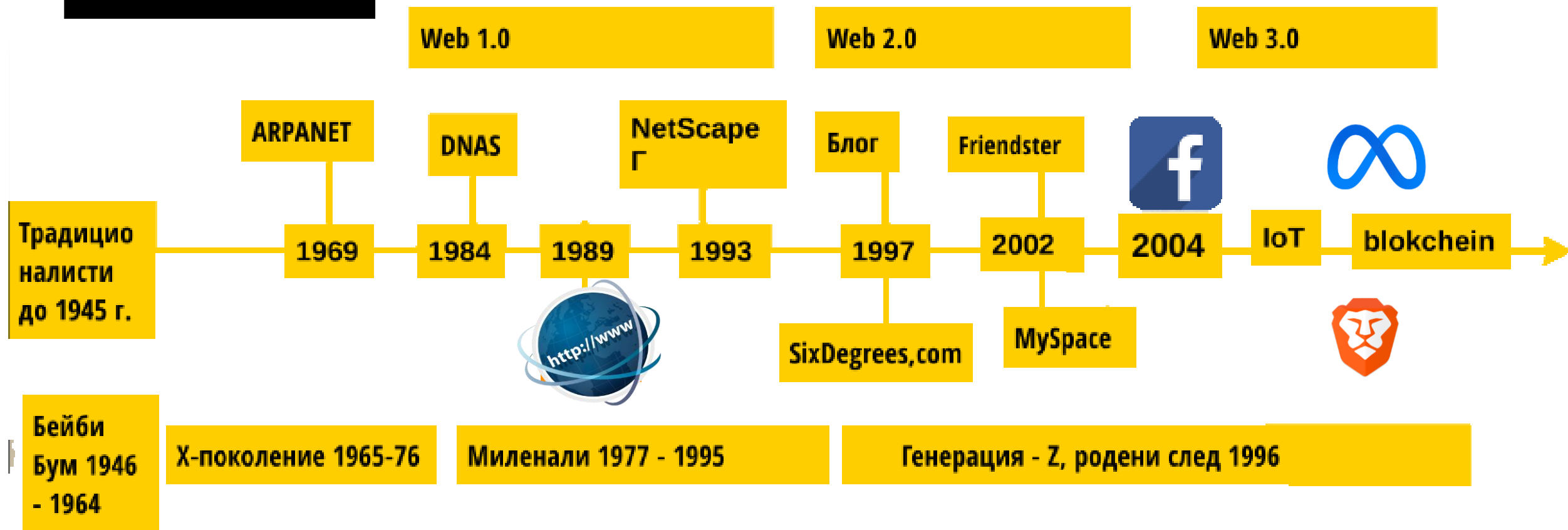


Сигурност в социалните медии

Петко Димов



Интернет



Социални медии – класификация

- 1. съвместни проекти (Wikipedia);**
- 2. блогове и микроблогове (LiveJournal, Blogger, LiveInternet, Diary);**
- 3. общности според съдържанието (Форуми, Подкастове и др.);**
- 4. сайтове за социални мрежи (Facebook, LinkedIn);**
- 5. виртуални игрови светове (World of Warcraft);**
- 6. виртуални социални светове (Active Worlds, Second Lif).**

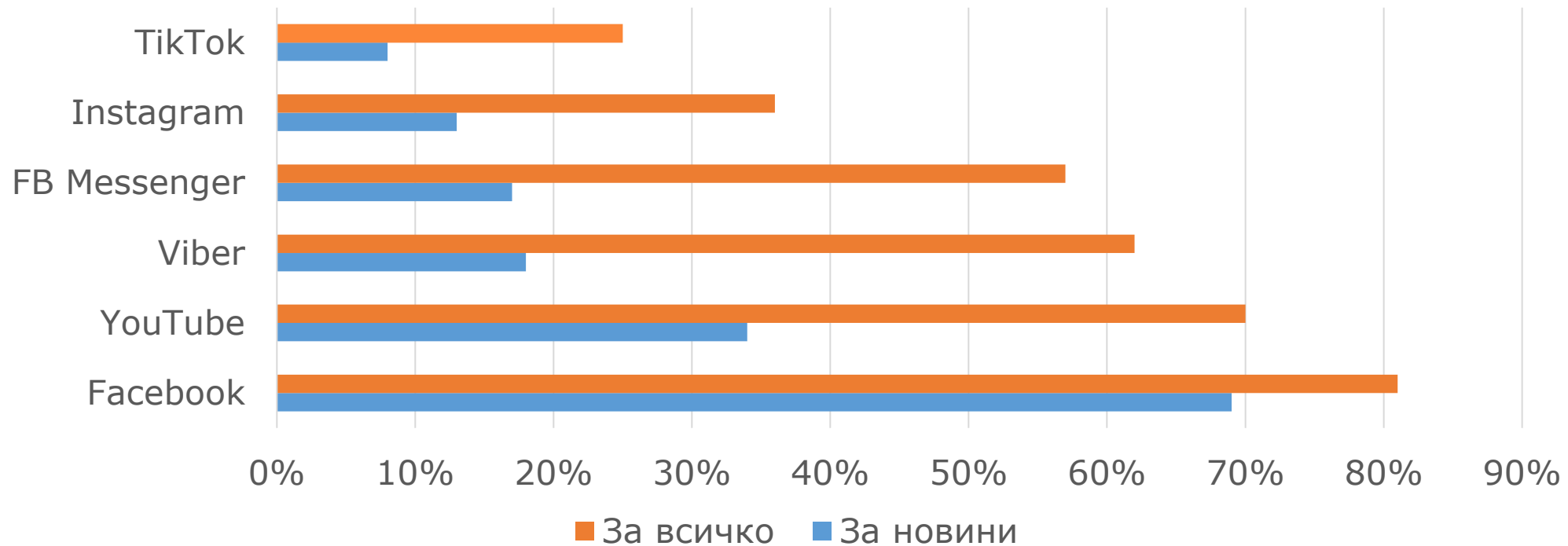
Средният български потребител във FaceBook



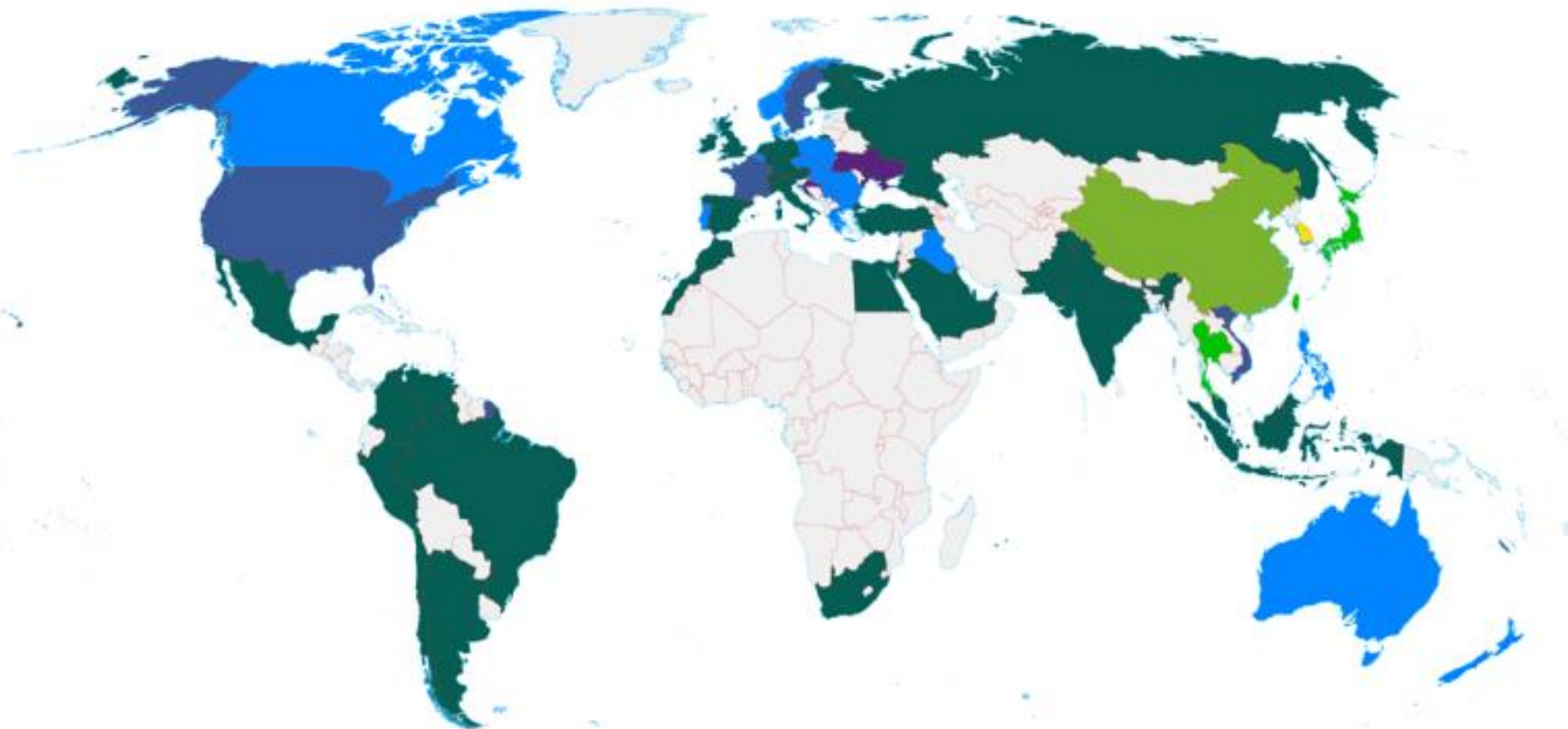
Има 229 приятели:

- от които е виждал само 7%
- 22 % съученици;
- 12 % по-далечни роднини;
- 10 % колеги;
- 9 от университета;
- 2 % съседни;
- 8 % близки приятели;
- 37 % други.

Доверие в социалните медии на България



[Източник: Reuters Институт за изследване на журналистиката 2022 \(ox.ac.uk\)](#)



Источник:
SimilarWeb и
Vincos.it

- | | | |
|--|---|---|
|  WhatsApp |  Facebook Messenger |  Line |
|  Facebook |  Viber |  WeChat |
| | |  KakaoTalk |

Информационно пространство



Хакери

Кракери

Фийкъри

Спамъри

Тролове

Прости и сложни тролове

1. Клонирание

2. Стоварване на десант

3. Плувки, куки и мрежи

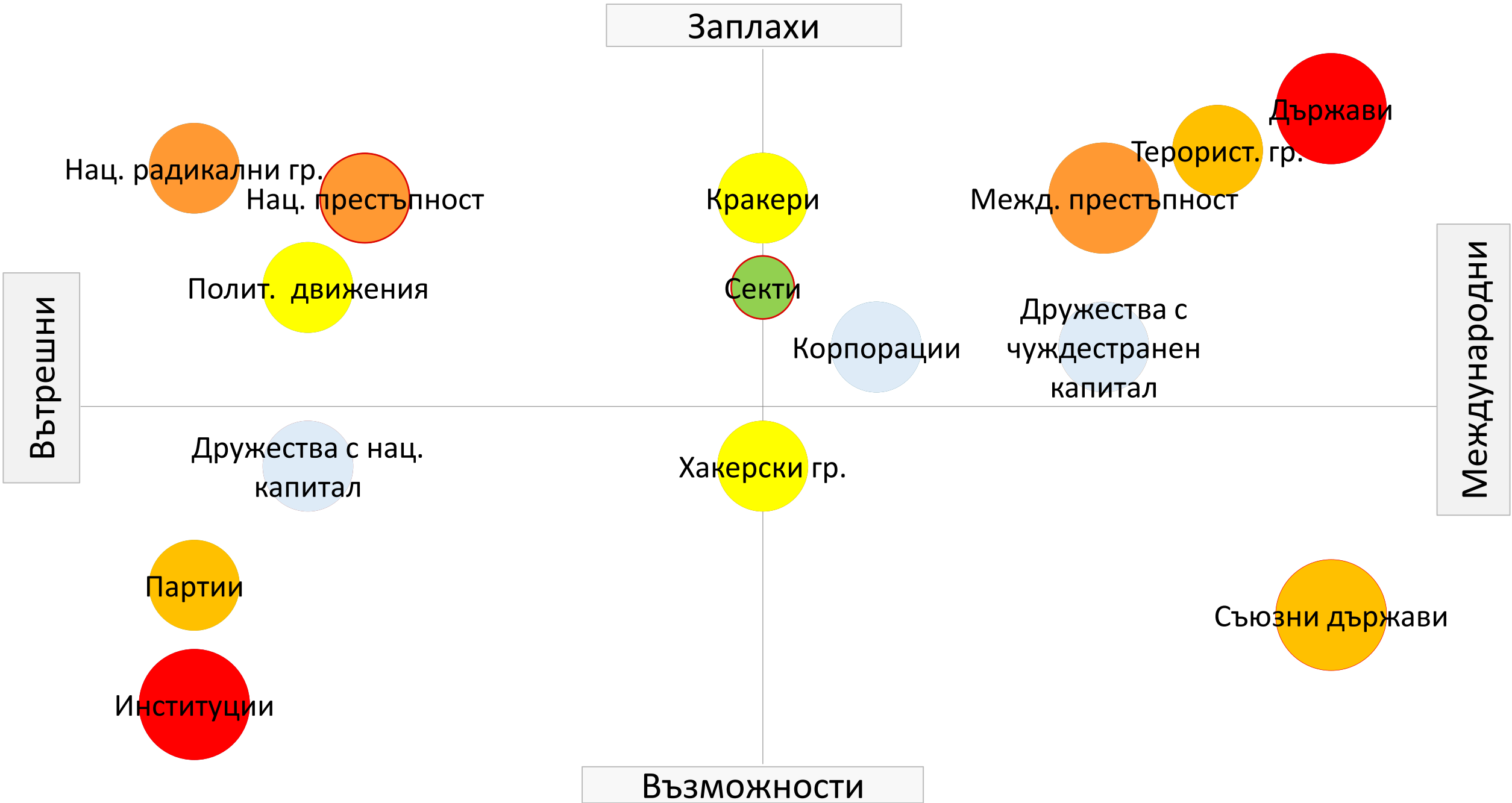
4. Потъване

5. Засада

Човек,
който публикува
провокативни коментари по
дадена тема с цел да смуги автора
или да разстрои
нормалната дискусия в даден
форум, като насочи темата в
определена посока.

[Наръчник за Интернет тролове!](#)

Источници на заплахи и възможности за националната сигурност

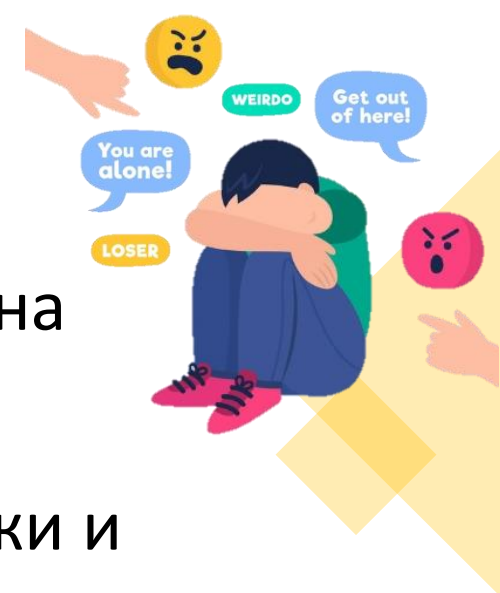


Най-често срещаните престъпления в социалните медии



1. Изнудване, киберпреследване и кибертормоз;
2. Фалшиви профили, кражба на идентичност и лични данни;
3. Фалшиви подаръци, онлайн измами и пирамидални схеми;
4. Фишинг и спам;
5. Корпоративен шпионаж и социално инженерство;
6. Кибератаки и пробиви от автоматично изпълними програми или вируси;
7. Фалшиви новини, дезинформация или изтичане на чувствителна информация.

Изнудване, киберпреследване и кибертормоз



Изнудване – Рансъмуеър или заплаха за разкриване на лична информация ако не платите.

Как да го избегнете? – Не кликайте върху съмнителни връзки и прикачени файлове .exe , .vbs, .scr, антивирусна и редовно архивиране.

Кибертормоз са съобщения, че притежават ваша снимка, която ви злепоставя, най-често с цел изнудване за пари или по други причини: лични, политически, психически нестабилни хора и др.

Киберпреследване с цел публично унижение и вреда на репутацията.

Как да реагираме? - Споделяне с роднина, близък приятел и запазете съобщенията със скрийншот; блокиране; докладване в социалната мрежа. Подаване на сигнал в полицията <https://www.cybercrime.bg/>

Фалшиви профили, кражба на идентичност и лични данни

Хакер с достъп до личната информация може да отвори акаунт за телефон или **хакнат профил** на друг човек за да планира престъпна дейност и да изиска облаги от негово име. Най-често извлича лична информация от медии или фишинг имейли водещи към копие на легитимен сайт. С кражба на идентичност може да направи **фалшив акаунт**, който изглежда като Илън Мъск и да предлага удвояване на биткойни! Често се представя като познат, които иска пари за финансов проблем. Те са двойници на аналоговите измами: включване в бизнес, уреждане на работа, евтини билети, спечелване от лотарията, почивки и др. за които се иска такса участие или лични данни.

Съвети за избягване;

- Добавете в любими;
- проверявайте УРЛ;
- Вижте колко последователи има човека;
- <https://phishingquiz.withgoogle.com/>¹³



Online измами (Scams), фалшиви подаръци, пирамидални схеми

Обещават големи приходи, като изпращат средства от новите на старите потребители

- реклами или спам имейли, които включват обещания за награди или оферти за нереални суми пари.
- щракването върху тях може да доведе до намеса на злонамерен софтуер и компрометиране на информация.



Phishing - Стръв за кълвене

Съобщение, което твърди, че идва от законна компания, например от вашата банка.

За какво да следим?

- адрес на електронна поща – не съвпадащ с адрес на конкретната банка или компания;
- логото е размазано, правописни грешки;
- прикачени файлове;
- URL адреси;
- често не се хващат като спам;
- потребителите са подмамани в имейли, твърдейки, че трябва да променят паролата си или да актуализират данните си за плащане, давайки достъп на престъпниците.



Корпоративен шпионаж и социално инженерство

Vishing вместо **Phishing** -
включва директен контакт
обикновено по телефон или
имейл.



Кибератаки и пробиви от автоматично изпълними програми § вируси

Какво може да направи един вирус?

- да запише аудио от микрофона?
- да запише видео от камерата?
- да събере информация от SIM картата и от мрежата ви?
- да намери локацията ви по GPS?
- да извади паролите ви съхранени върху устройството?



Софтуер копиращ данни - отвлича данните които сте копирали и поставили

Противодействие:

- антивирусни; защитете вашите устройства, браузъри и използвайте само доверен софтуер.

Рискове от споделяне на лични данни във Facebook

- [Настройки и поверителност](#)
- [Настройки за сигурност](#)
- [Проверка на поверителността](#)

За себе си

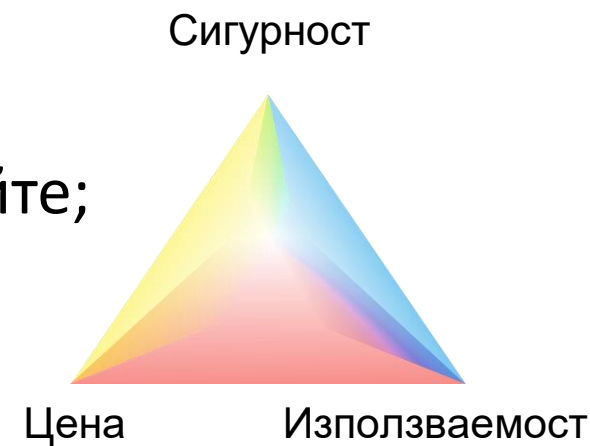
- Лични данни: ЕГН, адрес и т.н.;
- Снимки от ценни предмети в къщата, разположението в къщата, информация за времето, в което ви няма у дома;
- Снимки, които могат да бъдат използвани срещу нас;
- Снимки на деца и близки;

За другите

- Снимки, които могат да ги застрашат или поставят в унизително положение;
- Снимки от инциденти, които показват жертвите в близък план;
- Лични данни, до които имаме достъп;
- Съдържание, което е публикувано със статус приятели;
- Авторско съдържание без да посочваме автора.

Общи съвети за **дигитална сигурност**

- Силни различни пароли, които не се съхраняват в браузъра;
Двуфакторно удостоверяване (2FA) - [Google Authenticator](#);
- Внимание към приложения на трети страни, подозрителни връзки и проверявайте дали сте в оригиналния сайт;
- Гледайте разширението на прикачените файл изпратен от непознат;
- Ограничете споделянето на лична информация и архивирайте;
- Заклучване на елементи от акаунта, настройки за поверителност;
- Контрол върху снимките, тагванията;
- Избягване на незащитени публични мрежи;
- Докладвайте спама;
- Напишете името си в Google и вижте резултата – това, което намерите за себе си, може да бъде намерено от всеки;



Как най-често се компроментират паролите?

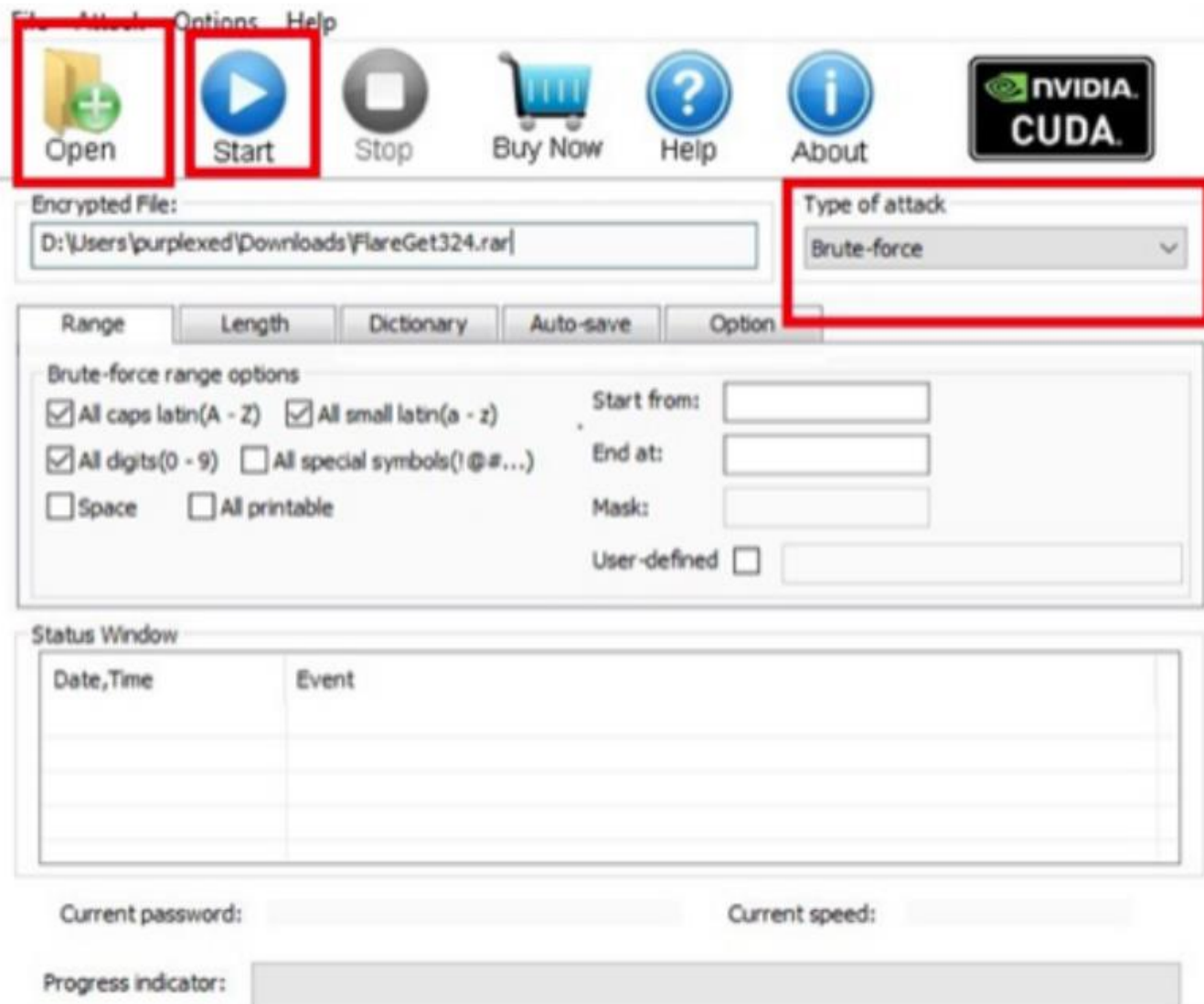
- Когато се споделят с други хора;
- Когато се съхраняват по лесно откриваем начин;
- Когато някой стане свидетел на въвеждане на парола на вашия екран и я запише, снима или запомни;
- Когато се използва имейл клиент без SSL (https) за цялата сесия, а само на страницата за вход, това оставя паролите и друга информация уязвима, тъй като те са видими от всеки, който има достъп до връзката след влизане;
- Когато достъпът до физическото ви устройство е отворен и паролите могат да се получат чрез настройките „Запазване на паролата ми“ или „Запомни ме“, запазени на уебсайтове чрез браузър;
- Зловреден софтуер, като keylogger, който може да документира всяко натискане на клавиш на устройство и да го изпраща на чакаща трета страна;
- Платформите също могат да бъдат хакнати или уязвимостите в техните системи да причинят излагане на информация на техните потребители.

Как изглежда лошата парола?

№	Парола	Бр. хора	Време за пробив	Изложени пъти
1	123456	2 543 285	1 секунда	23 597 311
2	123456789	961450	1 секунда	7 870 644
3	Picture1	371612	3 часа	11 190
4	password	360467	1 секунда	3 759 346
5	12345678	322187	1 секунда	2 944 678
6	111111	230607	1 секунда	3 124 782
7	123123	189004	1 секунда	2 238 979
8	12345	188268	1 секунда	2 389 912
9	1234567890	171124	1 секунда	2 264 487
10	senha	167234	10 секунди	8123

<https://nordpass.com/most-common-passwords-list/>

Как се разбиват паролите?

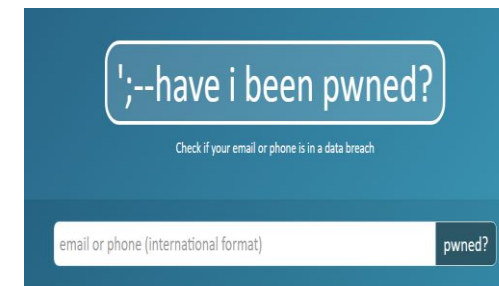


Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %\$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Как да изберем добра парола?

Силната парола има повече от десет знака, няма думи от речника и е комбинация от големи и малки букви, числа и символи. Не използвайте една и съща парола за вашия акаунт за управление на домейна, за вашия хостинг акаунт и администраторски панел.

- Компромитирани <https://haveibeenpwned.com/>
- Проверка на парола www.passwordmeter.com или www.geekwisdom.com/dyn/passwdmeter
- Двухфакторна автентикация
- Използвайте мениджър на пароли (LastPass, KeePass, Dashlane, LogMeOnce, 1Password, [Bitwarden](https://bitwarden.com/));
- Използвайте WOT и/или Ghostery;
- <https://www.mywot.com/>



СТАВАЛИ ЛИ СТЕ СВИДЕТЕЛ НА ОНЛАЙН ИЗМАМИ?

Помислете :

- Кога за последен път сте променили някоя от паролите си?
- Имате ли различни пароли за различните си акаунти?
- Пазете ли паролите, написани на бележка до компютъра?
- Съхранявате ли всичките си пароли на документ?
- Вашите телефони имат ли парола?
- Какво може да се случи ако паролата ви е компрометирана?
- Какво прави възможно едно киберпрестъпление?
- Какви са уязвимостите?
- Как един човек може да се предпази от това да бъде превърнат в жертва?

Не сте?

Да проверим

- <https://haveibeenpwned.com/>

Каква информация за вас смятате, че се проследява в социалните медии?

1. Уеб сайтовете, които посещавате;
2. Времето на вашата дейност;
3. Ключовите думи, които търсите;
4. Местоположението ви докато браузвате;
5. Вашият IP адрес;
6. С кого взаимодействате;
7. Какво е казано за вас;
8. Какво харесвате или споделяте;
9. Какво пазарувате и колко пари харчите;
10. Къде живеете, колко сте годишен;



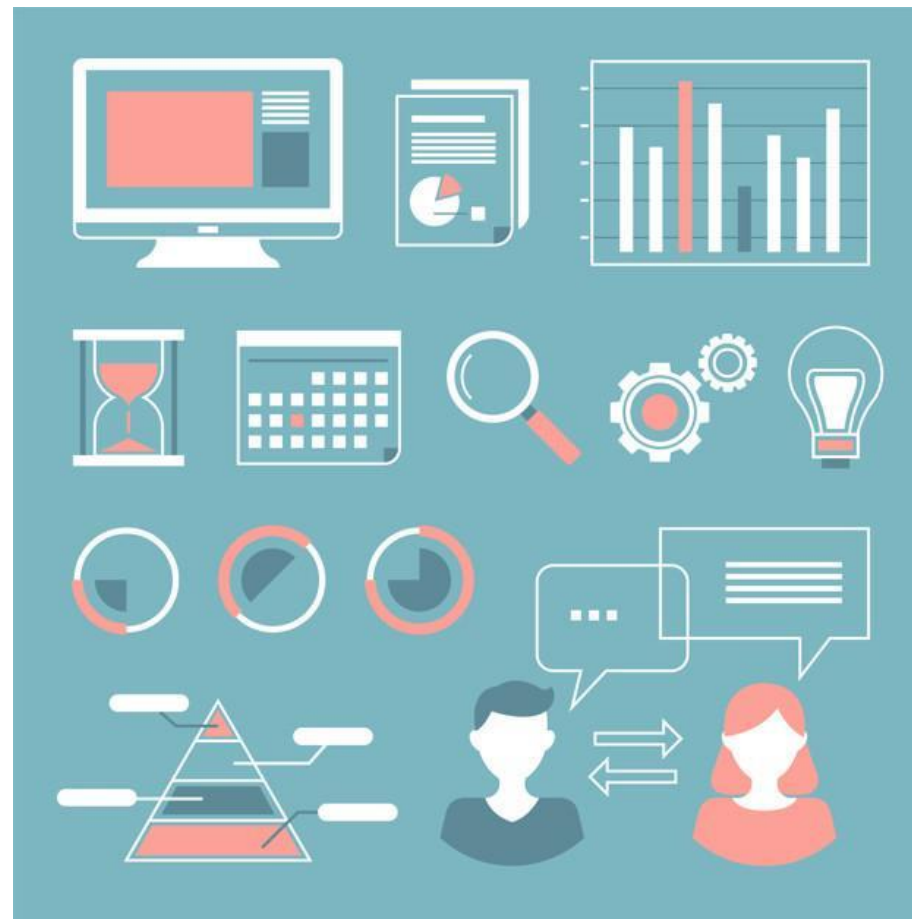
Как се събира информацията?

- Чрез профилът ви в търсачките;
- Браузърите;
- Бисквитки от уебсайтовете;
- Анкетите, които попълвате;
- Информацията, която поствате в социалните мрежи (лична и публична);
- Коментари;
- Покупки;
- Влизане в сайтове /регистрации;
- GPS данни от мобилен телефон
- Утстройства в мрежата(компютри, телефони, камери, IoT);
- Биометрика;
- Държавна администрация;
- Data mining;
- Проследяване на WiFi, сателит и др.



За какво се използват тези данни?

- Маркетинг;
- Социално влияние и политическа пропаганда;
- Онлайн репутация;
- Поведенческа икономика и препоръчани реклами;
- Имейли и други дигитални стратегии;
- Инвазивни атаки срещу личната ви неприкосновеност;
- Хакване, Cyber attacks & Malware; Spyware



Каква информация е достъпна за човек, който не е в списъка ви с приятели?

- Вид на профил (публичен/частен);
- Профилно име(истинско/псевдоним, с малко име или с име и фамилия);
- Снимки, ако да - колко (1, малко, много) и на кого (лични, семейство, деца, картинки);
- Информация за работно място;
- Информация за мястоадрес;
- Информация за семейство, обвързаност, роднини;
- Информация за интереси/хобита (харесани книги, филми, музикални групи, други);
- Отбелязвания на местоположение (тагване);
- Данни за контакт (телефон, имейл, друго).

ПЛАН ЗА ДИГИТАЛЕН ДЕТОКС!

- 1) Направете списък на всички ваши социални медии или други публични акаунти;
- 2) Създайте списък с ключови думи или фрази, които могат да бъдат свързани с вашата личност: име, роден град, мястото, където живеете, работа и др.;
- 3) Намерете колко информация има онлайн за вас, като използвате OSINT, не забравяйте да проверите метаданните и EXIF информация на снимките и видеоклиповете, които публикувате, както и помислете за гео маркерите, семейството и приятелите си;
- 4) Напишете всички намерени данни в една табличка на лист хартия и разберете каква информация искате да бъде изтрита;
- 5) Преминете през всеки свой акаунт в социалните медии и проверете настройките за поверителност (privacy settings);
- 6) Вижте дигиталната си сянка myshadow.org;
- 7) Направете заявка за премахване на вашите данни от търсачките и сайтовете, като [Archive.org](https://archive.org) с това [ръководство](#);
- 8) <https://datadetoxkit.org/en/privacy/profile/> и <https://datadetoxkit.org/en/privacy/degooglise/>

Таблица с информационни активи за оценка на риска

Risk Number	Risk Description	Risk Type (Strength or Opportunity)	Type of Risk (Categorise the risk using labels such as Office / Travel / Assets / Online research / Communication / Human Resources etc....)	Likelihood (1 - 5)	Impact (1 - 5)	Risk Rating (Multiply likelihood and impact for score)	Response (You will seek to either reduce/avoid likelihood of threat AND/OR Impact OR increase likelihood AND/OR IMPACT of an opportunity)	Likelihood (1-5)	Impact (1-5)	Residual Risk Rating
R1	Offices are raided at night by criminals	Threats	Office Location	4	5	20	Use Full Disk Encryption on all hard-drives	4	2	8
R2	Leverage high level of IT skills of partner organisation	Opportunity	Human Resources	2	3	6	Create joint training events where exchange our investigative expertise for their IT expertise.	4	3	12
R3	etc...									

Facebook Privacy Settings – настройки за поверителност

Център за безопасност на Facebook <https://www.facebook.com/safety>

Настройки и инструменти за поверителност

Вашата дейност	Кой може да вижда бъдещите ви публикации?	Публично	Редактиране
	Преглед на публикациите ви и местата, където сте отбелязани	Използване на Регистър на дейността	
	Ограничавате ли аудиторията за публикациите, които сте споделили с приятели на приятели или публично?	Ограничаване на стари публикации	
Как могат хората да ви намират и да се свързват с вас	Кой може да ви изпраща покани за приятелство?	Всички	Редактиране
	Кой може да вижда списъка ви с приятели?	Приятели	Редактиране
	Кой може да ви търси по имейл адреса, който сте предоставили?	Всички	Редактиране
	Кой може да ви търси по телефонния номер, който сте предоставили?	Всички	Редактиране
	Искате ли търсачките извън Facebook да имат връзка към профила ви?	Да	Редактиране

- Изключете местоположението;
- Лична информация (телефон, имейл, адрес) – никога с публичен статус;
- Публикациите ви – публични или приятели;
- Преглеждане на публикациите, в които сте отбелязани преди да се появят в дневника ви и на отбелязванията, които други правят в публикациите ви, преди да се появят във Фейсбук.
- Мислете преди да публикувате.
- [Докладване на нередности FB](#)
- [Акаунта ми е хакнат](#)
- Център за безопасност [Instagram](#)

Проверете състоянието на privacy & security settings

Check
Your
Accounts'
Privacy



- Център за безопасност на Google
<https://safety.google/>

- Център за безопасност
на [YouTube](#)

<https://datadetoxkit.org/en/privacy/degooglize/> degooglize your life

security.google.com

Security

Settings and recommendations to help you keep your account secure

We keep your account protected

The Security Checkup gives you personalized recommendations to secure your account



[Get started](#)

Signing in to Google



Password

Last changed Nov 28, 2016



2-Step Verification

☒ On



App passwords

None



Какво е подходящо онлайн поведение?

- Да бъдете учтиви и да не публикувате без разрешение;
- Използвайте настройките за поверителност и кой може да вижда акаунта ви;
- Използвайте внимателно социалното картографиране;
- Не публикувайте лични данни и не отговаряйте на съобщения, които изискват лична информация;
- Защитете устройствата си;
- Различавайте факт от становище;
- Не пишете нищо от гняв, злоба, или след прекаляване с алкохол;
- Не дискриминирайте и не крадете чуждо съдържание;
- Не регистрирайте местата, които посещавате и не разкривайте точното си местоположение;
- Внимавайте със задния фон на изображенията, които публикувате онлайн;
- **Помислете, преди да публикувате онлайн.**

Какво е неподходящо онлайн поведение?

1. Публикуване на неудобни снимки на други хора в социалните медии
2. Публикуване на неподходящи, обидни или болезнени коментари онлайн
3. Публикувайте лична информация онлайн – Ваша или друга
4. Правене на фалшиви самоличности
5. Извличане или изтегляне на съдържание безотговорно
6. Разпространяване на слухове и публикуване на лични истории за други онлайн

ORM = мониторинг+ контрол+ анализ+ защита на репутацията.

Как да реагираме при различните коментари?

- Положителен коментар + Невярна информация = Отговор
- Положителен + Верен = Слушане или Отговор
- Негативен коментар + Шега или Поучаване= Слушане
- Негативен + Без Шега + Неверен = Отговор
- Негативен + Без шега + Верен + Нещастие или вреда = Отговор
- Негативно + Без шега + Верен + без нещастие = Слушане

Справяне с отрицателни отзиви ->>

Отговорете публично, честно,
конструктивно и подкрепящо.
Използвайте хумор.

Защитете устройствата си

Лаптоп:

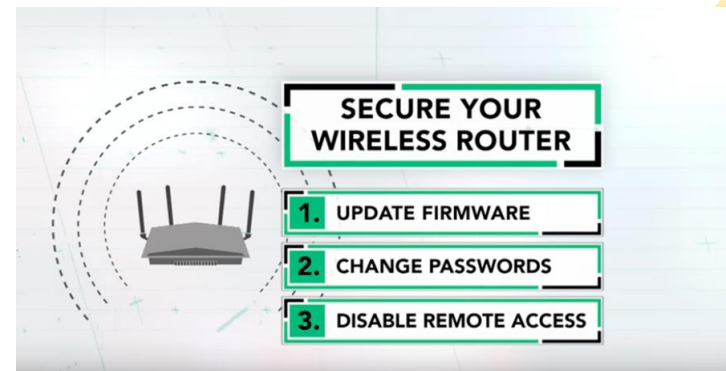
- Използвайте парола, за да го заключите когато ви няма.
- Не оставяйте компютъра / телефона си без надзор от вас.
- Запушете уеб камерата си със стикер.
- Унищожете стари данни.
- Не свързвайте не проверени USB към вашия компютър.
- редовен back-up+archive на чувствителни данни (записани видео или аудио, бележки за интервю, доклади и др.)
- Резервните копия - криптирани и отделно от устройствата.

Телефон:

- Поддържайте операционната система актуална
- Активирайте функцията "намери моя телефон"
- Използвайте парола за заключване и 2FA
- Редовно променяйте паролите си за iCloud и iTunes
- Избягвайте обществения Wi-Fi
- Купувайте приложения само от Google Play, Icloud, ITunes
- Използвайте VPN

• **Update! Update! Update!**

Колко сигурен е вашият WIFI Рутер?



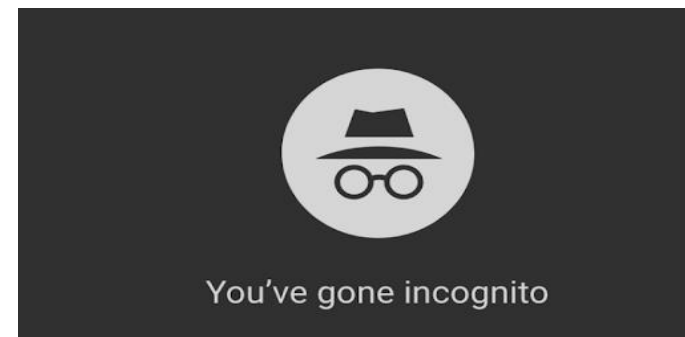
Браузър:

Деактивирайте бисквитите
Инсталирайте си add-ons за по-сигурно браузване

 ProtonMail

 Signal

[Комплект за детоксикация datadetoxkit.org](https://datadetoxkit.org)



Още полезни инструменти

- <https://www.safenet.bg/bg/>
- <https://www.internetmatters.org/>
- Защитете децата си <https://safety.google/families/>
- Проверка сигурността на сайт <https://sitecheck.sucuri.net/> , <https://wpscan.com/wordpress-security-scanner> , <https://www.siteguarding.com/en/sitecheck> , <https://observatory.mozilla.org/> , <https://www.virustotal.com/gui/home/upload>
- Проверете дали не са ви компрометирали email <https://haveibeenpwned.com/> и лични данни <https://www.f-secure.com/en/home/free-tools/identity-theft-checker>
- Сърфирай сигурно <https://1.1.1.1>
- Вижте дигиталната си сянка <https://myshadow.org>
- Комплект със сигурни социални приложения <https://datadetoxkit.org/en/alternative-app-centre/>
- Тест, дали разпознавате фишинг <https://phishingquiz.withgoogle.com/>
- <https://datadetoxkit.org/en/privacy/profile/>
- Подай сигнал [ДЗАД](#)

За въпроси и
предложения



petkodimoff@gmail.com

Postvai.COM

