#DigitSafe

2021-1-BE04-KA220-YOU-000029021

IO1.A2 Наръчник

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

#DigitSafe

"**#DigitSafe-Boosting digital safe spaces and resilience**" има за цел да даде възможност на младите хора да се превърнат в устойчиви и безопасни цифрови граждани, което ще им позволи да се справят с някои от предизвикателствата и отрицателните въздействия на цифровата ера.

Партньори по проекта:

CONEXX-EU

inova aspire

CESUR
Tu Centro Oficial de FP

alma radio

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

Съдържание

Въведение

Проектът **"#DigitSafe-Boosting digital safe spaces and resilience"** следва стратегията на ЕС за младежта за периода 2019-2027 г. и е в съответствие с цел 6 на ЕС за младежта "Информация и конструктивен диалог", като има за цел да даде възможност на младите хора да се превърнат в «дигитални граждани», което ще им позволи да се справят с някои от предизвикателствата и отрицателните въздействия на цифровата ера.

Проектът #DigitSafe се стреми да насърчи по-широки и по-задълбочени познания сред младите хора по двете ключови теми - "Кибертормоз и реч на омразата" и "Сигурност и неприкосновеност на личните данни и личния живот", по-специално сред най-уязвимите групи млади хора, да изгради по-безопасни общи цифрови пространства и практики, както и да повиши техния капацитет по отношение на цифровата устойчивост.

Проектът също така има следните три конкретни цели:

- Да насърчи дигиталното гражданство сред младите хора в участващите страни, като в съответствие със Стратегията на ЕС за младежта 2019-2027 г. им предостави практическа информация относно сигурността и неприкосновеността на личния живот, речта на омразата и кибертормоза.
- Да развие у младите хора, особено у тези с по-малко възможности, които често нямат изградена необходимата дигитална грамотност, компетентности за постигане на дигитална сигурност.
- 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. То 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. наръчникто дава възможност на младите хора да станат ангажирани дигитални граждани в един по-безопасен цифров свят. То събира значително количество информация, която е обобщена и структурирано представена.

Документът е разделен на два модула:

- Кибертормоз и реч на омразата
- Сигурност и неприкосновеност на личните данни и личния живот,

Те предоставят информация не само относно правната рамка, повишаването на осведомеността и превенцията, но и предлагат конкретни насоки за действие, съвети и препоръки за справяне с тези проблеми.

1. Кибертормоз

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"[1] - 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 - *Лице, извършващо агресията.*

Жертвата - *Лице, което страда от агресията.*

Странични наблюдатели - *Тези, които виждат какво се случва между тормозещия и жертвата, но не участват пряко в тормоза.*

По отношение на участващите лица е важно да се подчертае, че има важна разлика между тормоза и кибертормоза и тя е, че при

[1] Céline Chateau. (2016). *Cyberbullying among Young people.* European Parliament. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

кибертормоза извършителят (насилникът) може да остане анонимен, може да се скрие под фалшива самоличност (или под чужда самоличност), като зад тази самоличност може да се крият дори няколко души. Въпреки това кибертормозът оставя електронна следа, която може да послужи като доказателство и средство за спиране на подобно поведение. За съжаление, въпреки тази разлика, тормозът лице в лице и кибертормозът често се проявяват паралелно.

Съществуват и някои ключови характеристики на кибертормоза, които улесняват неговото идентифициране и разбиране:

- Кибертормозът **е злонамерен и никога не е случаен.** Кибертормозът 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. Също така агресорите могат да се възползват от неагресивна или уязвима жертва, която не е в състояние да се защити.

- То **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.***
- ***Платформи за изпращане на съобщения.***
- ***Платформи за игри.***
- ***Мобилни телефони.***

За да изясним кои действия попадат в обхвата на кибертормоза, ето няколко примера, които биха били определени като такъв:

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

1.2 Научете повече за значението на кибертормоза и последствията от него. Повишаване на осведомеността, как да го разпознаваме:

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]. 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].

WiredSafety, (най-голямата група за онлайн безопасност, обучение и помощ в света) не е съгласна с предложението кибертормозът да се квалифицира като "повтарящ се", тъй като може да не е необходимо някои сериозни случаи на кибертормоз да се повтарят, за да бъдат квалифицирани като кибертормоз. Например:

- Секс изнудване, секст тормоз и значими атаки срещу репутацията (например такива, свързани със сексуални предпочитания, сексуална активност и други видове атаки срещу репутацията, представляващи клевета)
- Смъртни заплахи или заплахи за сериозно телесно увреждане на жертвата или на някой близък на жертвата, предназначени да я притеснят[4].

[2] 'Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.8.
[3] https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)
[4] Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, *Council of Europe* (2017)

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

Според доклад на Европейския парламент от 2016 г. прякото участие на децата в разработването на решения и политики, свързани с кибертормоза, е признато за един от най-ефективните методи за справяне с проблема[5]. Освен това в доклад до Съвета на Европа от 2017 г. се стига до заключението, че за да се справим с кибертормоза, гласовете на младите хора трябва да бъдат представени и чути на европейско и национално равнище[6]. Следователно е ясно, че гласовете на младите хора трябва да бъдат на преден план в тези дискусии.

Последиците от кибертормоза не могат да се приемат с лека ръка или да се разглеждат като 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. В някои крайни случаи кибертормозът може да доведе дори до самоубийство. Консорциумът #DigitSafe стигна до тези заключения след интензивни проучвания, проведени на европейско равнище в четири държави, и свидетелствата на жертви на кибертормоз, събрани в рамките на проекта. Докладът за социалните мрежи и кибертормоза сред тийнейджърите, разработен от Съвместния изследователски център (JRC), спомага да се разбере обхватът на последиците от кибертормоза за жертвите му:

- **<u>Психически и емоционални последици</u>**

Жертвите могат да се чувстват тъжни, засрамени, смутени, глупави, депресирани, гневни и тревожни. Жертвите обикновено губят интереса си към нещата, които 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[7] .

С други думи, съществува реален шанс кибертормозът да причини дълбока психологическа вреда на жертвите. Жертвите на кибертормоз[8]:

- ❖ Е по-вероятно да страдат от депресия и тревожност

[5] Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.11

[6] Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, *Council of Europe* (2017) p.44

[7] Joint Research Centre (2013). Social Networks and Cyberbullying among Teenagers. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

[8] ttps://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)

- ❖ Е по-вероятно е да страдат от слаби академични постижения и проблеми с поведението в училище
- ❖ По-често изпитват трудности при развиването на основни компетентности и ценности като емпатия, уважение към другите, отвореност към други култури и вярвания, толерантност и самооценка

Физически последици

Стресът и безпокойството, които жертвата изпитва, могат да доведат до физически проблеми, като например чувство на умора поради нарушения на съня или реални здравословни симптоми като болки в стомаха или главоболие.

- **Правни последици**

Чувството, че другите им се подиграват или ги тормозят, 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, за да се предотврати той, е от съществено значение. Първата стъпка в идентифицирането на кибертормоза е да има ясно определение за това какво включва той. В Европа за предотвратяване на кибертормоза са взети политически решения и са определени и приложени множество програми. Въпреки това въздействието, което това явление оказва, показва, че европейските институции трябва да продължат да реализират изследвания, да приемат закони и да насърчават колективни и индивидуални действия за справяне с него[9].

Към младите хора:

Центърът за изследване на кибертормоза[10] 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.

- ***Следете настройките за поверителност.***

[9] Rizza C, Martinho Guimaraes Pires Pereira A. Social Networks and Cyber-bullying among Teenagers. EUR 25881. Luxembourg (Luxembourg): Publications Office of the European Union; 2013. JRC80157

[10] Cyberbullying Research Centre. (2021.)Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online

Социалниет 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 информацията си 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. Никога не знаете кой може да има достъп до тях и не можете да се доверите на всеки, който ви е "приятел" или "последовател".

- ***Научете интернет етикета***

За да предотвратите потенциални проблеми с други потребители в интернет, научете социалния етикет, свързан с взаимодействието в киберпространството. Например, не пишете с главни букви. За някои това може да се възприеме като викане. Също така се въздържайте от използването на сарказъм онлайн, тъй като той лесно може да бъде изтълкуван погрешно.

- ***Не изпращайте неподходящи снимки или видеоклипове.***

Не забравяйте, че може да се разделите със сегашното си гадже или приятел/ка и не искате някой, който има неподходящи ваши снимки или видеоклипове, да ги публикува онлайн и да ги сподели с останалия свят. 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 молби за приятелство от непознати***

Ако не познавате лицето, което ви изпраща молба за приятелство, игнорирайте я. Повечето сайтове и приложения на социалните медии ви дават и възможност да блокирате потребителя, ако желаете.

- ***Използвайте контрол, базиран на сайта***

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.

- ***Запазете информацията си защитена***

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. Всъщност правете това и на другите си мобилни устройства, ако има вероятност някой да дойде и да използва профила ви. Не давайте пароли на никого и често сменяйте паролата си. Също така се уверете, че телефонът и таблетът ви имат код за достъп и са заключени.

- ***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 направят живота на другите нещастен. 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!

<u>Към учителите и родителите</u>

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."***[11] 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. Това става и чрез налагането на дисциплина на учениците, които се занимават с тормоз или заплахи към други хора, и информирането им, че това, което правят, е повече от неправилно, то е престъпление.

От съществено значение е в различните области на учебните програми на образователните институции да се включи подходящо онлайн съдържание, в което да се обсъжда кибертормозът наред с други цифрови заплахи. Освен това посланията могат да бъдат подсилени и в други часове, особено в тези, в които се използват дигитални технологии и инструменти.

[11] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

Разработването на нови и креативни стратегии за борба с кибертормоза става все по-важно в днешно време, особено за да се посрещнат по-началните форми на тормоз, както и за да се предотвратят. Изследователите Хиндуджа и Пачин (2021 г.) от Центъра за изследване на кибертормоза дават различни примери:

- Учениците могат да имат задачата да създадат плакати срещу кибертормоза, които да бъдат изложени в цялото училище, или видеоклип, в който да се предаде послание срещу тормоза и/или за доброто отношение към другите.
- По-големите ученици може да направят кратка презентация пред по-малките ученици за значението на използването на технологиите по етичен начин.

Смисълът тук е да се осъди поведението (без да се осъжда детето) и същевременно да се изпрати послание до останалата част от училищната общност, че тормозът под каквато и да е форма е лош и няма да бъде толериран[12].

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 и двамата желаят един и същ краен резултат: кибертормозът да спре и животът да не стане по-труден"[13].

Центърът за изследване на кибертормоза подчертава колко е важно родителите да не се отнасят пренебрежително към гледната точка на децата си, а да утвърждават техния глас и мнение. Изключително важно е мишените на кибертормоза и страничните наблюдатели да знаят, че възрастните, тъй като са запознати със ситуацията на кибертормоз, *"ще се намесят рационално и логично и няма да влошат положението"*[14].

[12] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf
[13] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf
[14] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

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.

Изследователите Хиндуджа и Пачин (2021) предлагат на родителите ***"да култивират емпатия, като умишлено ги поставят в ситуации, които ги карат да се чувстват неудобно и които могат да смекчат сърцето им".***

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):

Съветите за това как да се процедира са формирани основно от предложенията на Центъра за изследване на кибертормоза и Amnesty Jeunes.

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 за 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.**

- Опитайте се да се изключите от социалните мрежи за известно време, **блокирайте лицето, което е източник на кибертормоз.**

- Отговорете и **напомнете на лицето, което ви тормози, за правната рамка**, като посочите, че онлайн тормозът е престъпление, което се наказва от закона.

- Ако това се случва в работна среда, **говорете с работодателя си.**

- **Уведомете работодателя си, ако лицето, което ви тормози, е ваш колега/съученик,** или ако тормозът се случва в свързан с работата форум или блог. Ако тормозът ви пречи да си вършите работата, работодателят ви трябва да знае за това.

- **Прекъснете връзките**
  Не се сприятелявайте с тези, които са злонамерени, и не се опитвайте да ги накарате да се сближат с вас. Ако смятате, че трябва да отговорите на човека, който ви тормози, направете го с уважение. Не се опитвайте да рационализирате или да се сприятелявате с някого, който е жесток към другите.

- **Не реагирайте гневно**

Тези, които упражняват кибертормоз, искат да реагирате. Ако реагирате гневно, агресорът ще продължи (и дори да увеличи интензивността на) кибертормоза. Освен това отговорът ви може да има последствия.

- **Свържете се с доставчика на интернет услуги**

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, като отидете в полицейски участък**

Вземете доказателства за атаката (например снимки на екрана). Полицията ще запише жалбата ви и цялата информация, свързана с нея, и ще я включи в доклад. Те ще ви дадат копие от доклада и удостоверение за подадена жалба. След това докладът се изпраща на прокуратурата, т.е. на хората, които отговарят за разследванията.

Поискайте номера на доклада, за да можете да проследите случая и да знаете коя прокуратура е компетентна.

- **Съобщете за кибертормоза публично**

Споделете снимки на екрана на от съобщението,(не забравяйте да скриете потребителското име и профилната снимка на агресора, за да не ви обвинят в клевета).

Като колега/съученик (на работа или в училище)

В тази област организацията "Save the Children"[15] много точно е посочила някои насоки за това как да се действа в случай на тормоз:

- В тази ситуация може да почувствате страх или отхвърляне, но действайте.
- Ако виждате, че не можете да го спрете сами и че не е най-добре да постъпите така, помолете за помощ възрастен или отговорно лице. Това не е доносничество, а подкрепа за тези, които се нуждаят от нея.
- Подкрепете колегата/съученика, който е подложен на тормоз. Никой не заслужава да бъде третиран зле.
- Предложете провеждане на обучение или разработване на материали за повишаване на осведомеността във вашата образователна институция или компания за предотвратяване на кибертормоза и търсене на помощ.

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.

[15] Save the children. Advice for students on how to deal with bullying. https://www.savethechildren.es/publicaciones/consejos-para-estudiantes-frente-al-bullying-o-acoso-escolar

- 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.

<u>Като родител</u>

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. За детето ви е много важно да не омаловажавате ситуацията. Тъй като социалните медии са се превърнали в продължение на ежедневието на децата, един неприятен коментар или текст може да бъде опустошителен за тях. **Да похвалите детето си за това, че е постъпило правилно, като поговори с вас за това, е добър начин да повишите доверието между вас двамата.**
- 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. Записвайте всички инциденти, за да подпомогнете процеса на разследване. Също така записвайте важни подробности като място, честота, тежест на вредата, участие на трети лица или свидетели и предистория.
- 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. Добър начин за подобряване на сигурността на децата онлайн е използването на инструментите и настройките за поверителност, предоставени от социалните медии. Трябва да се уверим, че децата са запознати с настройките и инструментите за поверителност, предлагани от доставчиците на услуги, и да зададем най-сигурните настройки за поверителност на всеки профил в социалните мрежи. Това означава да направите профилите си лични, да предотвратите отбелязването им от хора и т.н.

- **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. Това включва излизане от електронната поща, акаунти в социалните медии, училищния им акаунт или всеки друг акаунт, който могат да отворят.
- **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, неправителствени организации и т.н.)

Един от най-значимите аспекти на докладването на кибертормоза е, че в повечето европейски държави няма специално законодателство за кибертормоза. Въпреки важността, големия брой случаи и загрижеността сред младите хора, законодателството все още не е постигнало напредък в тази област. Поради това от съществено значение е работата на институциите и организациите, които помагат за идентифицирането на случаите, тяхното разобличаване и оказването на подкрепа на жертвите.

- **Белгия**

Правна рамка

В Белгия кибертормозът се разбира като "криминално престъпление", поради което е обект на наказателно преследване. Въпреки това, както и в много други държави, няма специален наказателен закон по отношение на кибертормоза.

Това обаче не означава, че престъпното деяние остава ненаказано, а по-скоро, че това става чрез други белгийски закони:

- Чл. 442 bis и чл. 442 ter от белгийския Наказателен кодекс = Тормоз.

"Всеки, който публично изрича вредни лъжи, които могат да навредят на чуждата чест или репутация, извършва нарушение на чл. 442 от Белгийския наказателен кодекс".

- Чл. 422 bis от белгийския Наказателен кодекс = Преследване

- Чл. 145.3bis от Закона от 13.06.2005 г. по отношение на електронната комуникация, обидата и клеветата

- Чл. 448 от белгийския Наказателен кодекс = Публични обиди

- Чл. 383 от Наказателния кодекс на Белгия= Публично непристойно поведение

В сферата на трудовото законодателство, кибертормозът е сравнително нов и неизследван феномен, въпреки повсеместното използване на ИКТ в съвременната работна среда и условия на труд. Наскоро приетата Конвенция на МОТ за насилието и тормоза, 2019 г. (№ 190), и придружаващата я Препоръка № 206 включват в обхвата си насилието и тормоза, които се случват и „чрез комуникации, свързани с работата, включително тези, които са възможни благодарение на информационните и комуникационните технологии“. В Белгия тези разпоредби са включени в законодателството в областта на здравословните и безопасни условия на труд.

Институции и неправителствени организации

В Белгия, ако *кибертормозът се прояви в учебно заведение, вътрешните разпоредби и правила позволяват на тези институции да налагат санкции срещу него.*

Освен това има някои *организации и платформи, които оказват подкрепа и ориентират жертвите, които търсят помощ* преди съдебния процес, който в повечето случаи е сложен, труден и травмиращ за младия човек.

- CyberHelp

Съвместна инициатива на белгийската федерална полиция, университета в Монс и Федерацията Валония-Брюксел. Това е приложение срещу кибертормоза, с което можете да съобщите за него чрез собствения си смартфон. Приложението включва бутон, който позволява да се направи скрийншот на историята на чата, който включва кибертормоз, и втори бутон, чрез който това съдържание може да се изпрати на хората, отговарящи за справянето с подобни ситуации в учебното заведение. През 2021 г. екипът на CyberHelp представи приложението на 12 000 ученици, като направи около 100 посещения в училища във Валония и Брюксел.

- Amnesty Jeunes Belgium

- Télé-Accueil Bruxelles

Télé-Accueil е телефонна и чат услуга. Всеки, който желае да намери "някого, с когото да поговори", намира такъв човек на номер 107, безплатно, 24 часа в денонощието, 7 дни в седмицата, в условията на анонимност и поверителност. Това е чудесна възможност за онези жертви, които поради срам или незнание, не могат да се справят с кибертормоза, киберпрестъпленията или речта на омразата, и получават помощ и човек, който да ги изслуша и посъветва.

- **Испания**

При кибертормоза трябва да се обърне внимание на няколко неща. Първо, не отговаряйте и не препращайте съобщенията за кибертормоз и блокирайте лицето, което ви тормози. Важно е да съхранявате доказателства за кибертормоза. Записвайте датите, часовете и описанията на кибертормоза.

Възможно е да съобщите за тормоза както в платформата, в която се извършва, така и по законов път, например в полицията.

Когато подавате сигнал чрез платформата, първо прегледайте нейните общи условия или разделите за права и отговорности. В тях се описва съдържанието, което е или не е подходящо, и след това докладвайте за кибертормоз на социалната медия, за да може тя да предприеме действия срещу потребители, злоупотребяващи с условията за ползване.

От друга страна, когато кибертормозът предполага заплахи за насилие, детска порнография или изпращане на съобщения или снимки със сексуално съдържание, или преследване и престъпления от омраза, той се счита за престъпление. В тези случаи трябва да се докладва на полицията.

Съществуват фондации, които предлагат подкрепа и помощ на онези деца или юноши и техните семейства, които не знаят как да се справят с този проблем или как да го докладват. Например:

- **Cybersmile** (https://www.cybersmile.org/who-we-are). Това е организация с нестопанска цел, ангажирана с цифровото благополучие и борбата с всички форми на тормоз и злоупотреба онлайн.

- **AEPAE** (https://aepae.es/plan-nacional). Това е Асоциация за превенция на тормоза в Испания. Целта на тази асоциация е да развива превантивно поведение у децата и юношите, насочено към разрешаване на конфликти в училищната среда.

- **INFOACOSO** (https://infoacoso.es/telefonos-de-ayuda-contra-el-acoso-y-el-bullying). Тази асоциация предлага на своя уебсайт наръчник за това как да действате, ако сте обект на кибертормоз, и къде да се обадите, за да съобщите за него, в зависимост от региона на Испания, в който живеете.

- **Нидерландия**

В Нидерландия следните институции и органи могат да ви помогнат, ако сте станали жертва на кибертормоз:
● **MiND** - горещата линия за дискриминация в интернет, която регистрира и оценява сигнали за дискриминация в интернет.
● **Обърнете се към служба за борба с дискриминацията** във вашия район. Всички общини в Нидерландия разполагат със служба за борба с дискриминацията, към която можете да се обърнете с въпрос или оплакване за дискриминация.
● **Обадете се на националната телефонна линия за помощ при дискриминация** (0900 235 5345)
● **Свържете се с полицията,** ако сте били тормозени, сплашвани, заплашвани и др.

Някои от горепосочените услуги са специфични за тези, които са се сблъскали с дискриминация. Обикновено дискриминацията се определя като неравностойно третиране на друго лице въз основа на неговата етническа принадлежност, пол, полова принадлежност или генетични характеристики. Дискриминацията е забранена от законодателството на ЕС:

Член 21: "Забранява се всякаква дискриминация, основана на признаци като пол, раса, цвят на кожата, етнически или социален произход, генетични характеристики, език, религия или убеждения, политически или други възгледи, принадлежност към национално малцинство, имотно състояние, рождение, увреждане, възраст или сексуална ориентация".[16]

[16] Article 21 EU law: Non discrimination https://fra.europa.eu/en/eu-charter/article/21-non-discrimination#:~:text=EU%20Charter%20of%20Fundamental%20Rights.-Previous%20title&text=1..2.

Тъй като кибертормозът има много форми, може да се почувствате жертва на кибертормоз, който не е конкретно дискриминационен. В тези случаи някои предложения са:

● Съобщете за кибертормоза в училището/работата (ако сте подложени на тормоз от някой на мястото, където учите/работите)
● "Спри онлайн тормоза" е холандска схема за интервенция, съобразена с нуждите на жертвите на кибертормоз с по-ниско образование, която има за цел да научи жертвите как да се справят с кибертормоза и неговите отрицателни последици.
● Блокирайте и докладвайте за кибертормоза в каналите си в социалните медии
● Блокирайте и докладвайте номера на тормозещия
● Поискайте информация от местното полицейско управление
● Подайте официален сигнал в полицията (ако това се възприема като най-добрия начин на действие след обсъждане с полицейското управление)

В Нидерландия на училищата са възложени конкретни отговорности за борба с кибертормоза и за неговото предотвратяване. Например програмата KiVa има за цел да подобри безопасността на учениците в училищата и се финансира с безвъзмездни средства от нидерландското министерство на образованието.

Програмата **KiVa** е финландска програма за борба с кибертормоза, базирана на научни изследвания и доказателства, която първоначално е разработена от Университета в Турку и е прилагана в училища по целия свят. Тя се основава на три основни елемента: превенция, интервенция и мониторинг[17].

● **Превенция:** в училищата се прилагат превантивни действия, като например програмата KiVa, които са насочени към предотвратяване на тормоза.
● **Интервенция:** Техниките за интервенция на KiVA са насочени към деца, които са били пряко въвлечени в тормоз. Целта е да се предоставят на училищата и учениците инструменти, насочени към намиране на решения.
● **Годишен мониторинг:** Годишните проучвания за учениците и персонала в училищата KiVa се използват за наблюдение на ефективността на програмата и за предоставяне на информация за това как да се подобри работата им за борба с тормоза.

От програми като KiVa могат да се извлекат поуки, които да се приложат към отделни хора и организации по целия свят. Очевидно е, че

[17] What is KiVa? https://www.kivaprogram.net/what-is-kiva/

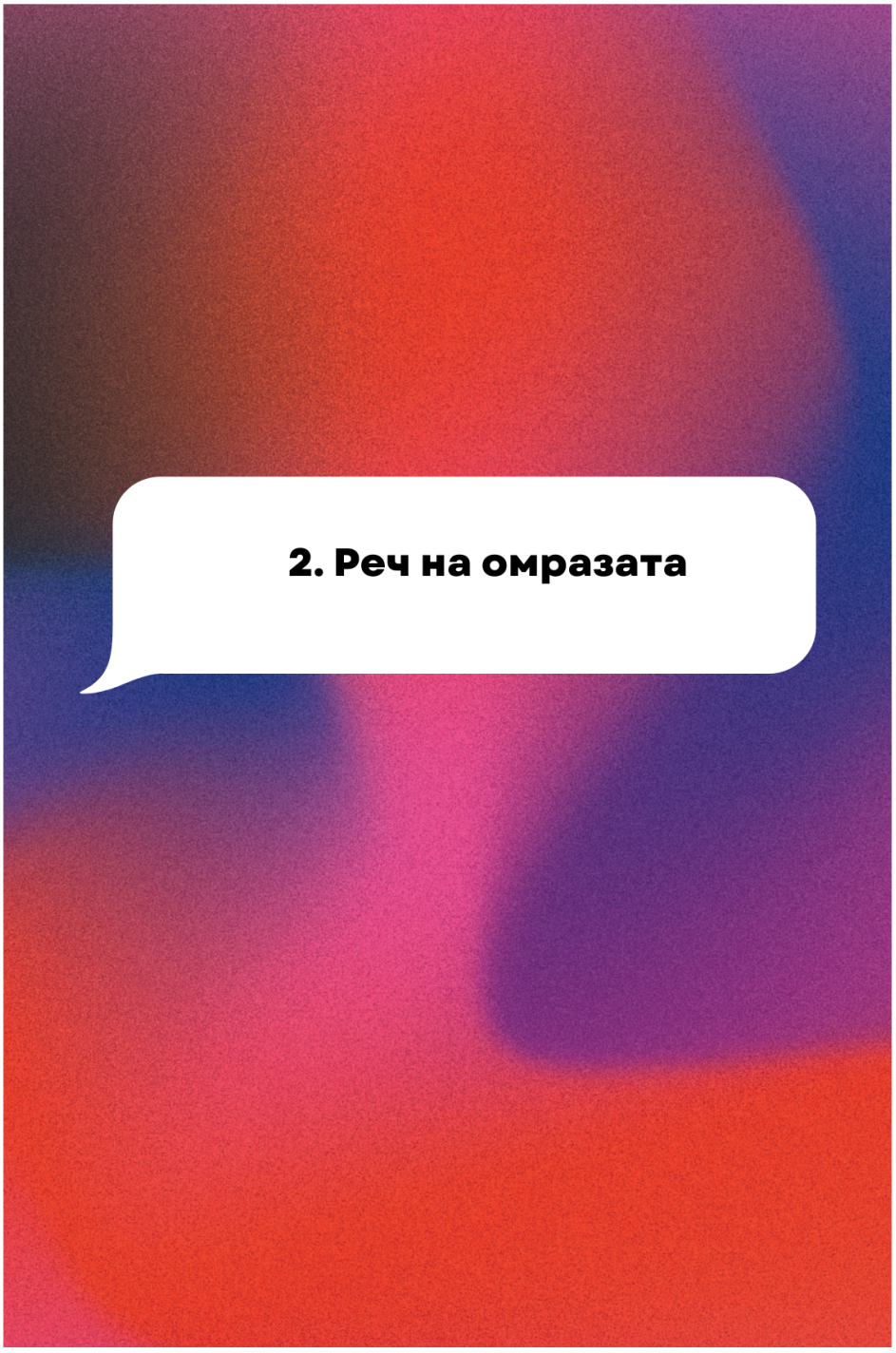
съсредоточаването върху превантивните мерки е от решаващо значение за гарантиране на справянето с всички форми на тормоз. Това може да бъде приложено към случаите на кибертормоз чрез образователни кампании. Тези мерки гарантират, че хората могат да използват интернет безопасно.

- **България**

Киберпрестъпленията, включително кибертормозът, рисковете за неприкосновеността на личния живот и личните данни, както и сигурността в интернет, се докладват на отдел "Киберпрестъпност" към Министерството на вътрешните работи на България. Това е общ механизъм за докладване на неспешни сигнали за киберпрестъпления (свързани предимно с киберизмами и детска порнография). Програмата се координира от отдел "Киберпрестъпност" към Главна дирекция "Борба с организираната престъпност" на Министерството на вътрешните работи.

- Чрез онлайн формуляр могат да се подават сигнали за кибертормоз, киберизмами и детска порнография. За спешни случаи може да се съобщи на общия телефон за спешни повиквания 112.

- Съществува и управляван от държавата механизъм за подкрепа и консултиране на деца и младежи по различни въпроси, включително кибертормоз, реч на омразата, рискове за неприкосновеността на личния живот и данни, както и сигурността онлайн. Този механизъм е **Националната телефонна линия за деца 116 111**, която се управлява и администрира от Държавната агенция за закрила на детето с цел подкрепа на всички деца и техните семейства в България. Операторите, които отговарят на обажданията, са обучени психолози, които 24 часа в денонощието, 7 дни в седмицата, анонимно и напълно безплатно, са готови да изслушат, подкрепят, консултират и насочат обаждащите се по всички въпроси, които ги вълнуват.


2. Реч на омразата

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[18].

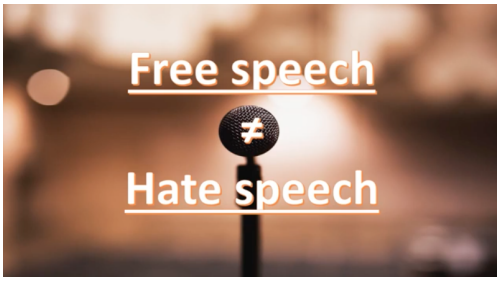
INACH (водещата мрежа в ЕС и в световен мащаб за борба с онлайн речта на омразата) определя речта на омразата като:

"Преднамерени или непреднамерени публични дискриминационни и/или клеветнически изявления; преднамерено подбуждане към омраза и/или насилие и/или сегрегация, въз основа на реална или предполагаема раса, етническа принадлежност, език, националност, цвят на кожата, религиозни убеждения или липса на такива, пол, полова идентичност, сексуална ориентация, политически убеждения, социален статус, възраст, психично здраве, увреждане, болест"[19].

Според правото на ЕС свободата на словото и изразяването са защитени, което кара някои да смятат, че съществува конфликт между защитата на свободата на словото и изразяването и криминализирането на речта на омразата. Според много експерти този предполагаем "конфликт на интереси" между криминализирането на речта на омразата и защитата на свободата на словото е разбран погрешно. Международният пакт за

[18] 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
[19] INACH definition of hate speech https://www.inach.net/cyber-hate-definitions/

граждански и политически права (МПГПП) забранява "всяко проповядване на национална, расова или религиозна омраза, което представлява подбуждане към дискриминация, враждебност или насилие"[20]. Този кратък видеоклип обяснява допълнително това погрешно схващане и защо свободата на словото не е абсолютна.



"Пирамидата на омразата" (показана по-долу) обозначава опасността от всички форми на реч на омразата[21]:

[20] ICCPR Article 20 (2)
[21] https://www.rightsforpeace.org/hate-speech

Пирамидата на омразата се използва за илюстрация на това как речта на омразата в миналото е била (и продължава да бъде) предвестник на крайно насилие. Тя има за цел да подчертае как речта на омразата може да представлява заплаха за другите, като допринася за пирамидата на омразата и насилието. Ето защо борбата с речта на омразата е от съществено значение за създаването на един по-мирен и толерантен свят.

2.2 Как да предотвратим речта на омразата?

Проблемът с речта на омразата се решава на равнище ЕС чрез Директивата за аудиовизуалните медийни услуги (AMSD), която изисква от националните органи във всяка страна от ЕС да гарантират, че аудиовизуалните медийни услуги не съдържат подбуждане към омраза[22].

Освен това на равнище ЕС Комисията договори с Facebook, Microsoft, Twitter и Youtube "Кодекс за поведение за противодействие на незаконната реч на

[22] 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

омразата онлайн". Прилагането на този кодекс на поведение се наблюдава редовно от мрежа от организации в целия ЕС[23].

Как можете на индивидуално ниво да предотвратите 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).

Организацията на обединените нации препоръчва следните практики за предотвратяване на речта на омразата[24]:

- **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.

За да научите повече за речта на омразата и начините за нейното предотвратяване, можете да направите този тест на Организацията на обединените нации: https://www.un.org/en/hate-speech/take-action/test-yourself

2.3 Как да съобщаваме за реч на омразата

INACH е водеща мрежа в ЕС и в световен мащаб, която работи за борба с онлайн речта на омразата. Тя е фондация по нидерландското законодателство и е със седалище в Амстердам, но има 32 членове от 28

[23] The EU Code of Conduct on Tackling Illegal Hate Speech https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[24] United Nations- how to deal with hate speech? https://www.un.org/en/hate-speech/take-action/engage

държави. Нейният уебсайт предлага онлайн платформа за докладване на всякакви случаи на кибер омраза. Освен че предлага услуга за подаване на жалби и сигнали за реч на омразата в онлайн пространството, INACH използва данните от всички получени жалби за изготвяне на доклади и анализи. По този начин организацията се стреми да повлияе на обществеността, социалните медии и международните институции, като се застъпва за международно законодателство срещу кибер омразата.

В допълнение към докладването на случаи на кибер омраза чрез INACH, потребителите могат също така 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[25]. 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 кампанията на Европейския съвет "Младежка кампания без реч на омразата". Списък на държавите и техните процедури за докладване можете да намерите на уебсайта на Съвета на Европа.

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

[25] Reporting on Social Media Channels https://www.coe.int/en/web/no-hate-campaign/reporting-on-social-media-platforms#{%2237117289%22


3. Киберсигурност и защита
на личните данни

3. Киберсигурност и защита на личните данни

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).

Видове данни, които изискват защита

Жизненоважна информация, като имена, адреси, имейли, телефонни номера, здравна информация или банкови данни, са данни, които трябва да се съхраняват и защитават внимателно. Ако подобна информация попадне в неподходящи ръце, тя може да застраши сигурността на хората в много форми, включително личната неприкосновеност, физическата безопасност и финансовата сигурност. Откраднатата информация може да се използва и за създаване на фалшиви профили и извършване на измами.

Примерите за лични данни включват:

- име и фамилия;
- домашен адрес;
- адрес на електронна поща, например name.surname@company.com;
- номер на лична карта;
- данни за местоположение (например функцията за данни за местоположение на мобилен телефон)*;
- адрес по интернет протокол (IP);
- идентификатор на уеб бисквитка;
- рекламния идентификатор на вашия телефон;

- данни, съхранявани от болница или лекар, които могат да бъдат символ, който еднозначно идентифицира дадено лице.

Примери за данни, които не се считат за лични данни, включват:

- регистрационен номер на фирма;
- адрес на електронна поща, например info@company.com;
- анонимизирани данни - лични данни, които са били анонимизирани по такъв начин, че лицето не може или вече не може да бъде идентифицирано, вече не се считат за лични данни. За да бъдат данните наистина анонимизирани, анонимизирането трябва да бъде необратимо.

Кой отговаря за защитата на нашите данни?

Защитата на данните е процесът на предпазване на важна информация от повреда, компрометиране или загуба. Значението на защитата на данните нараства, тъй като количеството на създаваните и съхранявани данни продължава да нараства с безпрецедентни темпове. Ето защо организациите, които съхраняват и управляват лична информация, са отговорни да гарантират, че тя е защитена от повреда, компрометиране или загуба. В Европейския съюз **Общият регламент за защита на данните (GDPR)** защитава личните данни на гражданите на ЕС. Това е най-строгият закон за защита на личните данни и сигурността в света. Въпреки че е изготвен и приет от Европейския съюз, той налага задължения на организациите навсякъде, стига да са насочени към или да събират данни, свързани с хора в ЕС. Регламентът влезе в сила на 25 май 2018 г.

Основни елементи на защитата на данните

Един много важен модел за защита на данните е триадата на CIA (ЦРУ), където трите букви на името на агенцията на английски език представляват трите елемента на защита на данните: поверителност (confidentiality), интегритет (integrity) и наличност (availability). Този модел е разработен, за да помогне на лицата и организациите да разработят цялостен подход към защитата на данните. Трите елемента са дефинирани, както следва:

- Конфиденциалност: данните се извличат само от упълномощени оператори със съответните пълномощия.
- Интегритет: всички данни, съхранявани в организацията, са надеждни, точни и не подлежат на необосновани промени.
- Наличност: съхраняваните данни са надеждно и лесно достъпни, когато е необходимо.

Според GDPR съществуват и няколко принципа за защита на личните данни, които организациите, събиращи и управляващи ги, трябва да спазват:

- Законосъобразност, справедливост и прозрачност - обработката трябва да бъде законосъобразна, справедлива и прозрачна за субекта на данните.
- Ограничаване на целите - администраторът на данни трябва да обработва данните за законните цели, изрично посочени на субекта на данните при събирането им.
- Минимизиране на данните - администраторът на данни трябва да събира и обработва само толкова данни, колкото е абсолютно необходимо за посочените цели.
- Точност - администраторът на данни трябва да поддържа личните данни точни и актуални.
- Ограничаване на съхранението - администраторът на данни може да съхранява данни за идентифициране на лица само толкова дълго, колкото е необходимо за определената цел.
- Цялостност и поверителност - обработката трябва да се извършва по такъв начин, че да се гарантира подходяща сигурност, интегритет и поверителност (например чрез използване на криптиране).
- Отчетност - администраторът на данни е отговорен за това да може да докаже спазването на всички тези принципи на GDPR.

Значението на защитата на данните нараства, тъй като количеството на създаваните и съхранявани данни продължава да нараства с безпрецедентни темпове. Също така има малка търпимост към прекъсвания, които могат да направят невъзможен достъпа до важна информация.
Както е обяснено по-горе, организациите, които събират, съхраняват и управляват лични данни, са отговорни за гарантирането на това, че с тези данни не се злоупотребява и че те са достъпни за упълномощения персонал по всяко време. GDPR гарантира това чрез конкретни правни изисквания и санкции за организациите, които не ги спазват. От друга страна, физическите лица също могат да предприемат мерки за сигурност срещу нежелани опити за достъп до техните данни от страна на външни лица, както и да защитават личните си данни от тези, с които не са съгласни да споделят личната си информация.

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

- **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. Тези действия могат да навредят на кредитния ви статус и да ви струват време и пари, за да възстановите доброто си име.

Кражбата на самоличност се случва, когато някой открадне личната ви информация - например номера на социалната ви осигуровка, номера на банковата ви сметка и информация за кредитни карти. Кражбата на самоличност може да бъде извършена по много различни начини. Някои крадци на самоличност претърсват кофите за боклук в търсене на извлечения от банкови сметки и кредитни карти. По-високотехнологичните методи включват достъп до корпоративни бази данни, за да се откраднат списъци с информация за клиентите. След като крадците на самоличност разполагат с търсената информация, те могат да разрушат кредитния рейтинг на дадено лице, както и да се сдобият с друга лична информация.

Крадците на самоличност все по-често използват компютърни технологии, за да получат лична информация на други хора с цел кражба на самоличността. За да намерят такава информация, те могат да претърсват твърдите дискове на откраднати или изхвърлени компютри; да проникват в компютри или компютърни мрежи; да получават достъп до компютърни публични регистри; да използват зловреден софтуер за събиране на информация, за да заразяват компютри; да преглеждат социални мрежи; да използват измамни имейли или текстови съобщения.

Видове кражба на самоличност

- **Кражба на финансова самоличност**

При финансовата кражба на самоличност някой използва самоличността или информацията на друго лице, за да получи кредит, стоки, услуги или облаги. Това е най-разпространената форма на кражба на самоличност.

- **Кражба на самоличност по линия на социалното осигуряване**

Ако крадците на самоличност получат номера на социалната ви осигуровка, те могат да го използват, за да кандидатстват за кредитни карти и заеми и след това да не плащат дължимите суми. Измамниците могат също така да използват номера ви, за да получават медицински, инвалидни и други помощи.

- **Кражба на самоличност по медицински причини**

При кражбата на медицинска самоличност някой се представя за друго лице, за да получи безплатна медицинска помощ.

- **Синтетична кражба на самоличност**

Синтетичната кражба на самоличност е вид измама, при която престъпникът комбинира истинска (обикновено крадена) и фалшива информация, за да създаде нова самоличност, която се използва за откриване на измамни сметки и извършване на измамни покупки. Синтетичната кражба на самоличност позволява на престъпника да открадне пари от всички компании за кредитни карти или кредитори, които отпускат кредити въз основа на фалшивата самоличност.

- **Кражба на самоличност на дете**

При кражбата на детска самоличност някой използва самоличността на дете за различни форми на лична изгода. Това е често срещано явление, тъй като децата обикновено нямат информация, свързана с тях, която би могла да създаде пречки за извършителя. Измамникът може да използва името и номера на социалната осигуровка на детето, за да получи жилище, да си намери работа, да получи заеми или да избегне арест. Често жертвата е член на семейството, дете на приятел или някой друг близък на извършителя. Някои хора дори крадат личната информация на починали близки.

- **Кражба на данъчна самоличност**

Кражба на данъчна самоличност се случва, когато някой използва личната ви информация, включително номера на социалната ви осигуровка, за да подаде фалшива данъчна декларация от ваше име и да получи възстановяване на данъци.

- **Криминална кражба на самоличност**

При кражба на самоличност по време на арест престъпникът се представя за друго лице, за да се опита да избегне призовка, да предотврати откриването на заповед, издадена на негово истинско име, или да избегне присъда или арест.

- **Кражба на самоличност при безработица**

Някой използва личните ви данни, за да поиска (и получи) обезщетение за безработица.

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.

Видове сексуален тормоз онлайн

- **Споделяне на интимни снимки и видеоклипове без съгласието на потребителите**

- **Споделяне на сексуални изображения и видеоклипове на дадено лице без негово съгласие или заснемане без негово съгласие.** Това включва редица поведения, като например:
  - ❖ Сексуални снимки/видеоклипове, направени без съгласие
  - ❖ Сексуални изображения/видеоклипове, направени по взаимно съгласие, но споделени без съгласие ("порно отмъщение")
  - ❖ Сексуални действия без съгласие (напр. изнасилване), записани в цифров вид (и потенциално споделени)

- **Експлоатация, принуда и заплахи**

Лице, което получава сексуални заплахи, е принуждавано да участва в сексуално поведение онлайн или е изнудвано със сексуално съдържание. Това включва редица поведения, като например:

- ❖ тормоз или натиск върху някого онлайн да споделя свои сексуални изображения или да участва в сексуално поведение онлайн (или офлайн)
- ❖ използване на заплахата от публикуване на сексуално съдържание (изображения, видеоклипове, слухове), за да заплашване, принуждаване или изнудване на някого
- ❖ онлайн заплахи от сексуално естество (напр. заплахи за изнасилване)
- ❖ подстрекаване на други хора онлайн да извършат сексуално насилие
- ❖ подстрекаване на някого да участва в сексуално поведение и след това споделяне на доказателства за това

- **Сексуализиран тормоз** - дадено лице е обект на нападение от страна на група или общност и е системно изключвано от нея с помощта на сексуално съдържание, което го унижава, разстройва или дискриминира. Това включва редица поведения, като например:

- ❖ Сплетни, слухове или лъжи за сексуално поведение, публикувани онлайн, в които директно се назовава името на някого или косвено се намеква за някого
- ❖ Обиден или дискриминационен сексуален език и наричане по име онлайн

- ❖ Представяне на някого и уронване на репутацията му чрез споделяне на сексуално съдържание или сексуален тормоз на други хора
- ❖ Споделяне на лична информация без съгласие онлайн с цел насърчаване на сексуален тормоз ("doxing")
- ❖ Тормоз заради действителен или предполагаем пол и/или сексуална ориентация
- ❖ Обидни коментари относно външния вид на дадено лице
- ❖ "Излагане" на някого, при което сексуалността или половата идентичност на лицето се обявява публично онлайн без неговото съгласие

- **Нежелана сексуализация**

Лице, което получава нежелани сексуални предложения, коментари и съдържание. Това включва редица поведения, като например:

- ❖ Сексуализирани коментари (напр. на снимки)
- ❖ Сексуализирани вирусни кампании, които оказват натиск върху хората да участват в тях
- ❖ Изпращане на някого на сексуално съдържание (изображения, емотикони, съобщения), без той да е дал съгласието си
- ❖ Нежелани сексуални аванси или искания за сексуални услуги
- ❖ "Шеги" от сексуално естество
- ❖ Оценяване на връстници по привлекателност/сексуална активност
- ❖ Промяна на изображенията на дадено лице, за да бъдат те сексуални

Сексуалният тормоз от този вид може да накара лицето да се чувства по някой от следните начини:

- ❖ да бъде застрашено или уплашено
- ❖ експлоатирано
- ❖ принудено
- ❖ че достойнството му е накърнено
- ❖ унизено или принизено
- ❖ засрамено или осъдено
- ❖ разстроено
- ❖ сексуализирано
- ❖ дискриминирано поради своя пол или сексуална ориентация
- ❖ виновно

Преживяването и въздействието на сексуалния тормоз онлайн е уникално за всеки отделен човек и може да се усети както в краткосрочен план, така и да има дългосрочни последици за психичното здраве и благополучие. Дългосрочните въздействия могат да се засилят поради повторната виктимизация, ако съдържанието се споделя отново онлайн, или поради

това, че първоначалната травма от инцидента се появява отново много по-късно. Важно е да се посочи, че няма един-единствен начин, по който един млад човек може да преживее сексуален тормоз онлайн, както и това, че тормозът може да засегне и други хора, които са станали негови свидетели.

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.

Понякога хакерите се задоволяват с получаването на вашите лични данни и информация за кредитни карти с цел финансова изгода. В други случаи фишинг имейлите се изпращат, за да се съберат данни за влизане в системата на служителите или други детайли, които да се използват за по-злонамерени атаки срещу няколко лица или конкретна компания.

Фишингът започва с измамно електронно писмо или друго съобщение, предназначено да подмами жертвата. Съобщението е направено така, че да изглежда, че идва от доверен подател. Ако то заблуди жертвата, тя бива подведена да предостави поверителна информация - често на измамен уебсайт. Понякога на компютъра на жертвата се изтегля и зловреден софтуер.

Киберпрестъпниците започват с идентифицирането на група лица, към които искат да се насочат. След това създават имейли и текстови съобщения, които изглеждат легитимни, но всъщност съдържат опасни линкове, прикачени файлове или примамки, които подмамват получателите да предприемат рисковано действие.

Рисковете от фишинг включват:

- Откраднване на пари от банковата ви сметка
- Измамни такси по кредитни карти
- Загуба на достъп до снимки, видеоклипове и файлове
- Фалшиви публикации в социалните медии, направени във вашите акаунти
- Киберпрестъпниците се представят за вас пред приятел или член на семейството, като го излагат на риск

Накратко:

- Измамниците често използват емоции като страх, любопитство и алчност, за да накарат получателите да отворят прикачени файлове или да кликнат върху линкове.
- Фишинг атаките са създадени така, че да изглеждат като идващи от легитимни компании и физически лица.
- Киберпрестъпниците непрекъснато правят нововъведения и се усъвършенстват.
- Необходима е само една успешна фишинг атака, за да се компрометира мрежата ви и да бъдат откраднати данните ви, ето защо е важно винаги да "мислите преди да кликнете".

За да избегнете фишинг атаки, CISCO дава следните съвети:

- Избягвайте непознати изпращачи. Проверявайте имената и имейл адресите преди да отговорите.
- Не се доверявайте на линкове или прикачени файлове в нежелани имейли.
- Бъдете подозрителни към имейли, обозначени като "спешни".
- Пазете се от съобщения с правописни или граматически грешки.
- Не се подмамвайте от "оферти". Обикновено те са твърде добри, за да са истина.
- Използвайте сигурен доставчик на електронна поща.
- Никога не предоставяйте лична или финансова информация въз основа на искане по имейл.
- Когато получавате електронна поща от институции (правителство, банки, вашият лекар), отидете директно при източника, вместо да кликвате върху връзките в електронното писмо.
- Бъдете предпазливи по отношение на общите поздрави, като например "Уважаеми господине или госпожо".
- Запознайте се с политиката на доставчика на услуги за проследяване и спиране на фишинг.
- Не давайте достъп до компютъра си на непознати.

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.

Интернет измамите, които са насочени към жертвите чрез онлайн услуги, представляват измамна дейност на стойност милиони долари всяка година, като цифрите продължават да се увеличават с разширяването на използването на интернет и усъвършенстването на техниките на киберпрестъпниците.

Киберпрестъпниците използват различни стратегии за извършване на интернет измами. **Това включва зловреден софтуер, електронна поща и незабавни съобщения за разпространение на зловреден софтуер, подправени уебсайтове, които крадат потребителски данни, и сложни, широкообхватни фишинг измами.**

Интернет измамите могат да бъдат разделени на няколко основни вида атаки, включително:

- Фишинг (обяснен подробно по-горе): Използването на електронна поща и услуги за онлайн съобщения за подвеждане на жертвите да споделят лични данни, идентификационни данни за вход в онлайн профили, както и финансови данни.
- Нарушаване на сигурността на данните: Кражба на поверителни, защитени или чувствителни данни от защитено място и преместването им в ненадеждна среда. Това включва кражба на данни от потребители и организации.
- Отказ от обслужване (DoS): Прекъсване на достъпа до трафика на онлайн услуга, система или мрежа с цел нанасяне на вреда.
- Зловреден софтуер: Използване на злонамерен софтуер за повреждане или деактивиране на устройствата на потребителите или за кражба на лични и чувствителни данни.
- Рансъмуер: Вид зловреден софтуер, който не позволява на потребителите да имат достъп до важни данни, след което изисква плащане срещу обещание за възстановяване на достъпа. Обикновено рансъмуерът се разпространява чрез фишинг атаки.
- Компрометиране на бизнес електронна поща: Усъвършенствана форма на атака, насочена към предприятия, които често извършват плащания по банков път. При нея се компрометират легитимни имейл акаунти, за да се изпращат неразрешени плащания.

Някои примери включват:

- **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.

- **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. Тези измами продължават да мамят хората въпреки широко разпространеното съзнание, че подобни оферти са твърде добри, за да са истина.

- **Измами с онлайн запознанства**

Друг типичен пример за интернет измама е насочен към множеството приложения и уебсайтове за онлайн запознанства. Хакерите се фокусират върху 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.

- **Лотарийна измама**

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.

Измамниците с лотарийни такси обикновено подготвят имейлите така, че да изглеждат и да звучат правдоподобно, което води до това, че много хора се хващат на измамата. Измамата е насочена към мечтите на хората да спечелят огромни суми пари, въпреки че те може никога да не са купували лотариен билет. Освен това никоя законна лотарийна схема не изисква от победителите да платят, за да получат наградата си.

- **Нигерийският принц**

Класическа тактика за интернет измами е измамата с нигерийския принц, която остава разпространена и процъфтява въпреки че много хора вече знаят за какво става въпрос.

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.
Измамникът неминуемо ще поиска по-обширни такси за покриване на допълнителни административни задачи и разходи по транзакциите, подкрепени от легитимно изглеждащи документи за потвърждение. Обещаната възвръщаемост на инвестицията обаче така и не пристига.

Съвети за избягване на интернет измами и мошеничества:

Важно е никога да не изпращате пари на някого, с когото сте се запознали по интернет, никога да не споделяте лични или финансови данни с лица, които не са легитимни, и никога да не кликвате върху хипервръзки или прикачени файлове в имейли или незабавни съобщения. След като станат обект на посегателство, потребителите на интернет трябва да докладват на властите за дейността на онлайн измамниците, както и за фишинг имейли.

Измамите с кредитни карти могат да бъдат избегнати и чрез внимателно следене на банковите сметки, настройване на известия за активност по кредитните карти, абониране за кредитен мониторинг и използване на услуги за защита на потребителите. Ако потребителите станат жертва на измама с кредитна карта, те трябва да съобщят за нея на съответните правни органи и банки.

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.

Терминът "спам", който се използва за описване на масови нежелани съобщения, идва от скеч на Монти Пайтън, в който актьорите заявяват, че всички трябва да ядат храната спам, независимо дали искат или не. По същия начин всеки, който има имейл адрес, за съжаление трябва да бъде притесняван от спам съобщения, независимо дали ни харесва или не.

Спамърите използват много форми на комуникация, за да изпращат масово своите нежелани съобщения. Някои от тях са маркетингови съобщения, които продават непоискани стоки. Други видове спам съобщения могат да разпространяват зловреден софтуер, да ви подлъжат да разкриете лична информация или да ви накарат да мислите, че трябва да платите, за да се измъкнете от неприятности.

Филтрите за спам в електронната поща улавят много от тези видове съобщения, а телефонните оператори често ви предупреждават за "риск от

спам" от непознати обаждащи се. Независимо дали става въпрос за имейл, текстови съобщения, телефон или социални медии, някои спам съобщения все пак достигат до нас и е необходимо да ги разпознаваме и да се предпазваме от потенциални заплахи. По-долу са изброени няколко вида спам, за които да внимавате:

- Фишинг имейли (вече описани по-горе)
- Подправяне на имейли - подправените имейли имитират или подправят имейл от легитимен подател и изискват от вас да предприемете някакво действие. Добре изпълнените фалшиви имейли съдържат познати марки и съдържание, често от голяма и известна компания, като PayPal или Apple.
- Измами с техническа поддръжка - при измама с техническа поддръжка спам съобщението посочва, че имате технически проблем и трябва да се свържете с техническата поддръжка, като се обадите на телефонния номер или кликнете върху връзка в съобщението.
- Malspam - съкратено от "malware spam" или "злонамерен спам", malspam е спам съобщение, което доставя зловреден софтуер на вашето устройство. Нищо неподозиращите получатели, които щракнат върху връзката или отворят прикачения файл на електронното съобщение, в крайна сметка се оказват с някакъв вид зловреден софтуер, напр. софтуер за откуп, троянски коне, ботове, устройства за кражба на информация, криптомонитори, шпионски софтуер и кийлогъри. Често срещан метод е включването на зловредни скриптове в прикачен файл от познат тип, например документ на Word, PDF файл или презентация на PowerPoint. След като прикаченият файл бъде отворен, скриптовете се стартират и извличат зловредния софтуер.
- Спам обаждания и спам съобщения - получавали ли сте някога роботизирано обаждане? Това е спам обаждане. Текстово съобщение от непознат подател, което ви призовава да кликнете върху непозната връзка? Това се нарича спам с текстови съобщения или "smishing" - комбинация от SMS и фишинг.

Ако получавате спам обаждания и текстови съобщения на вашия Android или iPhone, повечето големи оператори ви дават възможност да докладвате за спам. Блокирането на номера е друг начин за борба с мобилния спам.

Киберхакерство

Всеки, който използва компютър, свързан с интернет, е податлив на заплахите, които представляват компютърните хакери и онлайн хищниците. Тези онлайн злодеи обикновено **използват фишинг измами, спам имейли или незабавни съобщения и фалшиви уебсайтове, за да доставят опасен зловреден софтуер на вашия компютър и да компрометират дигиталната ви сигурност.**

Компютърните хакери могат също така да се опитат да получат **директен достъп до вашия компютър и лична информация,** ако не сте защитени със защитна стена. Те могат да наблюдават разговорите ви или да разглеждат задната част на личния ви уебсайт. Обикновено прикрити с фалшива самоличност, хищниците могат да ви подмамят да разкриете чувствителна лична и финансова информация.

Докато компютърът ви е свързан с интернет, злонамереният софтуер, който хакерът е инсталирал на компютъра ви, предава личната и финансовата ви информация без ваше знание или съгласие. Компютърен хищник може да се нахвърли върху личната информация, която неволно сте разкрили. И в двата случая хакерите могат да:

- Получат достъп до имена и пароли
- Откраднат парите ви и открият кредитни карти и банкови сметки на ваше име
- Поискат нови лични идентификационни номера (ПИН) или допълнителни кредитни карти
- Извършват покупки
- Добавят себе си или псевдоним, който контролират, като упълномощен потребител, за да е по-лесно да използват кредита ви
- Получават авансови плащания в брой
- Използват и злоупотребяват с номера на социалната ви осигуровка
- Продават информацията ви на други лица, които я използват за незаконни цели

За да се предпазите от тези заплахи, можете да направите следното:

- Непрекъснато проверявайте точността на личните си сметки
- Бъдете изключително предпазливи, когато влизате в чат стаи или публикувате в профилите си в социалните мрежи
- Ограничете личната информация, която публикувате на профилите си в социалните мрежи
- Внимателно следете заявките на онлайн "приятели" или познати за хищническо поведение
- Не включвайте лична и финансова информация в онлайн разговори
- Бъдете изключително предпазливи, когато се съгласявате да се срещнете лично с онлайн "приятел" или познат
- Използвайте двупосочна защитна стена
- Редовно актуализирайте операционната си система
- Увеличете настройките за сигурност на браузъра си
- Избягвайте съмнителни уебсайтове
- Изтегляйте софтуер само от сайтове, на които имате доверие
- Внимателно преценявайте безплатния софтуер и приложенията за споделяне на файлове, преди да ги изтеглите
- Не отваряйте съобщения от непознати податели

- Незабавно изтривайте съобщения, за които подозирате, че са спам
- Уверете се, че в компютъра ви са инсталирани най-добрите софтуерни продукти за сигурност
- Използвайте антивирусна защита
- Използвайте антишпионска софтуерна защита

Киберпреследване

Киберпреследването се отнася до използването на интернет и други технологии за тормоз или преследване на друго лице онлайн. Този онлайн тормоз, който е продължение на кибертормоза и личното преследване, може да бъде под формата на имейли, текстови съобщения, публикации в социалните медии и др., и често е методичен, преднамерен и настойчив.

В повечето случаи взаимодействието не се прекратява, дори ако получателят изрази недоволството си или помоли лицето да спре. Съдържанието, насочено към целта, често е неподходящо, а понякога дори обезпокоително, като може да накара лицето да се чувства уплашено, притеснено и разтревожено.

Когато става въпрос за киберпреследване, лицата, които се занимават с това поведение, използват различни тактики и техники, за да тормозят, унижават, сплашват и контролират своите мишени.

Всъщност много от лицата, които се занимават с киберпреследване, са технологично грамотни, както и креативни, и измислят множество начини да тормозят своите жертви. Ето някои примери за действия на хора, които извършват киберпреследване:

-Публикуване на груби и обидни коментари онлайн
- Следване на целта онлайн, като преследвачът се присъединява към същите групи и форуми, в които членува жертвата
- Изпращане на заплашителни, контролиращи или неприлични съобщения или имейли на мишената
- Използване на технологиите за заплашване или изнудване на мишената
- Прекалено често отбелязване на мишената в постове, дори ако нямат нищо общо с нея
- Коментиране или харесване на всичко, което мишената публикува онлайн
- Създаване на фалшиви акаунти за следване на мишената в социалните медии
- Изпращане на многократни съобщения на жертвата
- Хакерска атака на онлайн акаунтите на мишената
- Опит за изнудване на жертвата за секс или сексуални снимки
- Изпращане на нежелани подаръци или предмети на жертвата
- Публикуване на поверителна информация за жертвата онлайн
- Публикуване или разпространяване на истински или фалшиви снимки на мишената

- Бомбардиране на жертвата със свои снимки със сексуално съдържание
- Създаване на фалшиви публикации, предназначени да засрамят жертвата
- Проследяване на движението на мишената онлайн чрез инсталиране на устройства за проследяване
- Хакване на камерата на лаптопа или смартфона на мишената, за да бъде записана тайно
- Преследвачът продължава да се държи притеснително дори след като е помолен да спре

Подобно на преследването, киберпреследването може да доведе до широк спектър от физически и емоционални последици за лицата, които са негова мишена. Например, не е необичайно за тези, които са подложени на онлайн тормоз, да изпитват гняв, страх и объркване. Освен това те могат да имат проблеми със съня и дори да се оплакват от стомашни проблеми.

Начините за предотвратяване на киберпреследването са много сходни с тези, които се препоръчват за предотвратяване на други киберзаплахи, тъй като всички те са свързани и функционират по сходен начин. Някои от съветите включват:

- Създайте силни пароли. Уверете се, че разполагате със силни пароли за всичките си онлайн акаунти, както и със силни пароли за устройствата си. След това задайте напомняне на телефона си, за да сменяте редовно паролите си. Изберете пароли, които трудно биха могли да бъдат отгатнати, но са лесни за запомняне за вас.

- Не забравяйте да излизате от системата/профила си/имейла си всеки път. Може да ви се струва досадно, но не забравяйте да излизате от имейли, акаунти в социални медии и други онлайн акаунти, след като ги използвате. По този начин, ако някой успее да влезе в устройството ви, няма да има лесен достъп до акаунтите ви.

- Проследявайте устройствата си. Не оставяйте телефона си да стои на бюрото ви на работа или да се отдалечавате от отворен лаптоп. Нужни са само минута-две, за да може някой да инсталира устройство за проследяване или да хакне устройството ви, така че се уверете, че държите тези неща у себе си или че ги защитавате по някакъв начин.

- Бъдете внимателни при използването на публична Wi-Fi мрежа. Ако използвате обществен Wi-Fi в хотели или в местното кафене, се излагате на риск от хакерски атаки. Опитайте се да се въздържате от използване на обществени интернет мрежи или инвестирайте във VPN.

- Практикувайте навици за онлайн безопасност. С други думи, превърнете в приоритет приемането на заявки за приятелство само от хора, които

познавате лично, и запазете публикациите си лични. Също така трябва да обмислите възможността да имате един имейл адрес, който да е предназначен специално за вашата онлайн дейност. Използвайте този имейл, когато пазарувате онлайн или се присъединявате към програми за лоялност.

- Възползвайте се от настройките за сигурност на онлай акаунтите си. Прегледайте всеки от онлайн акаунтите си - особено тези в социалните медии - и се уверете, че използвате възможно най-силните настройки за поверителност. Можете да установите настройки, при които хората не могат да ви отбелязват или да публикуват ваши снимки без предварителното ви одобрение.

- Вместо да използвате пълното си име онлайн, помислете за създаване на псевдоним. По този начин ще затрудните хората да ви открият онлайн. Също така трябва да оставите незадължителните секции, като например датата на раждане или родния си град, празни.
- Помислете за деактивиране на настройките за геолокация в снимките, които публикувате. Също така се въздържайте от публикуване на местоположението си в реално време, като вместо това публикувате снимки, показващи къде сте били след това.

- Бъдете внимателни със сайтовете за онлайн запознанства. Въздържайте се да използвате пълното си име в тях. Също така трябва да избягвате да давате лична информация като фамилия, адрес, имейл и телефонен номер, докато не се срещнете лично и не изградите доверие с другия човек.

- Винаги е добра идея да прегледате акаунтите си в социалните медии и да премахнете снимки или публикации, които предоставят твърде много информация за вас или създават образ, който не искате да бъде разпространен. Имайте предвид също така, че дори да сте блокирали някого в социалните медии, той все още може да вижда профила ви, като използва профил на друго лице или като създаде фалшив профил.

Начините за справяне с киберпреследването, в случай че то вече се е случило, включват:

- Кажете на лицето да спре. Отговорете само веднъж на лицето, което ви преследва в киберпространството, и му кажете да спре да се свързва с вас. Не е необходимо да казвате нищо конкретно или да обяснявате отговора си, просто го помолете никога повече да не се свързва с вас.
- Блокирайте лицето. Уверете се, че сте блокирали лицето, което ви преследва в киберпространството, от всичките си акаунти. Трябва да го блокирате в социалните мрежи и на смартфона си.

- Откажете да отговаряте на всякакви контакти. Ако лицето, което ви преследва в киберпространството, продължава да намира начини да се свърже с вас, не отговаряйте на нищо, което публикува или ви изпраща.

- Променете имейл адреса и псевдонима/името си в социалните мрежи. Обмислете възможността да си осигурите нов имейл адрес и да смените името си в социалните мрежи, за да затрудните достъпа на лицето, което ви преследва в киберпространството.

- Ако сте помолили лицето, което ви преследва в киберпространството, да спре, а то продължава да се държи така, е важно да предприемете действия срещу него. Това включва свързване със съответните органи и събиране на доказателства за действията му. Също така може да искате да обмислите възможността да разговаряте с адвокат.

- Ето основните точки, на които ще трябва да се обърне внимание при предприемането на действия. Местните правоприлагащи органи могат да ви информират дали има нещо друго, което можете да направите, за да останете в безопасност.
- Запазете доказателства за всичко. Въпреки че може да ви се иска да унищожите всичко, важно е да запазите копия на всичко, което лицето, което ви преследва в киберпространството, е изпратило. Направете копие за себе си и копие за правоприлагащите органи.

- Уведомете местната полиция. Важно е да уведомите полицията и да подадете официална жалба, ако сте обект на киберпреследване. Дори и да не могат да направят нищо веднага, наличието на официална жалба в досието е важно, ако поведението продължава или се засилва.

- Съобщете за тях на сайта или услугата, която са използвали. Ако лицето, което ви преследва в киберпространството, ви е тормозило чрез Facebook, Instagram, Twitter, Snapchat, YouTube, Gmail или някакъв друг метод, уведомете съответните доставчици на услуги за това, което преживявате. В много случаи тези организации приемат сериозно оплакванията за киберпреследване и ще се заемат с въпроса.

3.3 Как да съобщаваме за заплахи за киберсигурността в социалните медии и в релевантни 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. По-долу можете да намерите 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.

За да докладвате профил:

- Отидете на профила, който искате да докладвате, като щракнете върху името му във вашия Feed или го потърсите.

- Щракнете върху "..." вдясно и изберете *Намиране на подкрепа* или *Докладване на профил*.

- За да дадете обратна връзка, щракнете върху опцията, която най-добре описва как този профил противоречи на стандартите на общността, след което щракнете върху *Напред*.

- В зависимост от обратната връзка, след това може да успеете да изпратите доклад до Meta. За някои типове съдържание Facebook не изисква от вас да подадете доклад, но използва обратната ви връзка, за да помогне на системите си да се обучават. Щракнете върху *Готово*.

За да докладвате публикация:

- Отидете на публикацията, която искате да докладвате.

- Щракнете върху "..." в горния десен ъгъл на публикацията.

- Щракнете върху *Намери подкрепа* или *Докладвай публикация*.

- За да дадете обратна връзка, щракнете върху опцията, която най-добре описва как тази публикация противоречи на стандартите на общността на Facebook. Щракнете върху *Напред*.

- В зависимост от обратната връзка след това може да успеете да подадете доклад до Meta. За някои видове съдържание Facebook не изисква от вас да подадете доклад, но използва обратната ви връзка, за да помогне на системите си да се обучават. Щракнете върху *Готово*.

За докладване на снимка или видеоклип:

- Щракнете върху снимката или видеоклипа, за да ги разширите. Ако профилът е заключен и не можете да видите снимката в пълен размер, щракнете върху *Намери подкрепа* или *Докладвай снимка*.

- Щракнете върху "..." вдясно от снимката или видеоклипа.

- Щракнете върху *Намиране на подкрепа* или *Докладване на снимка* за снимки или *Докладване на видео* за видеоклипове.

- Изберете опцията, която най-добре описва проблема, и следвайте инструкциите на екрана.

За да съобщите за съобщение:

- За да докладвате съобщение, което противоречи на стандартите на общността на Facebook:

- От всяка страница във Facebook щракнете върху иконата на Messenger в горния десен ъгъл.

- Отворете съобщението.

- Ако сте отворили съобщението като изскачащ прозорец, щракнете върху иконата за настройки.

- Щракнете върху *Нещо не е наред*.

- За да дадете обратна връзка, щракнете върху опцията, която най-добре описва как това съобщение противоречи на Стандартите на общността на Facebook.

- В зависимост от обратната връзка, след това може да успеете да изпратите доклад до Meta. За някои видове съдържание Facebook не изисква от вас да подадете доклад, но използва обратната ви връзка, за да помогне на системите си да се учат.

За да докладвате страница:

- Отидете на страницата, която искате да докладвате, като щракнете върху името ѝ във вашия канал или я потърсите.

- Щракнете върху *Повече* под снимката на корицата на страницата.

- Изберете *Намиране на подкрепа* или *Докладване на страница*.

- За да дадете обратна връзка, щракнете върху опцията, която най-добре описва как тази Страница противоречи на стандартите на общността на Facebook.

- В зависимост от обратната връзка, след това може да успеете да подадете доклад до Meta. За някои видове съдържание Facebook не изисква от вас да подадете доклад, но използва обратната ви връзка, за да помогне на системите си да се обучават.

Докладване на група:

- Отидете на групата, която искате да докладвате, като щракнете върху името ѝ във вашия канал или я потърсите.

- Щракнете върху повече под снимката на корицата на групата.

- Изберете *Докладване на група.*

За да докладвате събитие:

- От вашия Feed щракнете върху *Събития* в лявото меню.

- Отидете на събитието, което искате да докладвате.

- Щракнете върху "..." и изберете *Докладване на събитие*.

- За да дадете обратна връзка, щракнете върху опцията, която най-добре описва как този профил противоречи на Стандартите на общността на Facebook.

- В зависимост от обратната връзка след това може да успеете да подадете доклад до Meta. За някои видове съдържание Facebook не изисква от вас да подадете доклад, но използва обратната ви връзка, за да помогне на системите си да се учат.

За да докладвате коментар:

- Отидете на коментара, който искате да докладвате.

- Щракнете върху "..." до коментара.

- Щракнете върху *Дай обратна връзка* или *Докладвай този коментар*.

- За да дадете обратна връзка, щракнете върху опцията, която най-добре описва как този коментар противоречи на стандартите на общността на Facebook. Ако не виждате подходящи опции, щракнете върху *Нещо друго*, за да потърсите още.

- В зависимост от обратната връзка, след това може да успеете да подадете доклад до Meta. За някои видове съдържание Facebook не изисква от вас да подадете доклад, но използва обратната ви връзка, за да помогне на системите си да се учат.

Докладване на реклама във Facebook:

- Отидете на рекламата, която искате да докладвате, като щракнете върху името ѝ във вашия канал или я потърсите.

- Щракнете върху "..." до рекламата, която искате да докладвате.

- Щракнете върху *Докладване на реклама*, след което следвайте инструкциите на екрана.

· **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.

Докладване на коментари

- Ако видите коментар, който е спам или има за цел да тормози вас или някой друг, докладвайте го.

- Отворете разговора в приложението на Instagram.

- Докоснете и задръжте отделното съобщение, което искате да докладвате.

- Щракнете на *Докладване*.

- Изберете причина, поради която докладвате съобщението, след което докоснете *Изпрати доклад*.

- За повече информация посетете Центъра за помощ.

Докладване на съобщения

- Ако получите съобщение, което ви се струва неподходящо, докоснете и задръжте отделното съобщение, за да го докладвате. За повече информация посетете Центъра за помощ.

Докладване на истории

- Ако видите нечия история и смятате, че тя противоречи на Насоките за общността на Instagram, можете да я докладвате.

- Отворете историята.

- Докоснете трите точки в долната част на снимката или видеоклипа, които искате да докладвате.

- Докоснете *Докладване*, след което следвайте инструкциите на екрана.

- За повече информация посетете Центъра за помощ.

· **Tik Tok**

- 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.

- За въпроси, притеснения или проблеми, свързани с политиката за поверителност или измамите в TikTok, можете да намерите подкрепа тук. Ще бъдете пренасочени към онлайн формуляр, в който можете да поискате информация за вашите данни, да докладвате за нарушение на поверителността или да попитате за конкретен проблем с поверителността.

· **Twitter**

В Центъра за помощ на Twitter можете да намерите информация и помощ в случай на компрометирани и хакнати акаунти, за поверителност, спам и фалшиви акаунти, чувствително и обидно съдържание, обидно поведение и докладването му.

За докладване на туит:

- Навигирайте до туита, който искате да докладвате, на twitter.com или от приложението Twitter за iOS или Twitter за Android.

- Изберете иконата "...".

- Изберете Report (Докладване).

- Изберете за кого е предназначен докладът: Аз, Някой друг или конкретна група хора, или Всички в Twitter.

- След това Twitter ще ви помоли да предоставите повече информация за проблема, който докладвате. Twitter може също така да ви помоли да изберете допълнителни туитове от акаунта, за който докладвате, за да има по-добър контекст за оценка на доклада ви.

- След това Twitter ще се увери, че разполага с правилната Ви информация, като потвърди какво докладвате, както и допълнителния контекст, който сте споделили, и кое правило може да е нарушено.

- Twitter ще включи текста на съобщените от вас туитове в последващи имейли и известия до вас. За да се откажете от получаването на тази информация, можете да махнете отметката от квадратчето до *Updates about this report can show these Tweets*.

- След като изпратите доклада си, Twitter ще предостави препоръки за допълнителни действия, които можете да предприемете, за да подобрите работата си в Twitter.

За да докладвате акаунт:

- Отидете в акаунта и изберете иконата "...".

- Изберете Report (Докладване).

- Изберете за кого е предназначен отчетът: Аз, Някой друг или определена група хора, или Всички в Twitter.

- След това Twitter ще ви помоли да предоставите допълнителна информация за проблема, който докладвате. Възможно е също така да ви помолят да изберете туитове от този акаунт, за да имат по-добър контекст за оценка на доклада ви.

- След това Twitter ще се увери, че разполага с правилната Ви информация, като потвърди какво докладвате, както и допълнителния контекст, който сте споделили, и какво правило може да е нарушено.

- Twitter ще включи текста на съобщените от вас Туитове в последващи имейли и известия до вас. За да се откажете от получаването на тази информация, можете да махнете отметката от квадратчето до *Updates about this report can show these Tweets.*

- След като изпратите доклада си, Twitter ще предостави препоръки за допълнителни действия, които можете да предприемете, за да подобрите работата си в Twitter.

За да докладвате отделно съобщение или разговор:

- Изберете разговора за директни съобщения и намерете съобщението, което искате да докладвате. (За да докладвате целия разговор, щракнете върху иконата "...").

- Изберете информационната икона "i" и изберете *Report @username.*

- Ако изберете *It's abusive or harmful* (Оскърбително или вредно), Twitter ще ви помоли да предоставите допълнителна информация за проблема, който докладвате. Възможно е също така да ви помолят да изберете допълнителни съобщения от акаунта, за който съобщавате, за да разполагат с по-добър контекст за оценка на доклада ви.

- След като подадете доклада си, Twitter ще предостави препоръки за допълнителни действия, които можете да предприемете, за да подобрите работата си в Twitter.

- **Кога става въпрос за киберпрестъпление?**

Испания:

В Испания последствията от престъпленията в областта на киберсигурността варират от пет години затвор до глоби в размер до 2700 евро.

Преследването се превръща в престъпление, когато някой многократно ограничава чувството за сигурност на човека и когато кара жертвата да се чувства унизена, обидена, заплашена. Не е изненадващо, че всеки, който практикува това, трябва да се изправи пред няколко последствия, които варират от три месеца до две години затвор или заплащане на глоба на жертвата, която съдиите определят.

Разкриването на тайни има последствия и в Испания, тъй като е тежко престъпление. Всяко лице, което "без разрешението на съответното лице разпространява, разкрива или предава на трети лица аудиовизуални изображения или записи", може да бъде осъдено на лишаване от свобода

или също да плати глоба. Разпространението на сексуални изображения е още по-сериозно и може да има допълнителни последици.

Кражбата на самоличност също е наказуема. Това е присвояване на самоличността на дадено лице. С други думи, представянето за това лице, приемането на неговата самоличност от други лица. Пример за това може да бъде създаването на акаунт в социална мрежа, в който се опитвате да се представите за друго лице, за да събирате информация или с друга цел. То се наказва с лишаване от свобода от шест месеца до три години.

Всяка жертва, която иска да предприеме законови действия, трябва първо да събере доказателства за случващото се и след това да съобщи за това в полицейския участък възможно най-скоро. След като го направи, от полицията се свързват с жертвата, като проверяват случая и оценяват ситуацията. Това е предопоставка да бъдат предприети последващи правни действия.

Белгия

Киберсигурността е резултат от набор от мерки за сигурност, които свеждат до минимум риска от неоторизиран достъп до информационните и комуникационните системи. Тя включва всички разумни и приемливи мерки за защита на системите на гражданите, предприятията, организациите и правителството от киберзаплахи. Киберсигурността включва защита на системите (като хардуер, софтуер и свързаната с тях инфраструктура) и мрежите, както и на съдържащите се в тях данни.

В Националната оценка на риска на Белгия за периода 2018-2023 г. на Националния кризисен център киберсигурността се разглежда като един от основните рискове, с които Белгия ще се сблъска през следващите години. В рамките на този клъстер киберпрестъпленията и хактивизмът са определени като национални приоритетни рискове.

Това определение е взето от Центъра за киберсигурност в Белгия[26], националния орган за киберсигурност в страната, който посочва и 4-те основни заплахи, на които киберсигурността има за цел да отговори: чужди военни и разузнавателни служби, тероризъм, хактивизъм и киберпрестъпност. В този доклад киберсигурността е свързана главно със социалните медии, поради прякото им въздействие върху цялостната сигурност на всеки гражданин, включително на младите хора.

През юли 2016 г. беше приета Директивата за сигурността на мрежовите и информационните системи (МИС), която беше транспонирана в белгийското законодателство на 7 април 2019 г. в Закон за създаване на рамка за сигурността на мрежовите и информационните системи от обществен

[26] Centre for Cyber Security Belgium (2022, May).Cybersecurity Strategy Belgium 2.0 2021-2025. Available: https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf

интерес за обществена сигурност. Член 7 от тази директива (възпроизведен в член 10 от белгийския Закон за МИС) изисква от държавите членки да изготвят национална стратегия за сигурността на мрежовите и информационните системи. До публикуването на белгийския Закон за мрежовите и информационните системи през май 2019 г. страната не разполагаше с цялостно законодателство в областта на киберсигурността. Тази голяма стъпка беше постигната благодарение на Агенцията на Европейския съюз за киберсигурност (ENISA), която допринася за политиката на ЕС в областта на киберсигурността, повишава надеждността на ИКТ продуктите, услугите и процесите със схеми за сертифициране на киберсигурността, сътрудничи с държавите членки и органите на ЕС и помага на Европа да се подготви за киберпредизвикателствата на утрешния ден. Освен това бихме могли да подчертаем следното законодателство, което се прилага в Белгия в зависимост от преследваното киберпрестъпление:

- Белгийски наказателен кодекс: чл. 550 (б) "Хакерство", чл. 210bis "онлайн измама“;

- Закон от 1 юли 2011 г. за сигурността и защитата на критичните инфраструктури

-Директива (ЕС) 2016/1148 от 6 юли 2016 г. относно мерките за постигане на високо общо ниво на сигурност на мрежовите и информационните системи в Съюза

-Закон от 7 април 2019 г. за създаване на рамка за сигурност на мрежите и информационните системи от общ интерес за обществената сигурност

- Кралски указ от 12 юли 2019 г. за прилагане на закона от 7 април 2019 г. за създаване на рамка за мрежата за сигурност и информационните системи от общ интерес за обществена сигурност

- Регламент (ЕС) 2019/881 от 17 април 2019 г. относно ENISA

- Регламент за изпълнение (ЕС) 2018/1151 на Комисията от 30 януари 2018 година за установяване на правила за прилагането на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета по отношение на допълнителното уточняване на елементите, които доставчиците на цифрови услуги трябва да вземат предвид при управлението на рисковете за сигурността.

Нидерландия:

През 2021 г. близо 2,5 милиона души в Нидерландия на възраст 15 или повече години са съобщили, че са станали жертва на киберпрестъпление - това е близо 17% от населението!

Нидерландският парламент прие законодателство относно киберпрестъпността, което предотвратява следното:

● Член 138а: умишлено и незаконно получаване на достъп до автоматизирана система за съхранение или обработка на данни или до част от такава система;
● член 138б: незаконно сериозно възпрепятстване на обработката на данни;
● член 232: фалшифициране на електронен знак, който има доказателствена стойност, и използването на такива знаци като истински.

Киберпрестъпленията се определят като "престъпления, включващи цифрови форми на измама на самоличността, измама при покупка или продажба онлайн, хакерство и кибертормоз (клевета, преследване, изнудване и заплахи за насилие, извършени онлайн)"[27].

Киберпрестъпленията, свързани с неприкосновеността на личния, организационния и правителствения живот, са криминализирани от нидерландското законодателство (в съответствие с горепосочените членове). Най-често срещаните киберпрестъпления, за които се съобщава в Нидерландия, са:

● хакерство
● измами при онлайн пазаруване
● кибертормоз[28]

Често срещаните киберпрестъпления, идентифицирани от нидерландското правителство, са следните[29]:

● Фишинг: използване на фалшиви имейл съобщения за получаване на лична информация от интернет потребители
● Злоупотреба с лична информация (кражба на самоличност)
● Хакерство: злоупотреба с уебсайтове или компютърни мрежи
● Разпространение на омраза и подстрекаване към тероризъм
● Разпространение на детска порнография
● Подмамване: отправяне на сексуални предложения към непълнолетни лица

[27] The Netherlands in Numbers : https://longreads.cbs.nl/the-netherlands-in-numbers-2020/what-about-cyber-crime/#:~:text=Hacking%2C%20online%20shopping%20fraud%20and%20cyber%20bullying&text=Hacking%20was%20most%20common%2C%20mentioned,such%20as%20stalking%20or%20threats.
[28] *Ibid*
[29] Forms of Cybercrime: https://www.government.nl/topics/cybercrime/forms-of-cybercrime

Националната служба за киберсигурност (NCSC) отговаря за надзора на цифровата сигурност в Нидерландия[30]. Тя прави това като:
● Непрекъснато следи всички подозрителни източници в интернет
● съветва организациите как да се предпазват от онлайн заплахи
● следи развитието на цифровите технологии и актуализира системите за сигурност

България

"Киберпрестъпността" (наричана още "компютърна престъпност" или "високотехнологична престъпност") следва да се разбира като "престъпни деяния, извършени чрез използване на електронни комуникационни мрежи и информационни системи или срещу такива мрежи и системи". Всъщност терминът се отнася до три категории престъпни деяния. Първата обхваща традиционни видове престъпления като измама или фалшифициране, въпреки че в контекста на киберпрестъпността тази категория се отнася по-специално до престъпления, извършени чрез електронни съобщителни мрежи и информационни системи ("електронни мрежи"). Втората категория се отнася до публикуването в електронни медии на незаконно съдържание (като детска порнография или съдържание, подтикващо към насилие и свързано с реч на омразата и дискриминация). Третото включва престъпления, специфични за електронните мрежи, като атаки срещу информационни системи, отказ на услуга и хакерство.
България е ратифицирала Конвенцията за престъпленията в кибернетичното пространство, приета от Съвета на Европа през 2001 г., и протоколите към нея. Въз основа на нея Наказателният кодекс на България включва определения и санкции, свързани с киберпрестъпленията.
Наказателният кодекс очертава различните видове киберпрестъпления:
-Кибер измама е дефинирана в чл. 212a
-Особена форма на унищожаване и повреждане чрез използване на цифрови инструменти е дефинирана в чл. 216, ал. 2.
-Специален начин на нарушаване на тайната на кореспонденцията е определен в чл. 171.
-Детската порнография също е специално криминализирана.
-Киберпрестъпленията, очертани в глава 9 от Наказателния кодекс (чл. 319a до чл. 319e от Наказателния кодекс). Те засягат обществените отношения, които осигуряват правилното функциониране на компютрите, компютърните системи, компютърните ресурси и компютърните мрежи, както и законосъобразното създаване и използване на информация. Те включват неразрешен достъп, промяна, повреждане, унищожаване на данни или програми, въвеждане на вирус или разпространение на пароли.

[30] Fighting Cybercrime in the Netherlands: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands

-Първото се отнася до копирането или използването на компютърни данни без разрешение чрез получаване на неоторизиран достъп до компютърни ресурси (чл. 319а).
-Фалшифициране или унищожаване на компютърна програма или данни е изрично споменато като киберпрестъпление в чл. 319б. Това включва добавянето, модифицирането или изтриването на компютърна програма или компютърни данни, което ги прави неавтентични или несъответстващи на оригиналните програми и данни.
-Въвеждането на компютърен вирус в компютър или информационна мрежа е посочено в чл. 319г, ал. 1 от Наказателния кодекс.
-Чл. 319д, ал. 1 от Наказателния кодекс включва разпространението на компютърни или системни пароли, когато това води до разкриване на лични данни или лична тайна. Наказанието е до една година лишаване от свобода.

Що се отнася до неприкосновеността на личния живот и сигурността онлайн, важно е да се отбележи, че българските разпоредби са свързани с GDPR, който се регулира от Комисията за защита на личните данни. Тя е независим държавен орган, който защитава физическите лица при обработването на техните лични данни и при достъпа до тези данни, както и контрола върху спазването на Закона за защита на личните данни. Тя е независим, колегиален орган и се състои от председател и четирима членове. Членовете на комисията и нейният председател се избират от Народното събрание по предложение на Министерския съвет за срок от 5 години и могат да бъдат преизбирани за нов мандат. Една от най-важните роли на Комисията е да сезира Съда на Европейския съюз в България по въпроси, свързани с нарушения на GDPR.

3.4 Как да избегнем рисковете за сигурността на личните ни данни

Едно от най-важните неща, които трябва да направим, за да защитим данните си, е да имаме силна парола. 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. Някои от потенциалните последици от слабите пароли включват нарушаване на сигурността на данните, кражба на самоличност, превземане на компютъра, изнудване и загуба на лична информация.

Ето защо, за да се предпазим от тези последствия, можем да следваме някои съвети за това как да създадем силна парола на акаунтите си:

- Никога не използвайте лична информация. Може да изглежда очевидно, но много хора използват лична информация, когато създават паролата си. Препоръчително е да не използвате имена, рождени дни, адреси или телефонни номера.

- Включете комбинация от букви, цифри и символи. Колкото повече произволни символи използвате, толкова по-сложна ще бъде паролата ви.

- Дайте приоритет на дължината на паролата. Тя ще намали вероятността да станете жертва на кибератака.

- Никога не повтаряйте пароли. Хората са свикнали винаги да избират една и съща парола. Това е огромна грешка, тъй като ги излага на риск от credential stuffing атаки.

- Избягвайте да използвате истински думи. Хакерите използват злонамерени програми, които могат да обработват всяка дума, открита в речника, за да разбиват пароли. Ето защо използването на измислени думи може да помогне за създаването на силна и сигурна парола.

Освен това, за да запазите информацията си защитена, е препоръчително да използвате само уебсайтове, на които имате доверие. Много хора не знаят как да проверят дали даден уебсайт е безопасен или не, затова по-долу са дадени някои съвети за това:

- На първо място, проверете дали URL адресът се изписва правилно, дали е защитен с "https" и дали има някакъв индикатор, че е проверен, например знак за заключване.
- На второ място, 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.
- На трето място, трябва да можете да проверите дали 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 тя си има цена. Тези безплатни WIFI горещи точки позволяват на хакерите да се позиционират между лицето, което ги използва, и точката за връзка, така че вместо да говорят директно с горещата точка, хората изпращат информацията си на хакера, който след това разчита на нея. Тогава хакерите имат достъп до всяка информация, която хората изпращат в интернет: важни имейли, информация за кредитни карти и данни за сигурност. След като хакерите разполагат с тази информация, те могат да

получат достъп до вашите системи, сякаш са вие. За да не бъдете хакнати по този начин, се препоръчва да не използвате WIFI, когато не ви е необходим, а когато се налага да използвате този тип връзки, да го правите с VPN. VPN е виртуална частна мрежа, тъй като тя ще ви помогне информацията ви да бъде силно криптирана. Ако наистина се налага да използвате този безплатен WIFI, опитайте се да не извършвате онлайн банкиране, пазаруване или работа. Нещо, което може да помогне, е и изключването на Bluetooth и споделянето на файлове.

Как физическите лица могат да защитят личните си данни?

1. Защитете акаунтите си

През последното десетилетие нарушения на сигурността на данните и изтичане на пароли засегнаха големи компании като Facebook, Home Depot, Marriott, Yahoo и т.н., а правителствените институции също пострадаха от кибератаки, чрез които трети неоторизирани страни получиха достъп до лична информация на гражданите (например атаката срещу българската Национална агенция за приходите през 2019 г.). Ако имате онлайн акаунти, възможно е хакери да са изнесли данни от поне един от тях. За да проверите това, можете да потърсите имейл адреса си в сайта Have I Been Pwned?, за да съпоставите имейл адреса си със стотици случаи на нарушаване на сигурността на данни ("нарушение" е инцидент, при който данни са изложени по невнимание в уязвима система, обикновено поради недостатъчен контрол на достъпа или слабости в сигурността на софтуера).

Има и други начини за идентифициране на възможни признаци, че даден акаунт е бил хакнат, самоличността ви е била откраднатa или данните ви са били нарушени по някакъв друг начин. Образовайте се относно предупредителните знаци за потенциално нарушение и си създайте положителни навици за наблюдение на сигурността на личните ви данни, за да идентифицирате потенциални атаки или нарушения, преди да са прераснали в опустошителни. Прочетете съвети за защита на данните и информация, в която са описани обичайните предупредителни признаци за нарушаване на сигурността на данните или хакерска атака, като например този списък "15 признака, че сте били хакнати - и как да отвърнете на удара".

Ако профилът ви е бил хакнат, данните ви са били загубени или устройството ви е било откраднато, считайте това за възможност да научите нещо ново. Разберете какво точно се е объркало и как сте могли да защитите данните си, като вземете по-добри предпазни мерки. Докато поправяте нещата, е добър момент да направите крачка назад и да си зададете един по-основен въпрос: Каква е била причината за нарушението? Ако това е била банковата ви сметка, отговорът може да е очевиден. В други случаи, като например електронната поща, причините могат да бъдат много - от използването ѝ за изпращане на спам, през искане на пари от контактите ви, до получаване на нулиране на пароли за други услуги.

Нападателят може дори да се опитва да получи достъп до вашия бизнес. Знанието за причините, поради които сте били обект на атака, понякога може да ви помогне да разберете и как е било извършено нарушението.

Един от начините да повишим нивото на цифрова сигурност и да защитим личните си данни е да използваме мениджър на пароли, за да създаваме и помним различни, сложни пароли за всеки акаунт - това е едно от най-важните неща, които хората могат да направят, за да защитят личния си живот и сигурност днес. LastPass и 1password могат да ви помогнат да направите това, като генерират пароли, следят акаунтите за нарушения на сигурността, предлагат промяна на слабите пароли и синхронизират паролите между компютъра и телефона ви. Не използвайте номера на социални осигуровки, телефонни номера, адреси или друга лична информация като пароли.

Друго предложение е също така да използвате двустъпково удостоверяване, когато е възможно, за вашите онлайн акаунти. Повечето банки и големите социални мрежи предоставят тази възможност. Както подсказва името, двустъпковото удостоверяване изисква две стъпки: въвеждане на парола и въвеждане на номер, до който имате достъп само вие. Например първата стъпка е влизане във Facebook с вашето потребителско име и парола. При втората стъпка Facebook ви изпраща временен код в текстово съобщение или, още по-добре, чрез приложение като Google Authenticator, и вие въвеждате този код, за да влезете в системата.

2. Защитете сърфирането си в интернет

Компаниите и уебсайтовете следят всичко, което правим онлайн. Всяка реклама, бутон на социална мрежа и уебсайт събират информация за вашето местоположение, навици на сърфиране и др. Събраните данни разкриват за вас повече, отколкото бихте очаквали. Дори и да не споделяте публично личната си информация в социалните мрежи, има голяма вероятност уебсайтовете, които посещавате редовно, да предоставят всички данни, от които рекламодателите се нуждаят, за да определят какъв тип човек сте. Това е част от начина, по който целевите реклами остават едно от най-тревожните нововъведения в интернет.

Разширение за браузър като uBlock Origin блокира рекламите и данните, които те събират. Разширението uBlock Origin също така предотвратява стартирането на зловреден софтуер в браузъра ви и ви дава лесен начин да изключите блокирането на реклами, когато искате да поддържате сайтове, за които знаете, че са сигурни. Можете да комбинирате uBlock с Privacy Badger, който блокира тракери, и рекламите няма да се появяват навсякъде. За да забавите още повече рекламите на преследвачите, деактивирайте рекламите, базирани на интереси, от Apple, Facebook, Google и Twitter. Много уебсайтове предлагат средства за отказване от събирането на данни, но

трябва да го направите ръчно. Ако направите това, няма да елиминирате проблема напълно, но ще намалите значително количеството на събираните данни.

Инсталирането на разширението HTTPS Everywhere също помага за защита на личната ви информация. То автоматично ви насочва към защитената версия на даден сайт, когато сайтът поддържа това, като по този начин затруднява нападателя - особено ако сте на обществен Wi-Fi в кафене, на летище или в хотел - да подслушва дигитално това, което правите.

3. Използвайте антивирусен софтуер на компютъра си

Вирусите може и да не изглеждат толкова разпространени, колкото преди десетилетие, но те все още съществуват. Злонамереният софтуер на компютъра ви може да причини всякакъв вид хаос - от досадни изскачащи прозорци до скрито добиване на биткойни и сканиране за лична информация. Ако сте изложени на риск да щракнете върху опасни връзки или ако споделяте компютър с няколко души в домакинството, си струва да настроите антивирусен софтуер, особено на компютри с Windows. Ако компютърът ви работи с Windows 10, трябва да използвате вградения софтуер на Microsoft - Windows Defender. Можете също така да имате допълнителен слой защита, ако инсталирате антивирусна програма.

4. Актуализирайте софтуера и устройствата си

Операционните системи за телефони и компютри, уеб браузърите, популярните приложения и дори устройствата за интелигентен дом получават чести актуализации с нови функции и подобрения в сигурността. Тези актуализации за сигурност обикновено са много по-добри в предотвратяването на хакери от антивирусния софтуер.

И трите основни операционни системи могат да се актуализират автоматично, но трябва да отделите малко време, за да проверите дали сте активирали автоматичните актуализации за избраната от вас операционна система: Windows, macOS или Chrome OS. Въпреки че е неприятно да включите компютъра си и да трябва да изчакате актуализация, която може да повреди използвания от вас софтуер, ползите за сигурността си заслужават. Телефонът ви също има опции за автоматични актуализации, но понякога се налага ръчно да одобрявате инсталирането на актуализациите.

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

Всяко странно приложение, което инсталирате на телефона си, и всяко разширение за браузър или софтуер, който изтегляте от съмнителен уебсайт, представлява още една потенциална дупка в поверителността и

сигурността. Безброй мобилни приложения следят местоположението ви навсякъде, където отидете, и събират данните ви, без да искат съгласие, дори в детските приложения. Придържайте се към изтеглянето на програми и разширения за браузъри директно от техните създатели и официалните магазини за приложения.

Добре е да знаете кои приложения имат достъп до вашето местоположение, контакти, микрофон и други данни. Деактивирайте разрешенията, когато нямат смисъл - например Google Maps се нуждае от местоположението ви, за да функционира, но не и приложението ви за бележки. В бъдеще, когато инсталирате нов софтуер, мислете за разрешенията на приложенията; ако приложението е безплатно, то вероятно събира и продава данните ви.

6. Деактивирайте Bluetooth, когато не го използвате

Технологията Bluetooth предложи невероятни удобства на мобилния свят, но също така отваря врата за уязвимости. Повечето заплахи, използващи Bluetooth свързаност, зависят от активната Bluetooth връзка и макар че обикновено не са опустошителни или опасни, със сигурност са неудобни и могат да бъдат сериозни. Bluetooth атаките зависят от използването на процеса на искане/даване на разрешение, който е в основата на Bluetooth свързаността. Независимо от функциите за сигурност на вашето устройство, единственият начин да се предотврати напълно използването на този процес на искане/даване на разрешение от страна на нападателите е да изключите функцията Bluetooth на вашето устройство, когато не я използвате - не да я поставите в невидим или неоткриваем режим, а да я изключите напълно.

7. Бъдете предпазливи, когато споделяте лична информация

Този съвет се отнася както за онлайн, така и за офлайн света: Кой иска личната ви информация, като например номера на социалната ви осигуровка или информация за кредитна карта? Защо им е необходима? Как ще я използват? Какви мерки за сигурност прилагат, за да гарантират, че личната ви информация ще остане поверителна? Всички тези важни въпроси трябва да получат ясен отговор, преди да предоставите личните си данни на когото и да било.

8. Внимавайте за имитатори

Във връзка с предишния съвет има много измамници, които се опитват да подмамят нищо неподозиращите потребители да предоставят чувствителната си лична информация, като се представят за банката на лицето, компанията за кредитни карти или друга структура. Това може да се случи по телефона или онлайн, чрез фишинг имейли или уебсайтове,

създадени да имитират външния вид на автентичната компания. Уверете се, че знаете кой получава вашата лична или финансова информация. Не предоставяйте лична информация по телефона, по пощата или по интернет, освен ако не сте инициирали контакта или не знаете с кого имате работа. Ако компания изпрати имейл с искане за лична информация, не кликвайте върху линковете в имейла. Вместо това въведете името на компанията в уеб браузъра си, отидете на нейния сайт и се свържете с нея чрез отдела за обслужване на клиенти. Или се обадете на номера за обслужване на клиенти, посочен в извлечението от сметката ви. Попитайте дали компанията наистина е изпратила искане.

9. Не споделяйте твърде много информация в платформите на социалните мрежи

Социалните мрежи са се превърнали в начин на живот за много хора, но споделянето на твърде много лична информация в профилите ви в социалните мрежи може да бъде опасно. Например много хакери успешно отгатват пароли чрез методите "проба-грешка", като използват комбинации от често срещана информация (като имена на деца, адреси и други данни), която лесно се намира в профилите на потребителите в социалните мрежи. Не публикувайте информация, която би ви направила уязвими, като например адреса ви или информация за вашия график или ежедневие. Ако вашите приятели и познати публикуват информация за вас, уверете се, че комбинираната информация не е повече, отколкото бихте се чувствали комфортно непознати да знаят. Бъдете внимателни и когато публикувате информация, включително снимки, за вашите приятели и познати.

10. Персонализирайте настройките си за поверителност в социалните мрежи

Социалните мрежи като Facebook дават възможност на потребителите да персонализират настройките си за поверителност. Във Facebook, например, можете да изберете кой да вижда съдържанието, което публикувате, и кой да вижда информацията в профила ви, като например местоработата ви, датата на раждане и родния град. Винаги избирайте възможно най-високото ниво на поверителност, за да сте сигурни, че личните ви данни няма да попаднат в ръцете на злонамерен човек. Съдържанието, което публикувате онлайн, ще бъде на разположение дълго време, но можете да персонализирате настройките за поверителност в повечето сайтове на социални медии. Това ще повлияе на това кой може да се свърже с вас и кой може да види информацията, която публикувате. Бъдете избирателни: макар да е забавно да споделяте информация, имайте предвид онлайн репутацията си. Ако прекалите с публичното разкриване на информация, тя може да бъде използвана от крадци на самоличност, за да присвоят самоличността ви.

11. Не забравяйте да излезете от акаунта си

Влизането в онлайн услуги е необходимо, когато трябва да получите достъп до личните си акаунти, но много потребители забравят да излязат, когато приключат с използването на дадена услуга. Когато осъществявате достъп до уебсайтове, базирани на акаунти, чрез публичен компютър (или споделено устройство), не забравяйте да излезете от услугата, когато сесията приключи. Това, че след посещението на сайт, в който сте влезли, се получава достъп до нов уебсайт, не означава, че следващият потребител не може да натисне бутона за връщане и да получи достъп до вашия акаунт. Някои системи са настроени и за автоматично запазване на информация, така че не забравяйте да проверите дали тази функция е деактивирана.

12. Не отваряйте имейли от хора, които не познавате

Ако получите имейл от източник или лице, което не познавате, не го отваряйте и определено избягвайте да кликвате върху всякакви връзки или прикачени файлове. Има едно златно правило за справяне със спам имейли: ако изглежда като спам съобщение, вероятно е такова - затова го изтрийте, без да кликвате или изтегляте нищо. Такива съобщения могат да съдържат софтуер, който съобщава на изпращача, че сте отворили съобщението, потвърждавайки, че имате активен акаунт, което може да доведе до още повече спам съобщения. Някои зловредни програми могат да откраднат имейл адреса ви и да го използват за повторно изпращане на спам съобщения под прикритието на легитимен адрес. Например, измамниците могат да се представят за някой ваш познат, например приятел, роднина или колега/съученик. Ако въпросното съобщение изглежда, че идва от някой ваш познат, свържете се с него извън електронната си поща.

13. Не запазвайте пароли в браузъра си

Широко разпространената практика за "запомняне на пароли" в браузърите е опасна практика. Всъщност, ако някой получи достъп до вашия компютър или мобилно устройство, той ще може лесно да получи достъп до всички акаунти, за които сте запазили данни за вход в браузъра си. Макар че това може да направи влизането в системата по-удобно, това е рискован навик от гледна точка на защитата на данните. Следете за тези изскачащи прозорци и не забравяйте да ги откажете.

14. Не използвайте идентификационните данни от социалните медии за регистрация или влизане в сайтове на трети страни.

Изглежда като удобна опция: просто се регистрирате за даден уебсайт или онлайн услуга, като използвате профила си във Facebook или LinkedIn, и стига да сте влезли в тази социална мрежа, влизането в сайта на трета страна е бързо и лесно. Това обаче може да застраши поверителността ви. Въпреки че е удобна опция, влизането в друг акаунт с вашето потребителско име и парола във Facebook може да означава, че предоставяте на другия сайт

цялата информация, която Facebook е събрал за вас. По-лошото е, че ако някой похити информацията ви за вход в социалната мрежа, той може да получи достъп и до тези акаунти.

15. Изберете сигурен доставчик на електронна поща

Уверете се, че вашият доставчик на електронна поща гарантира подходяща сигурност. Трябва да се уверите, че доставчикът ви на електронна поща използва технология като DMARC, за да спре фишинга и да сведе до минимум рисковете. Добрата новина е, че Google го прави, Yahoo го прави, Microsoft го поддържа, AOL го поддържа, така че ако използвате един от тези доставчици на услуги, сте на път да сведете до минимум рисковете за поверителността и сигурността.


4. Неформално образование

В този раздел ще разгледаме накратко контекста на неформалните начини за повишаване на осведомеността относно кибертормоза и речта на омразата в партньорските държави по проекта:

Нидерландия

Съществуват и неформални начини, чрез които хората осъзнават по-добре проблемите, свързани с безопасността в интернет. За киберсигурността се говори не само в рамките на формалното образование, а в новините, в изказванията на влиятелните личности онлайн, в разговорите с родителите и учителите, както и в споделеното от жертвите на киберпрестъпления.

Киберсигурност и неприкосновеност на личния живот:

Справянето с киберсигурността и неприкосновеността на личния живот или регулирането им често се свързва с официални институции и органи или с формалното образование. Неформалното образование в тази област обаче също оказва влияние.

Шантал Стекеленбург е част от Асоциацията на общността "Жени в киберсигурността" и е спечелила голям брой последователи в интернет. Тя се изказва по въпросите на киберсигурността и основно се фокусира върху насърчаването на жените да станат експерти по сигурността.

Кибертормоз:

Влиятелните личности и други лица, които говорят за кибертормоза, оказват важно влияние върху начина, по който хората гледат на този проблем, и върху това колко образовани са те по отношение на него. Много млади хора често се срамуват да подават сигнали или да споделят за проблема с персонала в училище или в други институции. Затова неформалните подходи са полезни, тъй като позволяват на хората, които са се сблъскали с кибертормоз, да се свържат с други хора, да се чувстват по-малко самотни и по-склонни да говорят.

През 2018 г. в новинарска статия се съобщава, че нидерландски апелативен съд е потвърдил присъдата за лишаване от свобода на мъж, осъден за кибертормоз над много млади мъже и жени, много от които от Нидерландия. Той е оказвал натиск върху момичета да извършват сексуални действия пред уебкамери. Тази история привлече голямо внимание в медиите и може да се разглежда като ясен пример за неформално образование по отношение на кибертормоза и киберпрестъпленията. По същество колкото повече внимание се обръща на случаи като този, толкова повече се

повишава осведомеността и хората стават по-подготвени да предотвратяват и съобщават за такива случаи.

Реч на омразата:

Значението на неформалното образование се разпростира и върху речта на омразата, тъй като е жизненоважно хората да говорят за нея. По този въпрос се провеждат важни кампании.

В Нидерландия се провежда национална кампания, която е част от по-широката младежка кампания на Съвета на Европа "Без език на омразата" и има за цел да мобилизира младите хора да се борят с езика на омразата и да насърчават правата на човека. Това насърчава хората да съобщават за реч на омразата и директно да се борят с нея. Следователно онлайн активистите разполагат с платформа и общност, в която могат да споделят идеи и да се обединят срещу този проблем, давайки възможност на хората да осъждат речта на омразата.

Испания

Когато говорим за начините за повишаване на осведомеността относно кибертормоза и речта на омразата в Испания чрез неформално образование, няма как да не споменем важната роля на културата, влиятелните личности и големите кампании в тази сфера.

Кибертормоз

Влиятелните личности (инфлуенсъри) наистина са потенциален ориентир за хората. С милиони последователи тази нова професия е в състояние да достигне до по-висок таргет чрез социалните медии и онлайн платформите. Методологията е проста и ефективна, докато хората консумират социалните медии през свободното си време, те получават и цялата тази информация, предавана от инфлуенсърите, без да полагат допълнителни усилия.

В Испания има много примери за влиятелни личности, които са използвали известността си, за да повишат осведомеността относно кибертормоза. Например, Y luego ganas tú (Nube de Tinta) е книга с разкази, в която авторите (5 испански инфлуенсъри) разказват чрез собствените си истории и измислици, които се опират на реалността, за проблема с тормоза в училище. Проблем, който излиза извън контрол в обществото: един на всеки двама ученици в Испания твърди, че е претърпял някакъв вид тормоз или кибертормоз. Тези влиятелни личности са Хавиер Руескас, Ману Карбайо, Джедет Санчес, Мария Ерехон и Андреа Комптън и са популярни в Испания с борбата си за социални права и видимост.

Друг пример за усилия в борбата с кибертормоза е подкастът Estirando el chicle, ръководен от Каролина Иглесиас и Виктория Мартин. В този подкаст се интервюират много известни хора, които повдигат теми като кибертормоз или ЛГБТ общността. Всъщност подкастът е получил голямо признание и награди като Ondas Award за най-добър подкаст или програма за цифрово излъчване за това, че е "новаторска програма по отношение на езика и подхода, която съчетава хумор, интервюта и социално съдържание без предразсъдъци". Освен това би било уместно да се спомене и как известната марка шампоани H&S също е допринесла за борбата с тормоза. В кампанията "Спри тормоза" много испански публични личности, като Марта Помпо или Ебай, повишават осведомеността относно този проблем, като разказват собствения си опит с речта на омразата в социалните медии. Освен това на уебсайта на H&S е активиран образователен микросайт със съвети за ученици, учители и родители, за да ги накара да поемат активна роля в ситуации на тормоз.

Белгия

От Белгия бихме искали да обърнем внимание на една комуникационна кампания срещу кибертормоза сред младите хора и да подчертаем един от най-важните фактори в нея:

● Кампания WAT TEGEN WAT PESTEN

Младежката платформа WAT WAT работи съвместно с влиятелни личности и млади хора, за да обсъжда тормоза сред младежите, чрез споделяне на съвети и опит. С помощта на игра във Facebook Messenger WAT WAT предизвиква разговор за тормоза. Да тормозиш или да бъдеш тормозен, да тролиш или да харесваш, да тормозиш или да харесваш: изборът е твой.

Кампанията е разработена по време на фламандската "Седмица за борба с тормоза", за да запознае децата и младежите с това какво е тормозът, какво може да се направи по въпроса и какви са последиците от него.

Публично бяха споделени истински истории: Анжел (16 г.) е принудена от своите насилници да яде отпадъци. В седмицата срещу тормоза тя - заедно с Ясмин Начири (27 г.), Марго (22 г.) и Жорит (23 г.) - споделя историята си и показва белезите си от дългогодишния тормоз. Тези смели истории насърчават младите хора да се замислят, да говорят за това и да си помагат взаимно.

WAT WAT призовава всички да направят повече срещу тормоза. Тя спомага за повишаване на осведомеността, като дава възможност на ученици и учители да окачат плакатите на кампанията в класните си стаи и да

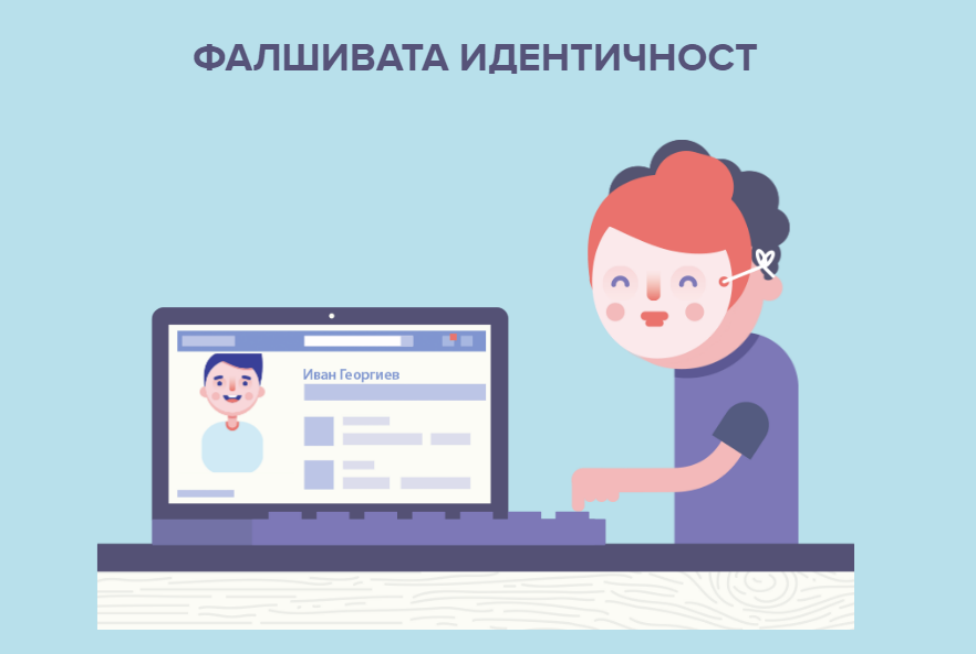
превърнат тормоза в тема за обсъждане. Кампанията използва хаштага #tegenpesten (#против тормоза).

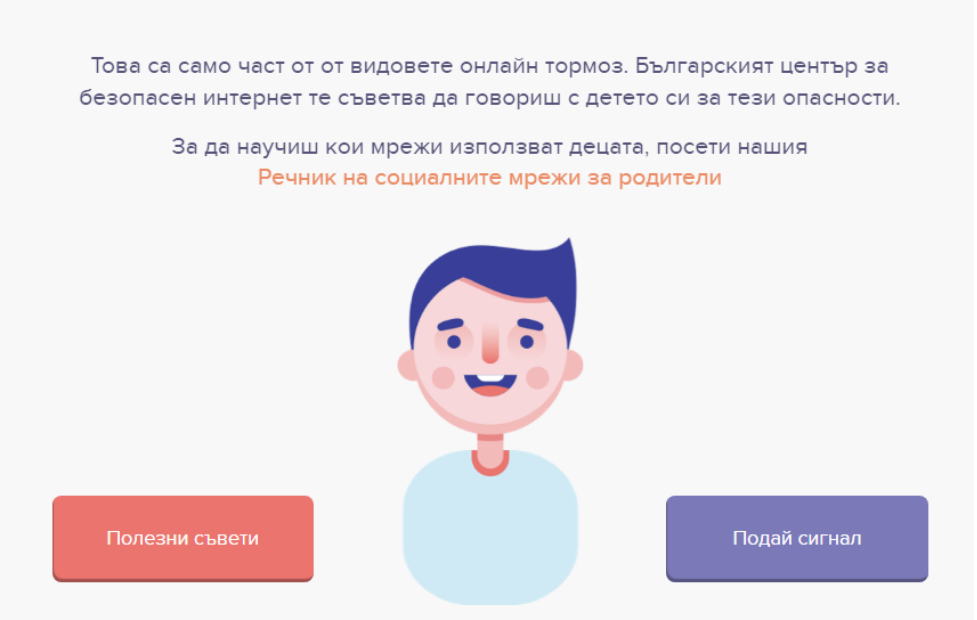
● Angèle, най-успешната белгийска певица в момента, е и най-следваният инфлуенсър в Instagram в страната с 3,6 милиона (Statista, 2019). Изпълнителката е доста ангажирана с прекратяването на речта на омразата срещу жените и ЛГБТ общността, и това намира отражение в нейните песни.

България

Кибертормозът е проблем, който се засяга от няколко онлайн кампании и организации, които работят за неговото предотвратяване и за повишаване на осведомеността на младите хора, родителите и учителите в тази сфера. Пример за такава онлайн кампания са Насоките за кибертормоз, разработени от Safenet.bg: https://cyberbullying.safenet.bg/

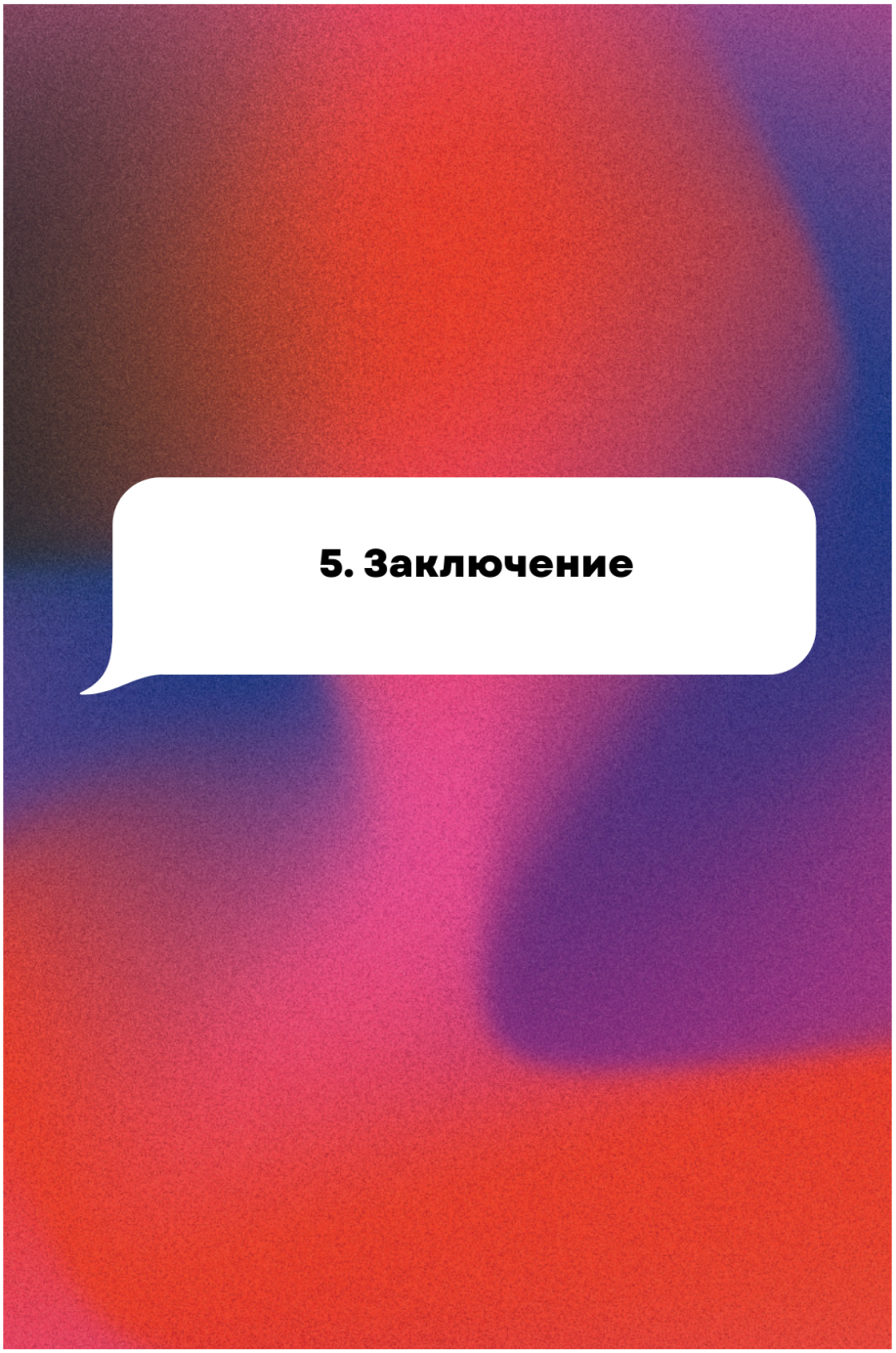
Тук по много нагледен начин младите хора могат да видят примери за кибертормоз и могат да споделят, ако са преживели нещо подобно - могат да съобщят за инцидент чрез предоставената връзка. Могат да прочетат и полезна информация, съвети и препоръки за кибертормоза и как да реагират на него.





Safenet.bg има и канал в YouTube, в който има видеоклипове, свързани с кибертормоза, речта на омразата онлайн и т.н., с цел повишаване на осведомеността на младите хора по тези въпроси по по-атрактивен и нагледен начин.

Телекомуникационната компания Yettel също има канал в YouTube, разработен през 2020 г., в който има разнообразни видеоклипове за млади хора с информация за различни онлайн рискове, с които младите хора могат да се сблъскат, като фалшиви профили, кибертормоз, опасни връзки, рискове в Tik-Tok и YouTube, в игрите и др.


5. Заключение

5. Заключение

В този наръчник кибертормозът и речта на омразата са обяснени и контекстуализирани. Определенията им могат да варират в различните страни, но и двете се считат за агресия към други хора. 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 различни начини за идентифициране, справяне със и докладване на кибертормоза и речта на омразата, в зависимост от това кой е жертвата (вие, съученик/колега, вашите деца и т.н.), както и от правната рамка на страната. В Испания например можете да подадете сигнал в полицията, докато в Нидерландия има специална национална телефонна линия за помощ при дискриминация.

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

В заключение, настоящият документ не само предлага определения или ключови понятия по отношение на кибертормоза и речта на омразата, но и служи като наръчник за предотвратяване, реагиране и докладване на тези видове дигитални опасности.


6. Източници

6. Източници

101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022. (2022, May 26). Digital Guardian. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

A, D. (2020). *Cyberbullying (for Parents) - Nemours KidsHealth*. Nemours KidsHealth. https://kidshealth.org/en/parents/cyberbullying.html

A, D. (2020). *Cyberbullying (for Parents) - Nemours KidsHealth*. Nemours KidsHealth. https://kidshealth.org/en/parents/cyberbullying.html

A. (2018). *Report security vulnerabilities | TikTok Help Center*. TikTok. https://support.tiktok.com/en/safety-hc/reporting-security-vulnerabilities/reporting-the-security-vulnerabilities.

Assistant Secretary for Public Affairs (ASPA). (2019b, December 4). *Report Cyberbullying*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/how-to-report

Assistant Secretary for Public Affairs (ASPA). (2021, May 21). *Tips for Teachers*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/tips-for-teachers

C, S. (2021). *Password security: How to create strong passwords in 5 steps.* Norton. https://us.norton.com/internetsecurity-privacy-password-security.html.

Caroline Rizza. (2013). *Social networks and Cyber-bullying among teenagers: EU Scientific e political report.* https://doi.org/10.2788/41784

Celine Chateau. (2016). *Policy department Citizen¡s rights and constitutional affairs*. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Center, C. R. (2021, October 18). *Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online*. Cyberbullying Research Center. https://cyberbullying.org/preventing-cyberbullying-adults

CISCO. (2021). *Think Before You Click* [Slides]. CISCO. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf

Commission for Personal Data Protection, available. (2019). FOLD. https://www.cpdp.bg/?p=element&aid=12

Convention on Cybercrim (No. 185). (2001, November). Convention on Cybercrime. https://rm.coe.int/1680081561

Cyberbullying Research Center. (2022). *Cyberbullying Fact Sheet: Identification, Prevention, and Response*. https://cyberbullying.org/cyberbullying-fact-sheet-identification-prevention-and-response

Defining online sexual harassment. (2021, December 15). Childnet. https://www.childnet.com/what-we-do/our-projects/project-deshame/defining-online-sexual-harassment/

Digital Guardian. (22–05-26). *101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022.* https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe.

Facebook - Meld je aan of registreer je. (2018). Facebook. https://www.facebook.com/unsupportedbrowser

Griffin, M. (2020, March 5). *Advice on what to do if your child is a victim of cyber bullying*. Laya Healthcare. https://www.layahealthcare.ie/thrive/family/what-to-do-if-your-child-is-victim-of-cyber-bullyi/.

How to Protect Your Digital Privacy. (2019). The Privacy Project Guides - The New York Times.
https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

Identity Theft. (2022, June 12). Investopedia. https://www.investopedia.com/terms/i/identitytheft.asp

Instagram Help Center. (2018). Instagram. https://help.instagram.com/192435014247952?helpref=uf_permalink

J. (2013). *Social Networks and Cyber-bullying among Teenagers*. JRC Publications Repository. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

L. (2021, 28 enero). *Ciberdelincuencia en el código penal - Letslaw*. LetsLaw. https://letslaw.es/ciberdelincuencia/

L.J. (2022, June 2). *Delitos en redes: de cinco años de cárcel a multas de hasta 2.700 euros*. Diario Noticias de Álava. https://www.noticiasdealava.eus/vivir-on/internet-y-ciencia/2022/04/24/delitos-redes-consecuencias/1183252.html.

Lex.bg - Р—Р°РєРѕРЅРё, РїРЂР°РІРёР»РЅРёС†Рё, РєРѕРЃС‚РёС‰, РєРѕРґРµРєСЃРё, РґРЉЂСЂР¶Р°РІРµРЅ РІРµСЃС‚РЅРёРє, РїРѕСЂСЂРёРІРёР»РЅРёС†Рё РїРѕ РїСЂРёР»Р°РіР°РЅРµ. (2017). Lex.Bg. https://www.lex.bg/laws/ldoc/1589654529

P. (2020). *Why is Data Protection Important?* PECB. https://pecb.com/article/why-is-data-protection-important

S, G. Cyberstalking: Prevention, Consequences, and Coping. (2021, August 17). Verywell Mind. https://www.verywellmind.com/what-is-cyberstalking-5181466

Safety and security. (2018). Twitter. https://help.twitter.com/en/safety-and-security

W, The Dangers of Hacking and What a Hacker. (2020). © Copyright 2004 - 2022 Webroot Inc. All Rights Reserved. https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers

What Is Internet Fraud? Types of Internet Fraud. (2019). Fortinet. https://www.fortinet.com/resources/cyberglossary/internet-fraud

What is personal data? (2018, August 1). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

What Is Phishing? (2022, May 5). Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#%7Ehow-phishing-works

Wilkey Oh, E. (2020, March 15). *Teachers' Essential Guide to Cyberbullying Prevention*. Common Sense Education. https://www.commonsense.org/education/articles/teachers-essential-guide-to-cyberbullying-prevention

Ф. (2009). *Киберсигурност*. Фондация. https://www.netlaw.bg/bg/a/kiber-sigurnost


www.digit-safe.com
info@digit-safe.com