Как да се предпазим от кибертормоза, онлайн злоупотребите, дезинформацията и разпространението на фалшивите новини?

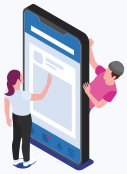
Поколението Z в дигиталния свят

Gen Z е първото поколение, родено в напълно дигитален свят и е по-свързано от всяко друго поколение.

Средно статистически детето от поколението Z получава първия си смартфон малко преди дванадесетия си рожден ден.

81% от членовете на поколението Z заявяват, че използването на социални медии им помага да поддържат връзка с приятелите си.

Средно потребителят от Gen Z отделя 2 ч. и 55 мин. на ден за сърфиране в социални медии.



Според статистиката на Generation Z, 45% от тийнейджърите съобщават, че са онлайн почти постоянно.

52% от поколението Z са загрижени за поверителността си онлайн.

41% от Gen Z потребителите на социалните медии са загрижени за времето, което губят онлайн.

Дигитална психология

Изследователите са установили, че хората от Z поколението изкарват средно по 7 часа онлайн всеки ден, половината от които на мобилни устройства.

Тези на възраст между 15 и 29 години прекарват най-много време онлайн, като проверяват телефоните си средно на всеки 12 минути.

Феноменът „информационно претоварване“. Случва се, когато количеството информация, което попада в полезрението ни, значително надвишава нашия капацитет за възприемане, което води до все по-голяма трудност при взимане на адекватни решения и справяне с предизвикателствата на дигиталното пространство.

Интернет пространството налага изисквания върху нас. Трябва да имате огромна мрежа от контакти и средно количество лайкове. Невъзможността да се постигнат води до чувство за малоценност и самота.

Социалните мрежи увеличават и т.нар. „страх от пропускането“. Гледайки посетените места и събитията на вашите приятели в социалните мрежи, е възможно да стигнете до извода, че пропускате много и пропилявате живота си, като пренебрегвате това, което вече имате.

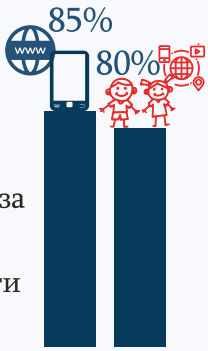
Формиране на дигиталния ни Аз-образ. Това е дигиталната версия на нашата личност, в която проектираме идеализирана представа за себе си, отразявайки най-доброто, опитвайки се да филтрираме негативното. Проверили ли сме обаче каква следа оставяме?

СТАТИСТИКА

Дигиталните технологии в България?

Българските деца са на второ място по използване на интернет след Швеция.

По данни на НСИ за 2021 г. 85% от домакинствата имат достъп до интернет, а над 80% са деца по-малки от 10 г.



Данните сочат още, че децата са уязвими - нямат преценка за риска и имат неразвити социални умения, а най-честите злоупотреби с тях са изнудване с интимни снимки, контакти на малолетни със сексуална цел, онлайн тормоз и заплахи, като разпространението е чрез мобилни връзки, тъй като всяко дете разполага с неограничен достъп до мрежата.

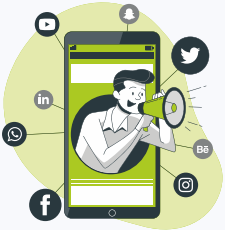
40% от 10 годишните са комуникирали в интернет;

50% казват, че децата не знаят какво правят;

84% са преживели агресия в социалните мрежи;

39% са с откраднат профил.

Младите прекарват от 5 до 8 часа всеки ден в интернет.

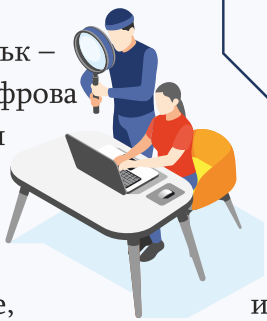


Най-често 9 -12-годишните деца използват и социални мрежи.

Важно е да се знае, че в основните изследвания на НСИ влизат хората между 16 г.-74 г., а извън измерванията остават децата до 16 г.

Дигитален отпечатък

Какво е дигитален отпечатък?



Дигиталният отпечатък – понякога наричан цифрова сянка или електронен отпечатък – се отнася до следите от данни, които оставяте, когато използвате интернет - уебсайтове, имейли и всякаква информация, която изпращате онлайн. Дигиталният или цифровият отпечатък може да се използва за проследяване на онлайн дейностите и устройствата на дадено лице.

Активно или пасивно интернет потребителите създават своя цифров отпечатък чрез дейността си в мрежата.

Всеки път, когато използвате интернет за публикации в социалните медии, различни абонаменти, оставяне на коментар, пазаруване и така нататък, оставяте след себе си следа от информация, известна като вашия дигитален отпечатък. Понякога не винаги е очевидно, че допринасяте за цифровия си отпечатък. Например уебсайтовете могат да проследяват активността ви, като инсталират бисквитки на вашето устройство, а приложенията могат да събират данните ви, без да знаете. След като разрешите на дадена организация достъп до вашата информация, тя може да продаде или сподели вашите данни с трети страни. Още по-лошо, вашата лична информация може да бъде компрометирана като част от нарушение на сигурността на данните.

Поради тези причини си струва да обмислите какво казва вашият цифров отпечатък за вас. Много хора се опитват да управляват цифровия си отпечатък, като внимават по отношение на своите онлайн дейности, за да контролират данните, които могат да бъдат събрани на първо място.

Какви дигитални отпечатъци оставям?

Дигиталните отпечатъци се определят като активни и пасивни цифрови отпечатъци

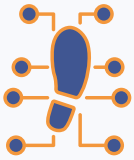
Активен цифров отпечатък

е мястото, където потребителят съзнателно е споделил информация за себе си – например чрез публикуване или участие в сайтове за социални мрежи или онлайн форуми. Ако даден потребител е влязъл в уебсайт чрез регистрирано потребителско име или профил, всички публикации, които прави, са част от неговия активен цифров отпечатък.

Други дейности, които допринасят за активен дигитален отпечатък, включват попълване на онлайн формуляр като абониране за бюлетин или съгласие за приемане на бисквитки във вашия браузър

Пасивни цифрови отпечатъци

Пасивен цифров отпечатък се създава, когато се събира информация за потребителя, без той да знае, че това се случва. Например, когато уебсайтовете събират информация за това - колко пъти потребителите посещават даден сайт, откъде идват и техния IP адрес. Това е скрит процес, който потребителите може да не осъзнават, че се извършва. Други примери за пасивни отпечатъци включват сайтове за социални мрежи и рекламодатели, които използват вашите харесвания, споделяния и коментари, за да ви профилират и да ви насочват към конкретно съдържание.



Цифровият отпечатък може да определи цифровата репутация на човек, която сега се счита за толкова важна, колкото и офлайн репутацията му.

Работодателите могат да проверят цифровите отпечатъци на своите потенциални служители, особено техните социални медии, преди да вземат решения за наемане.

Думите и снимките, които публикувате онлайн, могат да бъдат изтълкувани погрешно или променени, причинявайки неволна обида.

Съдържанието, предназначено за частна група, може да се разпространи в по-широк кръг, като потенциално навреди на връзки и приятелства.

Киберпрестъпниците могат да експлоатират вашия цифров отпечатък – да го използват за цели като фишинг за достъп до акаунт или създаване на фалшиви самоличности въз основа на вашите данни.

Инфо за моята дигитална самоличност?

Как се представям в интернет?

Социални мрежи.

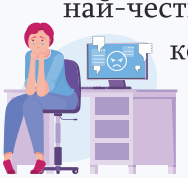
Какво казвам, какво показвам? Какви публикации поствам? Къде ходя? С кого общувам? facebook.com, instagram.com... Какво споделям с другите? Какви са моите интереси, лични и политически нагласи, разбирания и ориентация към света.

Професия. Къде работя? Linkedin...
Мнение. Какво мисля? Какви коментари слагам? С кого споря? Проверена ли е информацията, за която претендирам? Технологии за споделяне - коментари, отзиви за места, събития и т. н., които оставяте. maps.google.com/localguides...

Информация за мен. Регистрации в платформи, форуми, участие в онлайн дейности и събития, попълването на анкети и т. н.
Кибер репутация. Какво казват за мен? Отзиви за дейността и коректността ви в отношенията с хората.
Хоби. Какво ме вълнува? Групи, в които членувам, организации, които следвам, места, на които членувам, музиката, която споделям и т. н.

Сертифициране. Кой може да потвърди моята идентичност? Какви лични сертификати качвам онлайн, публикации в интернет, места, на които уча онлайн или работя онлайн. OpenID; ClamID; Nang.
Покупки. Какво купувам? Сайтове, през които пазарувам.
Знание. Какво знам? Публикации в сериозни сайтове или специализирани издания. Wikipedia; Yahoo; Google;
Аудитория. Кого познавам? Каква е моята общност? С кого общувам и каква е ориентацията на аудиторията ви?

Какво е кибертормоз?



Кибертормозът е една от най-честите заплахи, пред които са изправени децата и тийнейджърите онлайн. Може да възникне чрез използване на текстови съобщения, имейл, онлайн игри, приложения за чат, социални медии и онлайн форуми.

Някои често срещани тактики на кибертормоз включват:

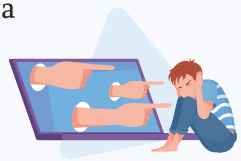
Публикуване на злобни или обидни изображения или коментари. Разпространяване на клюки или слухове в социални мрежи, чатове, форуми, имейли или онлайн игри, които съдържат заплахи, обиди, подигравки и т.н.

„Doxxing“ или разпространяване на лична информация за жертвата в публични форуми

Този конкретен метод на атака включва събиране и публикуване на лична и чувствителна информация за вас онлайн без ваше разрешение. Целта може да е да ви тормозят, заплашват или просто да ви се подигравят. Излага на риск от атака вашата физическа, финансова сигурност и сигурност на идентичността ви.

Кражба на самоличност – пращане на съобщение от ваше име или на вас, но без вие да сте съгласни. Тук се включва и кражбата на пароли или разбиването на акаунти - непозволено влизане в чужд профил в социалните мрежи или в чужд имейл.

Пускане в интернет на снимки или клипове, които ви унижават по какъвто и да е начин. Към този вид спада и пращането на вируси или нежелани файлове, както и на задръстващи пощата имейли.



Емоционални ефекти от кибертормоза

Кибертормоз

Кибертормозът е значителен стресов фактор в живота на младите хора.

Всъщност изследванията показват, че 32% от децата, които са обект на кибертормоз, съобщават, че изпитват поне един симптом на стрес.

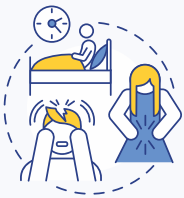
Психични ефекти от кибертормоза

Когато кибертормозът продължава, жертвите може да се отнасят към света около тях по различен начин от другите. За мнозина животът може да изглежда безнадежден и безсмислен.

Те могат да загубят интерес към нещата, които някога са харесвали, и да прекарват по-малко време в общуване със семейството и приятелите.

Физически ефекти от кибертормоза

Да бъдеш мишена на кибертормози може да бъде смазващо, особено ако в това участват много деца. Чувството на претоварване и стрес може да се прояви физически.



Поведенчески ефекти от кибертормоза

Децата, които са обект на кибертормоз, може да проявят същите промени в поведението като тези, които са обект на тормоз офлайн. Например те проявяват загуба на интерес към всякакви дейности и се държат потайно.

В екстремни случаи или когато кибертормозът е продължителен, децата понякога дори показват по-значителни промени в поведението.

Онлайн злоупотреби

Измамите с фишинг се прокарват в различни форми, така че бъдете бдителни, когато някой ви поиска да предостави вашата лична информация по телефона или чрез интернет. Имейлите, които се опитват да извлекат вашето потребителско име, парола, номер на сметка, данни за кредитна карта или друга лична информация, обикновено са фишинг имейли, особено ако не са поискани.

Кражба на кредитна карта. Този тип атака засяга по-големи деца, тийнейджъри и техните родители в зависимост от конкретната ситуация. Киберпрестъпниците използват фишинг имейли и съобщения като начин да превземат онлайн акаунтите ви или да откраднат данни за кредитни карти, които са свързани с тези акаунти.

Шпиониране на уеб камера. Всички устройства, които са свързани към интернет, са потенциално уязвими за атака. В някои случаи киберпрестъпниците избират да се насочат към конкретни устройства или да сканират цели мрежи в търсене на уязвимост, която могат да използват. Това може да включва уеб камери, лаптопи и настолни устройства, смарт телефони и IoT устройства като бебефони, системи за домашна сигурност и камери на звънци.

Интелигентни играчки и свързани устройства. Не винаги са безопасни и е възможно да не защитят поверителността и данните ви. Те може да събират информация от деца, които играят игри. Децата трябва да предоставят много информация само за да играят игра.

Случайно изтегляне на зловреден софтуер. Софтуер, който се инсталира без знанието и разрешението на жертвата и извършва вредни действия на компютъра. Това включва кражба на лична информация от компютъра ви или отвличането му за използване в „ботнет“, което причинява ниска производителност. Киберпрестъпниците често подвеждат хората да изтеглят зловреден софтуер. Фишингът е един такъв трик, но има и други - като убеждаването на жертвите да изтеглят зловреден софтуер, маскиран като игри.

Онлайн злоупотреби

Киберпреследване

Този тип дейност включва някой - дете, тийнейджър или възрастен - да използва различни методи за електронна комуникация, за да ви преследва онлайн. Може да се случва чрез имейл, социални медии, текстови съобщения, телефонни обаждания, както и създаване на фалшиви профили, онлайн публикации и др.

Грумингът (Child grooming) е сред най-опасните видове киберзаплахи за децата. Привличането се случва, когато хищник - обикновено по-възрастен мъж - стане „приятел“ с деца и тийнейджъри. За онлайн хищниците целта е да накарат детето вече да не смята възрастния за непознат и да започне да му се доверява, така че в крайна сметка да пожелае да се срещне лично с цел да го накара да участва в сексуални дейности.

Измамите с изнудване и „сексуално изнудване“ са сред най-често срещаните заплахи, които се срещат в днешно време. Това включва киберпрестъпник, който се интегрира в онлайн кръга от приятелите ви, достига със схема за изнудване до вас, при която твърди, че има една или повече неподходящи ваши снимки, които ще сподели с всички, освен ако не му изпратите други снимки или пари.

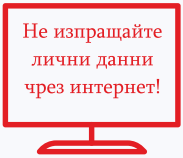
Секстингът може да включва обмен на сексуално открито съдържание — текстове, снимки и/или видео — чрез телефони, компютри или други устройства. Едната страна може да поиска от другата да изпрати свои голи снимки. И изпращачът на изображения, мислейки, че обменът ще остане частен, изпраща изображения, които получателят е възможно след това да сподели с приятелите си или да публикува онлайн.

Порнографията без съгласие , по-известна като порнография за отмъщение. Този тип престъпление включва разпространение или публикуване на сексуално явни изображения на някого без неговото съгласие.

Противопоставяне на кибертормоза

Внимавайте какво споделяте и какво казвате в интернет – нищо не изчезва завинаги от виртуалното пространство, дори и да го изтриете! Мислете, отложете, редактирайте, тогава качвайте!

Не приемайте непознати хора в контактите си с приятели! Запознайте се с настройките за поверителност на използваните приложения! Не се доверявайте на непознати!



Настройте опциите си за местоположение! Ако споделяте местоположението си с хората, то тези хора винаги ще знаят къде се намирате. Някои снимки, направени със смартфони, вече съдържат геотагове, които показват къде е направена снимката. Хората могат да използват тези снимки, за да определят местоположението ви, дори и да не се споменава къде е направена снимката.

Правете одит на социалните си профили – веднъж месечно преглеждайте какво е състоянието на профила ви и чистете неща, които биха ви компрометирали. Това е инвестиция във вашето бъдеще.

Не използвайте профила си през чужди или обществени устройства! Вие не сте единствените, които имат достъп до това устройство и не знаете кой ще седне след вас.

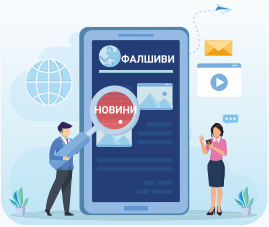
Не отговаряйте на хора, които се опитват да ви кибертормозят! Те търсят емоционална реакция от ваша страна. Ако вие не отговорите, общуването прекъсва! Направете екранна снимка за доказателство, ако се наложи в бъдеще.

Докладвайте за кибертормоз!

Как да разпозная дезинформацията и фалшивте новини?

Фалшивите новини

(Fake news) могат да се разпространяват като горски пожар в социалните медии, като подхранват отрицателни стереотипи, страх и опасно напрежение.



С огромното количество информация, която е налична, как как да пресеете и да намерите само това, което е точно и необходимо?

Обърнете внимание откъде идват вашите новини.

Ако новината идва през вашата емисия в TikTok, Facebook или Instagram, не мислете за това като информация от тези платформи, защото не е.

Запитайте се кой е авторът и каква е предисторията?

Ако статията, отправя обвинения, запитайте се кого облагодетелстват? Какъв е основният изходен материал? Потърсете как се използват източниците и посочват ли се въобще.

Четете отвъд заглавието

Важно е да прочетете историята изцяло. Много често заглавията са подвеждащи и не са там, за да ви информират. Целта на заглавието е да ви накара да кликнете върху връзката и да отворите статията.

Бъдете информирани!

Как да попреча на дезинформацията и фалшивите новини?

Получавайте новините си от различни източници

Ако прочетете нещо и ако реакцията ви е някаква екстремна емоция, възмущение или неограничена радост, това е ясен

индикатор, че определено трябва да четете по-задълбочено. Много от примерите за дезинформация, на които се натъкват различните изследвания, не са предназначени да информират, а по-скоро да активират силен отговор на гняв или страх. Хората трябва да се консултират с допълнителни източници на новини, за да потвърдят информацията, към която изпитват силни чувства.

Когато видите, че вашите приятели и семейство споделят грешна информация, поправете ги

Винаги бъдете любезни, когато помагате на хората да идентифицират дезинформация. Не обиждайте интелигентността на хората. Не повтаряйте лъжи, защото, когато подчертаете нещото, което са сбъркали, те всъщност са по-склонни когнитивно да си спомнят същото. Представете нова информация, която идва от възможно най-реномиран

източник, който може да посочите.

Разберете каква друга информация има там

Когато прочетете нещо, бъдете критични и постъпете експертно - проверете го, прочетете какво са написали други източници по темата. Може да е трудоемко, но бихте могли да намалите паниката.

Не забравяй своите собствени пристрастия – хората са склонни да вярват на неща, които съответстват на техните убеждения.

И Google, и социалните мрежи имат опции за докладване на фалшиви новини.

Организации, институции, закони

Съвети за следващия път. Остани информиран

Никога не забравяй, че всичко, което публикуваш в интернет, губи своя поверителен характер. Публикуването на лична информация в профили, социални мрежи, блогове, чатове може да бъде изключително опасно и да доведе до множество злоупотреби. Не прави и не говори в интернет неща, които не би направил и не би казал и в реалния живот. Мисли кой вижда твоите публикации – приятели, приятели на приятели, напълно непознати хора… Защити се!

БОРБА С КИБЕРПРЕСТЪПНОСТТА ГДБОП-МВР

ГДБОП-МВР в Youtube

Правила, за да си в безопасност в мрежата

Защита на данните и неприкосновеност на личния живот в интернет

Защита на данните и онлайн поверителност

Как да зададете настройките си за поверителност в социалните медии

Брошура за родители - Кибертормозът

Ден за безопасен интернет

Международен ден срещу насилието и тормоза в училище, включително кибертормоза

ЕС срещу фалшиви факти

Бъди в безопасност в интернет

GDPR

Проект
„БЪДИ В БЕЗОПАСНОСТ
В ИНТЕРНЕТ”

Инфо за проекта

Договор № 25-00-54/03.08.2022г., Национална програма за изпълнение на младежки дейности по чл. 10 а от Закона за хазарта за 2022 г., Министерството на младежта и спорта, Република България. Тематична област 4 „Превенция на кибертормоз и злоупотребите онлайн, дезинформацията и разпространение на фалшиви новини“

Проектът „Бъди в безопасност в интернет“ се изпълнява от Сдружение „Национална асоциация за развитие и подкрепа“ – гр. Пловдив
https://narpbg.com/

НАЦИОНАЛНА АСОЦИАЦИЯ ЗА РАЗВИТИЕ И ПОДКРЕПА

http://mpes.government.bg/
Министерство на младежта и спорта
Проектът „Бъди в безопасност в интернет” се осъществява с финансовата подкрепа на Национална програма за изпълнение на младежки дейности по чл.10а от Закона за хазарта за 2022 г., Министерство на младежта и спорта”

МИНИСТЕРСТВО НА МЛАДЕЖТА И СПОРТА

https://cpocreativity.com/
Фирма – подизпълнител на проекта „Креативност“, ЕООД – гр. Пловдив

КРЕАТИВНОСТ
ЦЕНТЪР ЗА ОБУЧЕНИЕ

Използвана литература:
Тофлър, Алвин. Шок от бъдещето, изд. Народна култура, 1992 г.
McCrindle , Understanding Generation Z: Recruiting, Training and Leading the Next Generation, August 2019
Justin W. Patchin, Sameer Hinduja, Bullying Today: Bullet Points and Best Practices (Corwin Teaching Essentials)
https://digitalworldedu.com/
https://europa.eu/youth/home_en
https://nsi.bg/bg
https://sacp.government.bg/
https://www.unicef.org/bulgaria/
Използвани изображения: freepik.com /Premium plan/
Дизайн и изработка: Борис Михайлов