#DigitSafe

2021-1-BE04-KA220-YOU-000029021

IO1.A2 Наръчник

Co-funded by the
Erasmus+ Programme
of the European Union

Съдържание

ВЪВЕДЕНИЕ

Проектът **#DigitSafe,** *Boosting Digital Safe Spaces and Resilience Project"* има за цел да подобри безопасността и неприкосновеността на младите граждани в цифровото пространство, което ще им позволи да се справят с някои от предизвикателствата и отрицателните въздействия на цифровата ера. Това е в съответствие с цел 6, "Информация и конструктивен диалог", от Стратегията на ЕС за младежта 2019-2027 г.

#DigitSafe се стреми да насърчи по-широки и по-задълбочени познания сред младите хора по двете ключови теми: "Киберсигурност и език на омразата" и "Сигурност и неприкосновеност на личния живот". Проектът има за цел да достигне по-специално до най-уязвимите групи млади хора, чрез изграждане на по-безопасни общи цифрови пространства и практики, като същевременно повишава капацитета им по отношение на цифровата сигурност.

Този проект се стреми да постигне и следните три конкретни основни цели:

1. **Да насърчи цифровото гражданство** сред младите хора в участващите държави, като в съответствие със Стратегията на ЕС за младежта 2019-2027 г., им предостави събрана на едно място практическа информация за сигурността и неприкосновеността на личния живот, както и за речта на омразата и кибертормоза.

2. Да предостави на младите хора, особено на тези с по-малко възможности (често без достатъчно знания за дигиталната грамотност), компетентности за постигане на дигитална сигурност.

3. Да разработи иновативна методология, която да пресъздаде събраната в настоящото наръчник важна информация в информационна кампания за повишаване на обществената осведоменост, като използва най-разпространените сред младите хора аудиовизуални комуникационни практики и език, инструменти и тенденции. Тази мултимедийна и многоканална стратегия, която се възползва от огромния брой възможности за създаване на съдържание, достъпни за всеки потребител, предлагани от настоящата среда на социалните медии, има за цел да засили способността на младите хора да правят рационален избор, познавайки своите дигитални права.

Настоящият наръчник за цифрова устойчивост по въпросите на кибертормоза, речта на омразата, сигурността и неприкосновеността на личния живот предлага насоки, практическа информация (от правен и психологически характер, съвети, и ресурси за обучение), както и ключови препоръки по различни въпроси за младежите, за да придобият те по-задълбочени познания за своите права, онлайн рисковете и заплахите в контекста на тези теми.

Наръчникът има за цел да повиши осведомеността относно наличните възможности и ресурси за изграждане на умения за справяне с проблеми, произтичащи от настоящия цифров живот на младите хора.

#DigitSafe

Boosting digital safe spaces and resilience

Co-funded by the
Erasmus+ Programme
of the European Union

1. Кибертормоз

1.1. Какво е кибертормоз?

На европейско равнище има множество определения на кибертормоза, които включват едни или други аспекти в зависимост от специфичните характеристики на всяка от страните, в които е проведено проучването (Белгия, България, Нидерландия и Испания). Въпреки това, проучването, реализирано през 2016 г. от политическия отдел за граждански права и конституционни въпроси към Европейския парламент - "Кибертормоз сред младите хора" - е довело до сравнително точно и хомогенно определение, което може да се използва на транснационално ниво в Европейския съюз:

- "Кибертормозът описва онези ситуации, при които тормозът се осъществява в интернет, най-вече чрез мобилни телефони и социални медии. По този начин кибертормозът съответства на едновременно агресивен и умишлен акт, извършен чрез използването на информационни и комуникационни технологии (ИКТ)."
-

Както и при офлайн тормоза, кибертормозът обикновено включва следните три основни участника:

- **Извършителят:** *Лицето, извършващо агресията.*
- **Жертвата:** *Лицето, страдащо от агресията*
- **Страничните наблюдатели**: *Тези, които виждат какво се случва между насилника и жертвата, но не участват пряко в тормоза.*

Деянието винаги е умишлено и извършено многократно, няма баланс във властовите отношения между агресора и жертвата. Съществуват ключови характеристики на кибертормоза, които улесняват неговото идентифициране и разбиране:

- **Кибертормозът е злонамерен и никога не е случаен.** Извършителят има ясна и съзнателна цел да навреди на жертвата, да ѝ причини болка, да я унижи, да я накара да страда физически или психически.
- **Извършва се от позиция на власт.** Извършителят на кибертормоз винаги има предимство и е в позиция на превъзходство. В зависимост от средата, в която се извършва кибертормозът, той може да означава извършване на кибертормоз в група срещу една жертва, която е сама.

Агресорите могат да се възползват от уязвимостта на жертвата, която не е в състояние да се защити.

- **Това е повтарящо се действие** и има за цел да сплаши, разгневи или злепостави жертвите. Едно изолирано агресивно действие все още не е кибертормоз. То се превръща в кибертормоз, когато агресията се повтаря отново и отново срещу едно и също лице (или едни и същи лица).

Цифровизацията увеличи многократно каналите, по които може да се извършва тормоз чрез интернет. Въпреки това някои от най-често срещаните начини, по които жертвите на кибертормоз биват атакувани, са следните:

Социални мрежи

Мобилни телефони

Платформи за изпращане на съобщения

Платформи за игри

За да изясним кои незаконни действия биха попаднали в обхвата на кибертормоза, ето няколко примера:

- *Разпространяване на лъжи или публикуване на неудобни снимки/видеоклипове на някого в социалните мреж*
- *Изпращане на обидни съобщения или заплахи чрез платформи за съобщения.*
- *Изпращане на злонамерени съобщения под чужда самоличност.*

1.2 Последствия от кибертормоза и как да го разпознаем

Идентифициране на кибертормоза

Един от основните начини за справяне с кибертормоза е да го разпознавате и да следите за предупредителните знаци. Няма общоприето определение за кибертормоз на международно или европейско равнище.

Европейската комисия обаче определя кибертормоза като "повтарящ се вербален или психологически тормоз, упражняван от индивид или група срещу други хора чрез онлайн услуги и мобилни телефони".”(2)

(2)‘Cyberbullying among Young People’, Directorate General for Internal Policies (European Parliament), 2016, p.8.

Според Съвета на Европа кибертормозът се отличава от другите видове тормоз поради риска от публичност, сложната роля на наблюдателите и размера на аудиторията, която се появява с цифровите технологии и комуникации. (3)

За да се създаде един по-толерантен и по-безопасен свят онлайн, кибертормозът трябва да бъде преодолян в по-широк мащаб както на индивидуално, така и на организационно ниво.

Последиците от кибертормоза не могат да се приемат с лека ръка или да се разглеждат като обикновена шега, тъй като това не само отрича емоциите и страданието на жертвата, но и нормализира този вид насилие в цифровата среда. Последиците от кибертормоза могат да бъдат дълготрайни и да засегнат жертвите по много начини.

Бихме могли да изтъкнем като основни последици от кибертормоза:

- **Психически и емоционални последици** жертвите могат да се чувстват тъжни, засрамени, смутени, глупави, депресирани, гневни и тревожни. Жертвите обикновено губят интерес към нещата, които преди са обичали. Развиват по-ниска самооценка или се чувстват изолирани, неспособни да общуват с връстниците си. Понякога жертвите на кибертормоз могат да се превърнат в "жертви-агресори", които възпроизвеждат поведението и тормозят други.(4)

(3) https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)
(4) Joint Research Centre (2013). Social Networks and Cyberbullying among Teenagers

- **Физически последици** Стресът и тревожността, които жертвата изпитва, могат да доведат до физически проблеми, като например чувство на умора поради нарушения на съня или изпитване на реални здравословни симптоми като болки в стомаха или главоболие.
- **Правни последици** Чувството, че са осмивани или тормозени от другите, често пречи на жертвите на кибертормоз да съобщят или да се опитат да се справят с проблема. Това, заедно с бавното развитие на правната квалификация на престъплението, означава, че то често остава ненаказано и насърчава повтарянето на атаките.

Повишаването на осведомеността за кибертормоза с цел предотвратяването му е от съществено значение. Първата стъпка в идентифицирането на кибертормоза е да се даде ясно определение на това какво включва той. В Европа за предотвратяване на кибертормоза са взети политически решения и са определени и приложени множество програми.

Центърът за изследване на кибертормоза е разработил серия от структурирани съвети за това как да действаме, за да предотвратим кибертормоза и да се предпазим като потребители. Превенцията винаги е най-добрият вариант за борба с този проблем.

За младите хора:

- ***Следете настройките за поверителност*** - Социалните медии често променят и актуализират настройките си за поверителност. Уверете се, че сте запознати с новите опции на профила и че запазвате възможно най-много информация само за тези, на които наистина имате доверие.
- ***Ограничавайте достъпа до вашата информация за контакт -*** Не давайте имейл адреса или телефонния си номер на хора, които не познавате. Също така не публикувайте имейла и телефонния си номер в социалните медии.
- ***Научете интернет етикета*** За да предотвратите потенциални проблеми с други потребители в интернет, научете социалния етикет, свързан с взаимодействието в киберпространството.
- ***Не изпращайте неподходящи снимки или видеоклипове*** Помнете че връзките не траят вечно и може да се разделите с вашия партньор, ако той има неподходящи ваши снимки или видеоклипове, би могъл да ги публикува онлайн. Не се поставяйте в положението да се притеснявате за това.

- ***Потърсете се в Google*** - Винаги трябва да знаете какво се говори за вас. Често е изненадващо да откриете, че информация, която сте смятали за лична, се появява в публични бази данни, статии или страници в социалните медии, които са индексирани от търсачките.
- ***Не приемайте покани за приятелство от непознати*** - Ако не познавате лицето, което ви изпраща покана за приятелство, игнорирайте я. Повечето сайтове и приложения на социалните медии ви дават и възможност да блокирате потребителя, ако желаете.

- ***Използвайте опциите за сигурност на конкретния сайт*** - Деактивирайте опциите за търсене в някои социални медии, за да попречите на всеки от широката публика да ви търси или да ви изпраща съобщения. Това ви позволява да имате по-голям контрол върху това с кого взаимодействате онлайн, тъй като само вие можете да инициирате комуникацията.
- ***Защитете информацията си*** - Ако използвате публичен компютър или безжична мрежа, не забравяйте да излезете от всеки сайт, в който сте влезли, когато се отдалечите от компютъра - дори за минута.

- ***Бъдете скептични в онлайн взаимодействията*** - Дори сред хора, на които имате доверие, е рисковано да разкривате твърде много информация, защото никога не знаете със сигурност дали човекът, с когото си мислите, че общувате, наистина е там - или дали е сам.
- ***Пазете се от тролове*** - Не забравяйте, че някои хора имат много свободно време и единственото, което искат, е да навредят на другите. Не им позволявайте да го направят. Не споделяйте твърде много лична информация онлайн, която може да бъде използвана за тормоз или унижение, и не си взаимодействате с такива хора по какъвто и да е начин. Както се казва, не хранете интернет троловете!

За учителите и родителите

Важно е организациите, училищата, работните места и отделните хора да се ангажират с борбата с кибертормоза поради въздействието, което той може да окаже върху жертвите. Изследването, разработено от Центъра за изследване на кибертормоза през 2021 г., "Кибертормозът: идентифициране, превенция и реакция през 2021 г." дава обширно обяснение за това как учителите и родителите биха могли да се справят с кибертормоза по отношение на идентифицирането и превенцията:

Обучението на младите хора за отговорно използване на дигиталните устройства е може би най-важната превантивна стъпка по отношение на образователните институции и ролята на учителите.

С други думи, важно е да започнем да въвеждаме в рамките на формалното образование в училище неформални и информални дейности за борба и превенция на кибертормоза по креативен начин.

От друга страна, **родителите** "трябва да покажат на децата си с думи и действия, че желаят един и същ краен резултат: кибертормозът да спре и животът да не стане по-труден".

Как трябва да реагират родителите, ако открият, че детето им е извършител на кибертормоз? На първо място, те трябва да му обяснят как това поведение провокира и причинява вреда и болка в реалния свят.

След това родителите трябва да могат да му/ѝ дадат възможност да продължи напред и да прекрати това поведение. Децата трябва да знаят, че всяко действие, дори и да е онлайн, има сериозни последствия. От страна на родителите е важно да започнат да обръщат по-голямо внимание на поведението и действията на децата си онлайн.

1.3 Насоки: Как да подкрепяме жертвите на кибертормоз?

(процедури, съпричастност, изслушване, емоционална и психологическа подкрепа)

Когато вие сте жертва

Ако сте жертва на кибертормоз, бихме искали да ви посъветваме да предприемете следните стъпки:

- **Потърсете помощ** - На първо място, трябва да говорите, да обсъждате с роднини или професионалисти!
- **Докладвайте съдържанието** - Ако кибертормозът е бил осъществен чрез социална мрежа, докладвайте съдържанието на тази платформа. Това не винаги е ефективно, но е важно социалната мрежа да знае кой е обвиняемият, за да може да предприеме действия, понякога след няколко доклада.
- **Защитете се** - Сменете паролата си, увеличете поверителността на публикациите си, премахнете лична информация, като например имейл адрес, телефонен номер или връзки към други акаунти. Като временна мярка, **изтрийте профила си или променете псевдонима си.**

- **Свържете се с вашия доставчик на интернет услиги (ISP).** Опитайте се да се свържете с доставчика на интернет услуги на лицето, което ви тормози, ако той е бил идентифициран. След това доставчикът на интернет услуги може да се свърже с лицето или може би директно да закрие неговия интернет акаунт.
- **Подайте жалба в полицейски участък** - Съберете доказателства за атаката (например екранни снимки). Полицията ще запише жалбата ви и цялата информация, свързана с нея, и ще я включи в доклад.
- **Споделете публично за кибертормоза** - Споделете скрийншот на атаката (скрийте потребителското име и профилмата снимка на насилника, за да не бъдете обвинени в клевета).

Като учител:

Учителите трябва да обръщат внимание на различни признаци, които могат да покажат, че дадено дете е обект на кибертормоз. Някои от тези признаци могат да бъдат бързо увеличаване или намаляване на използването на дигиталното устройство или емоционален отговор на това, което се случва на устройството. Ако детето крие екрана или устройството си, когато другите са наблизо, и избягва дискусии, това трябва да се вземе предвид.

Учителите могат да помагат на децата да разпознават, да реагират и да избягват кибертормоза. Някои насоки за това са следните:

- **Комуникацията** е много важна, така че ако мислите, че някое дете е подложено на кибертормоз, поговорете с него насаме и го попитайте за това. Можете също така да поговорите с родител. Учителите могат да бъдат посредници между детето, родителите и училището.

- Насърчавайте **безопасна среда в класа**. Помогнете на децата да развият емоционална интелигентност, за да могат да усвоят умения за самоосъзнаване и саморегулация, и да се научат да проявяват съпричастност към другите.

- Насърчавайте учениците да обръщат внимание на **знаците**, които могат да им помогнат да разпознаят кога в цифровите медии се случва нещо, което ги кара да се чувстват неудобно, притеснени, тъжни или тревожни.
- Научете ги **да мислят, преди да публикуват** нещо онлайн.
- Обяснете на учениците **трите начина, по които могат и трябва да реагират**, ако станат свидетели на кибертормоз: ако подкрепите жертвата на тормоза, вие сте съюзник, ако се опитате да спрете кибертормоза, вие сте поддръжник, а ако сте жертва на кибертормоз, трябва да съобщите за него на възрастен.

Като родител:

Много е вероятно децата да не разпознаят, че са обект на кибертормоз, защото може да се чувстват засрамени. Много често се случва младежите да страдат мълчаливо, без да споделят. Те може да се страхуват, че родителите ще реагират, като ограничат достъпа им до интернет, може да се чувстват смутени, че не могат сами да се справят с тормоза, може да се страхуват, че родителите ще се отнесат към нещата по начин, който засилва тормоза, или че няма да разберат проблема.

Поради тези причини, ако родителите забележат някакви признаци у децата си, трябва да предприемат незабавни действия. На първо място, опитайте се да разговаряте с детето си и да го изслушате.

Най-добрият начин да го направите е да го въвлечете в разговор за това, което се случва, по спокоен начин. Отделете време, за да разберете какво точно се е случило и контекста, в който се е случило.

След като разберете за това, предложете утеха и безусловна подкрепа, тъй като жертвите на кибертормоз често изпитват чувство на изолация. Покажете на детето си, че тази ситуация може да бъде решена по начин, който не включва онлайн отмъщение. Направете така, че детето ви да се чувства в безопасност, това трябва да бъде първостепенен приоритет, както и да му дадете да разбере, че вината не е негова.

Опитайте се да съберете възможно най-много доказателства за случая. Разпечатайте или направете скрийншоти или записи на разговори, съобщения, снимки, видеоклипове и други елементи, които могат да послужат като ясно доказателство, че детето ви е било подложено на кибертормоз.

Следващата стъпка е да се свържете с доставчика на онлайн услугата, тъй като кибертормозът винаги нарушава условията за ползване на всички легитимни доставчици на услуги. Те трябва да предприемат действия по този въпрос, така че детето ви да не пострада отново.

Ако кибертормозът е извършен от съученик или ученик от същото училище като детето ви, трябва да уведомите училището възможно най-скоро, тъй като то може да има правила за реакция при кибертормоз.

Родителите могат да се обърнат и към полицията, в случай че горепосоченото не помогне за подобряване на ситуацията.

Ако е необходимо, опитайте се да потърсите консултация за детето си. Децата могат да имат полза от разговор със специалист по психично здраве. Те може да предпочетат да водят диалог с трета страна, която може да се възприеме като по-обективна.

1.4 Мерки за превенция

Няма сигурен начин да предотвратите кибертормоза. Въпреки това има различни начини да намалите вероятността дадено дете да стане негов обект.

На първо място, важно е да използвате пароли за всичко и да не споделяте тези пароли с никого.

Децата трябва да знаят, че е важно да пазят личните си данни и подробности за личния си живот в тайна. Те никога не трябва да споделят онлайн своя адрес, номер на мобилен телефон или имейл адрес. Трябва да внимават да не споделят твърде много информация за това къде ходят на училище, особено ако имат приятели или последователи онлайн, които не познават добре.

Те също така трябва да знаят, че трябва да излязат от системата, когато използват обществени устройства, като например обществени компютри или лаптопи в училище или в библиотеката.

Накрая, но може би най-важното е, децата да знаят, че ако някога станат жертва на кибертормоз, трябва да съобщят за това на своите родители или учители.

1.5 Как да съобщаваме за кибертормоз?
(правна рамка, институции, НПО и др.)

По отношение на докладването на кибертормоза е важно да знаем, че повечето държави в момента нямат конкретно законодотелство за такива прояви.

Въпреки измеренията на проблема и големият брой случаи, изготвянето на законодателство все още не е в напреднал стадий.

Именно това създава необходимост от работата на институции и организации, които да работят в партньорство, за да идентифицират случаи, да ги изобличават и да окажат подкрепа на жертвите.

Настоящият наръчник разполага с комплирина и систематизирана информация на съществуващите към момента разнообразни механизми за справяне с проблема. Той сам по себе си е опит да се окаже помощ на засегнатите, докато диалогът за законодателни мерки тече.

2. РЕЧ НА ОМРАЗАТА

2.1 Какво е реч на омразата?

Няма общоприето определение за реч на омразата. В този раздел ще представим няколко определения, които са изложени както в законодателството на ЕС, така и от водещи организации, борещи се с речта на омразата.

- (Незаконната) реч на омразата се определя от правото на ЕС като "публично подбуждане към насилие или омраза въз основа на определени характеристики, включително раса, цвят на кожата, религия, произход и национален или етнически произход". Въпреки че рамковото решение се отнася до расизма и ксенофобията, повечето държави членки са разширили обхвата на националните си закони, за да включат и други признаци, като сексуална ориентация, полова идентичност и увреждания. (5)

2.2 Как да предотвратим речта на омразата

Един от начините за борба с речта на омразата е да блокирате и докладвате акаунти на реч на омразата, с които се сблъсквате онлайн (вж. следващия раздел със съвети как да докладвате реч на омразата).

ООН препоръчва да предприемете следните стъпки за предотвратяване на речта на омразата(6):

(5) Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016) https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf
(6) United Nations- how to deal with hate speech? https://www.un.org/en/hate-speech/take-action/engage

- **Пауза** - въздържайте се сами да правите коментари, съдържащи омраза, и/или да споделяте такова съдържание
- **Проверка на фактите** - уверете се, че не откривате невярна и пристрастна информация, преди да разпространявате дезинформация
- **Оспорване** - разпространявайте собствена контрареч и оспорвайте речта на омразата, когато е възможно
- **Подкрепа** - заемете публична позиция и изразете солидарност с жертвите на речта на омразата
- **Докладвайте** - проверете правилата на социалните медии, които използвате, и докладвайте за случаи на реч на омразата, които нарушават тези правила. При по-сериозни случаи може да подадете жалба в полицията (напр. когато има подбуждане към насилие).
- **Образование** - споделяйте образователни ресурси и публични кампании или провеждайте разговори по темата с приятелите и семейството си
- **Ангажирайте се** - обмислете възможността да се присъедините към неправителствена организация или инициатива, която работи за справяне с речта на омразата във вашата общност.

www.un.org/en/hate-speech/take-action/engage

#DigitSafe

2.3 Как да съобщим за реч на омразата?

Потребителите могат да докладват директно за всякакви случаи на реч на омразата чрез самата социалната медия, в която са се сблъскали с тях. Уебсайтът на Съвета на Европа предоставя информация за това как да се докладва за реч на омразата в социалните медии. В някои случаи не е необходимо да имате акаунт, за да докладвате. Например във Facebook можете да попълните този онлайн формуляр, без да имате или да сте влезли в профил във Facebook.

Някои европейски държави са въвели национални процедури и механизми за докладване на случаи на реч на омразата, престъпления от омраза и кибертормоз като част от младежката кампания на Европейския съвет "No Hate Speech Youth Campaign"

Други възможности за докладване на реч на омразата включват:

- Съобщете за речта на омразата в полицията
- Докладвайте на авторитетен орган, например граждански или административен съд
- Докладвайте на неправителствена организация, например MiND - националният център за докладване на реч на омразата и дискриминационно съдържание в Нидерландия
- Поговорете с някого, на когото имате доверие - например родител, приятел, учител

3. КИБЕРСИГУРНОСТ И НЕПРИКОСНОВЕНОСТ НА ЛИЧНИЯ ЖИВОТ

3.1. Защо защитата на личните данни е важна?

Терминът "защита на личните данни" е дефиниран в чл. 4, параграф 1 от Общия регламент относно защитата на данните: лични данни са всяка информация, свързана с идентифицирано или подлежащо на идентифициране физическо лице. Имената и имейл адресите очевидно са лични данни. Информация за местоположението, етническа принадлежност, пол, биометрични данни, религиозни убеждения, уеб бисквитки и политически мнения също могат да бъдат лични данни. В следващите параграфи ще разгледаме по-подробно видовете данни, които изискват защита.

Защитата на данните е важна, тъй като предотвратява злоупотребата с информацията на дадено лице или организация, има за цел да предотврати различни рискове за неприкосновеността на личния живот и сигурността, като например измамни дейности, хакерство, фишинг и кражба на самоличност (описани в следващия раздел).

3.2. Видове заплахи и престъпления, свързани с личните данни и неприкосновеността на личния живот.

1 Кражба на самоличност

Кражбата на самоличност е престъпление, при което се получава лична или финансова информация за друго лице, за да се използва неговата самоличност за извършване на измама, например извършване на неразрешени транзакции или покупки. Кражбата на самоличност се извършва по много различни начини и обикновено жертвите й понасят щети, свързани с техните финанси и репутация. Крадецът на самоличност може да използва информацията ви, за да кандидатства за кредит, да подаде данъчна декларация или да получи медицински услуги.

2 Сексуален тормоз онлайн

Сексуалният тормоз онлайн се определя като нежелано сексуално поведение в която и да е дигитална платформа и се признава за форма на сексуално насилие.

Сексуалният тормоз онлайн обхваща широк спектър от поведения, при които се използва цифрово съдържание (изображения, видеоклипове, постове, съобщения, страници) на различни платформи (частни или публични). То може да накара дадено лице да се почувства заплашено, експлоатирано, принудено, унижено, разстроено, сексуализирано или дискриминирано.

3 Фишинг

Фишинг атаките са практика на изпращане на измамни съобщения, които изглеждат като идващи от надежден източник. Обикновено се извършват чрез електронна поща. Целта е да се откраднат важни лични данни като номера на кредитни карти и информация за вход в профили, или да се инсталира зловреден софтуер на компютъра на жертвата. Фишингът е често срещан вид кибератака, за която всеки трябва да научи, за да може да се предпази ефективно.

4 Интернет измами

Интернет измамите включват използване на онлайн услуги и софтуер с достъп до интернет за измама или извличане на полза от жертвите. Терминът "интернет измама" обикновено обхваща киберпрестъпна дейност, която се извършва по интернет или по електронна поща, включително престъпления като кражба на самоличност, фишинг и други хакерски дейности, предназначени за измама с пари.

5 Измами с поздравителни картички

Много интернет измами се фокусират върху популярни събития, за да измамят хората, които ги отбелязват. Това включва рождени дни, Коледа и Великден, които обикновено се отбелязват чрез споделяне на поздравителни картички с приятели и членове на семейството по имейл. Хакерите обикновено използват това, като инсталират зловреден софтуер в поздравителна картичка по имейл, който се изтегля и инсталира на устройството на получателя, когато той отвори поздравителната картичка.

6 Измами с кредитни карти

Измамите с кредитни карти обикновено се случват, когато хакери придобиват с измама данните на кредитни или дебитни карти на хора, за да откраднат пари или да направят покупки.

За да се сдобият с тези данни, интернет измамниците често използват привидно много примамливи оферти за кредитни карти или банкови заеми, за да примамят жертвите. Жертвата може да получи съобщение от банката си, в което се казва, че отговаря на условията за специална кредитна сделка или че й е предоставена огромна сума пари назаем.

7 Измами с онлайн запознанства

Друг типичен пример за интернет измама е фокусиран към множеството приложения и уебсайтове за онлайн запознанства. Хакерите използват тези приложения, за да подмамят жертвите да изпращат пари и да споделят лични данни. Измамниците обикновено създават фалшиви профили, за да общуват с потребителите, да развият връзка, бавно да изградят доверие с тях, да създадат фалшива история и да поискат от потребителя финансова помощ.

8 Измама с печалба от лотария

Друга често срещана форма на интернет измама са измамите по имейл, които съобщават на жертвите, че са спечелили от лотарията. Тези измами информират получателите, че могат да получат наградата си само след като платят малка такса.

9 Нигерийският принц

При измамата се използва историята за богато нигерийско семейство или лице, което иска да сподели богатството си в замяна на помощ за получаване на наследство. При нея се използва тактика на фишинг за изпращане на имейли, в които се описва емоционална история, след което жертвите се подмамват с обещание за значително финансово възнаграждение. Обикновено измамата започва с искане на малка такса за помощ при правни процедури и оформяне на документи с обещание за голяма сума пари по-нататък.

10 Спам

Спамът е всякакъв вид нежелана, непоискана цифрова комуникация, която се изпраща масово. Често спамът се изпраща по имейл, но може да се разпространява и чрез текстови съобщения, телефонни обаждания или социални медии.

3.3. Как да съобщаваме за заплахи за киберсигурността в социалните медии/институции

Всички социални мрежи имат създадени механизми за докладване на различни видове заплахи за киберсигурността, включително онлайн реч на омразата, кражба на самоличност, сексуален тормоз, кибертормоз и др.

Ето информация за някои от най-популярните социални мрежи:

Facebook

- Проблемите със сигурността във Facebook се разделят на няколко категории. Възможно е да има страница със злоупотреба или омраза, която искате да докладвате, или някой да се представя за вас във Facebook и т.н. Най-добрият начин да докладвате за обидно съдържание или спам във Facebook е като използвате връзката Докладване в близост до самото съдържание.

https://www.facebook.com/help

Twitter

- Ако имате въпроси, притеснения или проблеми с профила си, можете да намерите информация и подкрепа тук. В раздела **Безопасност** можете да видите опцията **Докладване на проблем**

https://help.twitter.com/en

Instagram

- *Докладване на публикации*

Ако видите публикация, съобщение или акаунт, които смятате, че са в разрез с Насоките за общността на Instagram, можете да ги докладвате. Можете да докладвате отделни части от съдържанието, като докоснете трите точки над публикацията, като задържите съобщението или като посетите профила и докладвате директно от него. За повече информация посетете Центъра за помощ на Instagram

- *Докладване на акаунти*

Акаунти, които нарушават Насоките за общността на Instagram, могат да бъдат докладвани в приложението или чрез уеб формуляр. За повече информация можете да се обърнете към Центъра за помощ.

https://help.instagram.com/

TikTok

- Ако имате въпроси, притеснения или проблеми с профила си, можете да намерите информация и подкрепа тук. В раздела ***Безопасност*** можете да видите опцията **Докладване на проблем** и да докладвате за видеоклип на живо, коментар на живо, видеоклип, коментар, директно съобщение, звук, хаштаг, а също така можете да докладвате някого. Стъпките са много лесни за изпълнение, просто трябва да намерите опцията **Докладване** и да следвате инструкциите.

https://support.tiktok.com/en/

3.3. Как да избегнете рисковете за сигурността на данните

Силната парола е най-доброто ви оръжие за защита на личните. Тя ще ви бъде много полезна, тъй като в днешно време киберпрестъпниците не спират да измислят нови и иновативни начини за хакване на акаунти и получаване на лични данни.

Силно препоръчително е да използвате само уебсайтове, на които имате доверие. Много хора не знаят как да проверят надеждността на един уейбсайт, ето няколко полезни насоки:

1. Първо, проверете дали URL адресът се изписва правилно, дали е защитен с "https" и дали има някакъв индикатор, че е проверен, например знак за заключване.

2. Запомнете - уебсайтовете, които изглеждат опасни, обикновено са такива. Ако собственикът на уебсайта не инвестира във външния вид и потребителското изживяване, той вероятно не инвестира и в сигурността на сайта. Следователно тези сайтове са податливи на зловреден софтуер, който може да бъде заплаха за вашата сигурност.

3 Важно е на уебсайта да има налична информация за контакт, както и достъпна политика за поверителност. Те обикновено се намират в най-долната част на началната страница. Друг полезен съвет е да прочетете някои свидетелства и отзиви за сайта от други хора, за да се запознаете с опита, който други хора са имали, използвайки тези уебсайтове.

Съществуват и други практики, които могат да изложат на риск цифровата сигурност, като например използването на публичен ***WIFI.***

Вярно е, че тази услуга, която някои хотели и летища предоставят, е безплатна, но трябва да сме много предпазливи. Тези безплатни WIFI горещи точки позволяват на хакерите да се позиционират между лицето, което ги използва, и т.нар **hotspot** (точката за връзка). Съществува риск от това личните ни данни да попаднат в ръцете на хора, които е използват за измами.

Как да защитим личните си данни?

1. Защитете онлайн акаунтите си

2. Защитете сърфирането си в интернет

3. Използвайте антивирусен софтуер на компютъра си

4. Актуализирайте софтуера и устройствата си

5. Не инсталирайте софтуер, който не познавате и на който нямате пълно доверие

6. Деактивирайте Bluetooth, когато не го използвате

7. Бъдете изключително предпазливи, когато споделяте лична информация

8. Внимавайте за имитатори

9. Не споделяйте твърде много информация в платформите за социални мрежи

10.Персонализирайте настройките си за поверителност в социалните мрежи

11. Не забравяйте да излезете от акаунта си

12. Не отваряйте на имейли от хора, които не познавате

13. Не запазвайте пароли в браузъра си

14. Не използвайте идентификационните данни от социалните медии, за да се регистрирате или да влизате в сайтове на трети страни

15. Изберете сигурен и надежден доставчик на електронна поща

4. ЗАКЛЮЧЕНИЕ

В този наръчник се стремим да дадем обяснение и представим повече контекст за явленията **кибертормоз** и **реч на омразата.** Определенията им варират в различните страни, но и двете се считат за проява на агресия.

При ***кибертормоза*** обикновено има три страни (извършител, жертва и странични наблюдатели), докато при ***речта на омразата*** обикновено имаме лицето, което дискриминира, и жертвата, която е дискриминирана.

Настоящият наръчник включва съвети и методи за идентифициране на проблемите, свързани с кибертормоза и речта на омразата, както и стъпки за докладването на тези прояви. Представили сме начините за справяне с проблема, в зависимост от това кой е жертвата (вие, ваш колега/съученик, вашето дете и т.н), както и полезна информация за законовата рамка в различни държави.

В Испания например можете да подадете сигнал в полицията, докато в Нидерландия има национална телефонна линия за помощ при дискриминация.

В наръчника е обяснено и защо са важни понятия като защита на данните, както и видовете заплахи за неприкосновеността на личния живот, като кражба на самоличност, сексуален тормоз онлайн, фишинг или онлайн измами.

В заключение, настоящият документ съдържа организирана информация за ключови понятия и съвети по отношение на кибертормоза и речта на омразата, като може да послужи с полезни насоки при сблъсък с тези явления.

#DigitSafe
Boosting digital safe spaces and resilience

Co-funded by the
Erasmus+ Programme
of the European Union

ЗА ВЪПРОСИ И ПОВЕЧЕ ИНФОРМАЦИЯ :

info@digit-safe.com

www.digit-safe.com