Споделяй отговорно

борба с дезинформацията чрез медийна грамотност

GLOBAL LIBRARIES - BULGARIA FOUNDATION

Сигурност онлайн

Цели и очаквани резултати

- Познавам рисковете за сигурността ми онлайн
- Знам как да защитавам личните си данни в социалните мрежи

- Знам моите права като медиен потребител
- Знам какво мога да направя, за да бъда отговорен потребител на социалните мрежи

Какви са рисковете онлайн

- Контакт с неподходящи хора
- Риск от онлайн тормоз
- Излагане на неподходящо съдържание
- Фалшиви профили
- Зловредни приложения и измами
- Увредена онлайн репутация
- "Потъване" във виртуалния свят за сметка на реалния - развиване на зависимости

Данни от онлайн проучване на Национален център за безопасен интернет

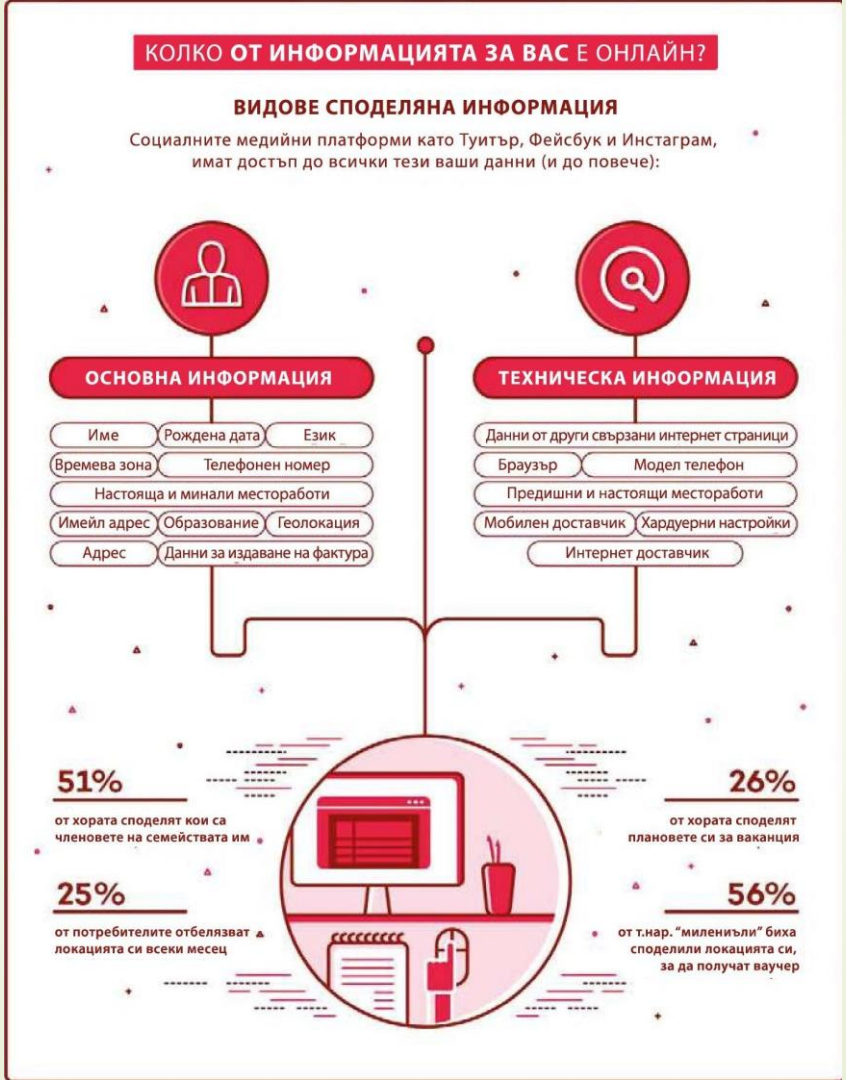
- Онлайн насилието: водеща заплаха сред децата онлайн
- В онлайн проучване на Центъра сред 213 деца на възраст между 12-18 години 84% споделят, че им се е случвала да бъдат обидени, засрамени или унижени в Интернет. В 87% от случаите децата смятат, че извършителят го е направил за забавление. Най-използвани средства: Фейсбук и Скайп
- Изразяването на враждебност, омраза, унижаването на другия, агресията и обидата са неразделна част от онлайн поведението на младежите
- Вредно и незаконно съдържание в Интернет
- Детска порнография, порнография, расизъм и ксенофобия: 751 постъпили сигнала към web112.net от началото на 2011 г.
- **НО:** Висока търпимост сред децата, незначителен процент споделят, че са били притеснени от такова съдържание (изследване „Децата на ЕС онлайн“, 2010 г.).
- Подмамване на дете с цел сексуална злоупотреба (grooming)

Съвети за защита на личните данни в социалните мрежи

- Използвайте сложни пароли и никога не използвайте една и съща парола за профилите си в различни платформи.
- Не използвайте социални мрежи на публични устройства, например на училищните компютри, а ако много ви се наложи – не забравяйте да излезете от профила си.
- Не разрешавайте на мобилните си приложения достъп до вашата геолокация.
- Бъдете нащрек, когато следвате линкове, споделени от ваши приятели в социалните мрежи – те може да съдържат вируси или да са хакнати.
- Използвайте система за двойна идентификация или редовно сменяйте паролите на всичките си профили онлайн.

Съвети за защита на личните данни в социалните мрежи

- Дори и в личните си профили в социалните мрежи, споделяйте минимално количество лична информация.
- Замисляйте се кой може да чете публикациите ви.
- Избягвайте да попълвате твърде много от полетата за лична информация в профилите ви, като град на раждане, рожден ден, членове от семейството, и др.
- Споделяйте внимателно информация за пътуванията си.


КОЛКО ОТ ИНФОРМАЦИЯТА ЗА ВАС Е ОНЛАЙН?
ВИДОВЕ СПОДЕЛЯНА ИНФОРМАЦИЯ
Социалните медийни платформи като Туитър, Фейсбук и Инстаграм, имат достъп до всички тези ваши данни (и до повече):
ОСНОВНА ИНФОРМАЦИЯ
Име
Рождена дата
Език
Времева зона
Телефонен номер
Настояща и минали месторабoти
Имейл адрес
Образование
Геолокация
Адрес
Данни за издаване на фактура
ТЕХНИЧЕСКА ИНФОРМАЦИЯ
Данни от други свързани интернет страници
Браузър
Модел телефон
Предишни и настоящи месторабoти
Мобилен доставчик
Хардуерни настройки
Интернет доставчик
51%
от хората споделят кои са членовете на семействата им
25%
от потребителите отбелязват локацията си всеки месец
26%
от хората споделят плановете си за ваканция
56%
от т.нар. "милениъли" биха споделили локацията си, за да получат ваучер

Групова работа с казуси

- Разделете класа на 4 групи
- Стъпка 1 Всеки екип получава казус, който трябва да обсъди
- Стъпка 2 Екипите Всяка група трябва да определи какъв тип лична информация е била разкрита, как това може да повлияе на засегнатата страна и как това е можело да бъде предотвратено.
- Стъпка 3 Екипите публикуват анализа на казуса си в padlet чрез сканиране на QR кода

Казус 1

- Млада учителка забравя отключено устройството си на бюрото в класната стая. Без нейно разрешение, ученик разглежда снимките, избира една с личен характер и я показва на своите съученици, а след това я публикува в социалните мрежи.

Казус 2

- След като се разделя с приятеля си, млада жена разбира, че той е успял да влезе в личния й профил в Инстаграм, публикувайки лични съобщения и информация, свързани с връзката им. Също така, той е сменил паролата й за достъп, така че тя да не може повече да влезе в него и я обвинява, че сама е публикувала информацията.

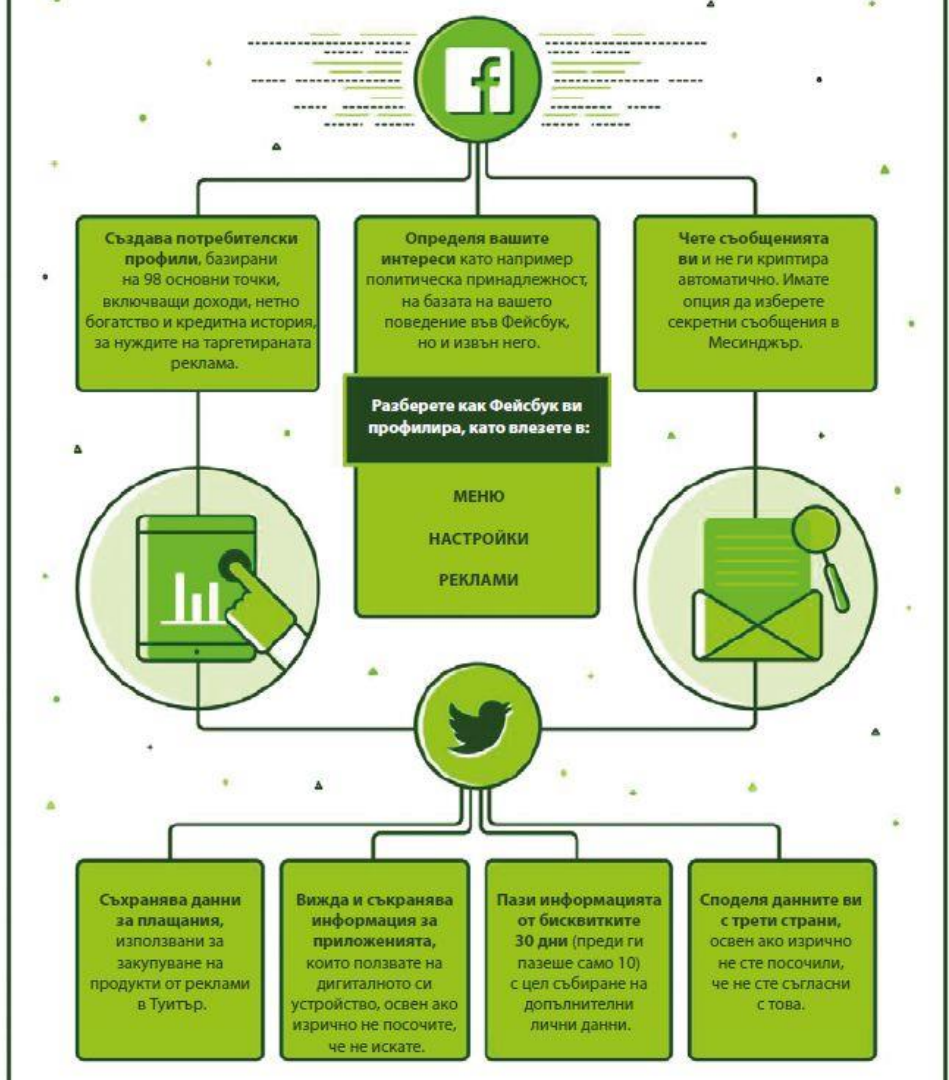
Казус 3

- Семейство отива на почивка и дъщерята пуска снимки на всички от плажа в профила си във Фейсбук. Телефонът й автоматично отбелязва локацията. Когато семейството се прибира след седмица, разбира, че домът му е бил ограбен. Крадецът е разбрал, че къщата е празна, от публикациите на момичето в социалните мрежи.

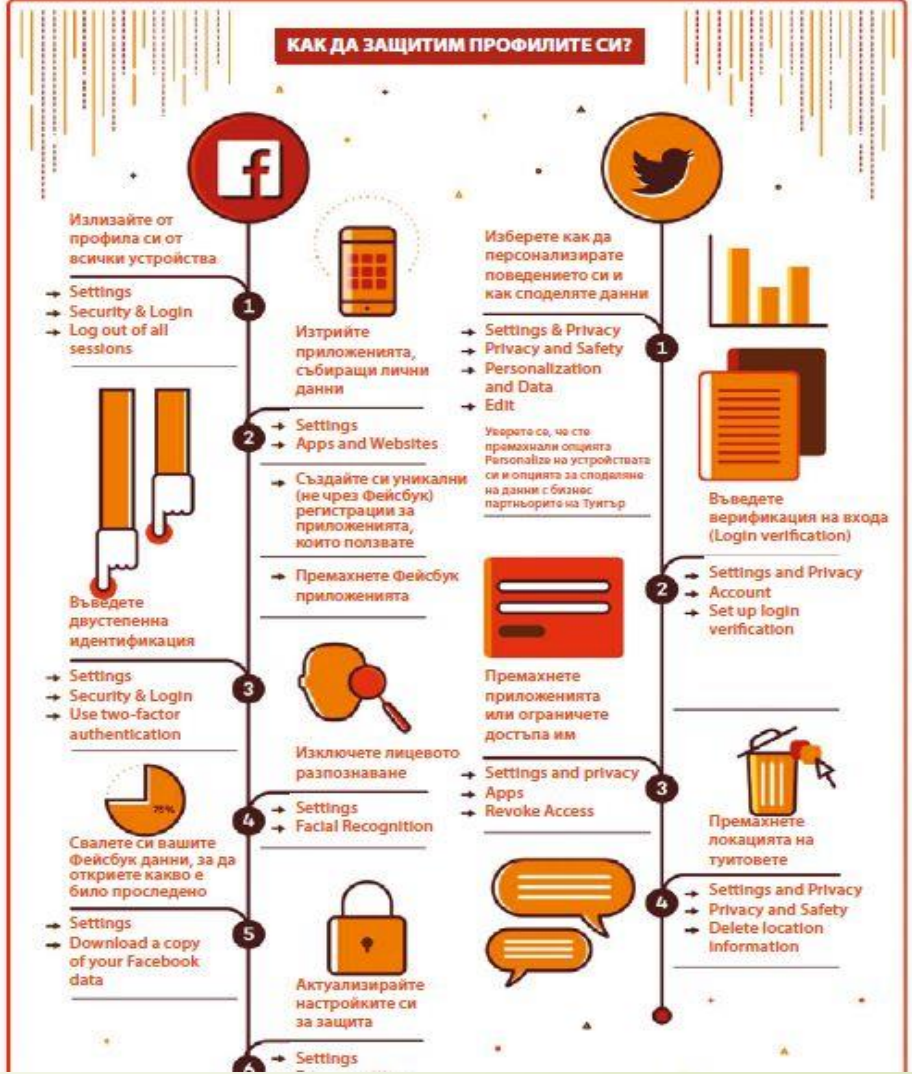
Казус 4

- Известен политик бива заснет с тайната си любовница и снимките излизат в пресата. Журналисти интервюират съпругата на политика във връзка с аферата. Скоро след това, в страната се провеждат избори, които политикът губи.

Моите права като медиен потребител



Как да защитим профилите си?



Благодаря за вниманието!

- Десислава Огнянова
- dognianova@abv.bg

GLOBAL LIBRARIES - BULGARIA FOUNDATION