаптира и да е на разположение навсякъде, където е нужно.

Освен това, нашият екип е готов да споделя натрупаното знание във всяко училище в България – чрез обучение на преподавателите по темите от наръчника и чрез подготовка за новата професия ***„Киберсигурност“*** според държавния образователен стандарт. Вярваме, че именно в класните стаи се полагат основите на бъдещата дигитална култура на страната.
С този наръчник поставяме началото на път – път към по-осъзнато, по-сигурно и по-отговорно присъствие онлайн. И път, който можем да извървим само заедно – ученици, родители, учители, експерти.

Проект "ClickSmart - Една крачка пред киберзаплахите" на сдружение " Сейфър- Дигитално читалище за онлайн сигурност" се изпълнява с финансовата подкрепа на Столична Община, Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)
ПРОГРАМА Европа СТОЛИЧНА ОБЩИНА

Проект "ClickSmart - Една крачка пред киберзаплахите"
на сдружение " Сейфър- Дигитално читалище за онлайн сигурност"
се изпълнява с финансовата подкрепа на Столична Община,
Програма " Европа" (договор СОА25-ДГ56-1742/03.07.2025)