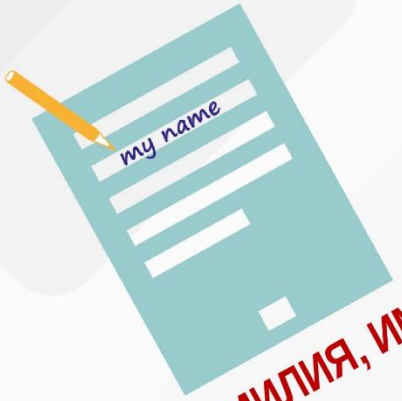
Береги свои персональные данные

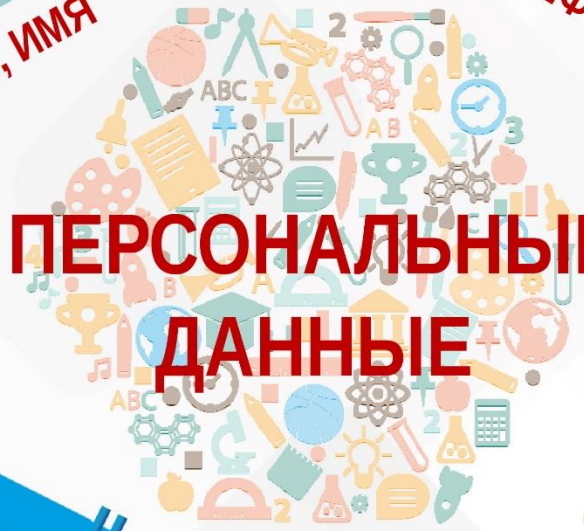
Что такое персональные данные?



ФАМИЛИЯ, ИМЯ

НОМЕР ТЕЛЕФОНА

НОМЕР ШКОЛЫ, КЛАССА



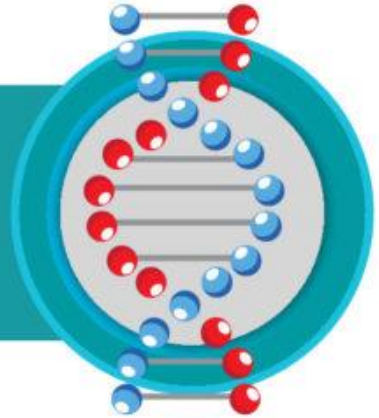
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

ДАТА РОЖДЕНИЯ

ДОМАШНИЙ АДРЕС

БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.



СПЕЦИАЛЬНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты


ПЕРСОНАЛЬНЫЕ ДАННЫЕ
СОСТОЯНИЕ ЗДОРОВЬЯ
120
70
НОМЕР ВАШИХ ДОКУМЕНТОВ
PASSPORT
ФАМИЛИЯ, ИМЯ,
ДАТА РОЖДЕНИЯ,
НОМЕР ТЕЛЕФОНА
ОТПЕЧАТКИ ПАЛЬЦЕВ,
ФОТОГРАФИЯ

Правила защиты персональных данных

Не выкладывай свои фотографии и видео в интернет

Не указывай в Сети, где ты живешь

Не отправляй важную информацию о себе в социальных сетях

Если тебе предлагает встретиться виртуальный друг – посоветуйся с родителями

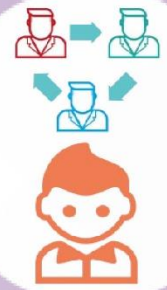
Ограничь доступ к своему профилю в социальной сети

Хорошо, если у тебя есть вторая электронная почта

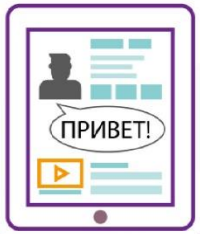
для игр и развлечений

Не ставь геолокацию под своими постами

Не скачивай приложения с непроверенных сайтов



Не рассказывай, когда и куда ездишь с родителями отдыхать



Не знакомься в интернете

Если не соблюдать эти правила

Основные угрозы безопасности детей в Интернете

Киберхулиганы

И дети, и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей.

Злоупотребление общим доступом к файлам

Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ.

Неприличный контент

Если дети используют Интернет без присмотра, они могут столкнуться с изображениями или информацией, от которой их желательно оградить.

Хищники

Эти люди используют Интернет для того, чтобы заманить детей на личную встречу.

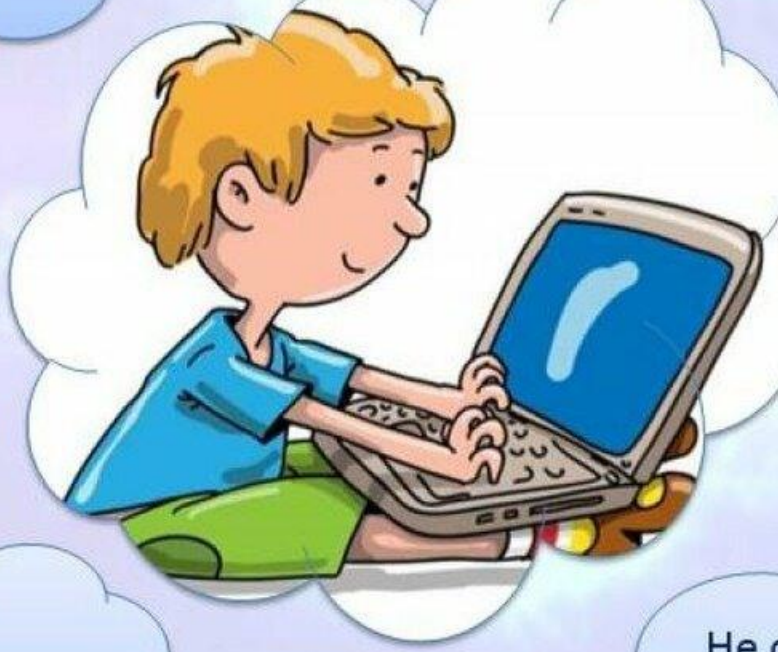
Вторжение в частную жизнь

Заполняя различные формы в Интернете, дети могут оставить конфиденциальные сведения о себе или свой семье.

Правила безопасности в сети Интернет

Не рассказывать о себе и друзьях незнакомым людям в сети Интернет

Не встречаться со знакомыми из сети Интернет без предупреждения родителей



При регистрации придумывать сложный логин и пароль, не говорить их никому

Не отправлять смс для получения доступа к информации без ведома взрослых

Не используй способ разблокировки телефона через ОТПЕЧАТОК ПАЛЬЦА или FACE ID

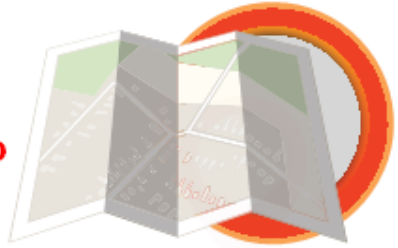
Не играй в игры, при использовании которых нужно разрешить ДОСТУП К ТЕЛЕФОННОЙ КНИГЕ, ГАЛЕРЕЕ, ГЕОЛОКАЦИИ

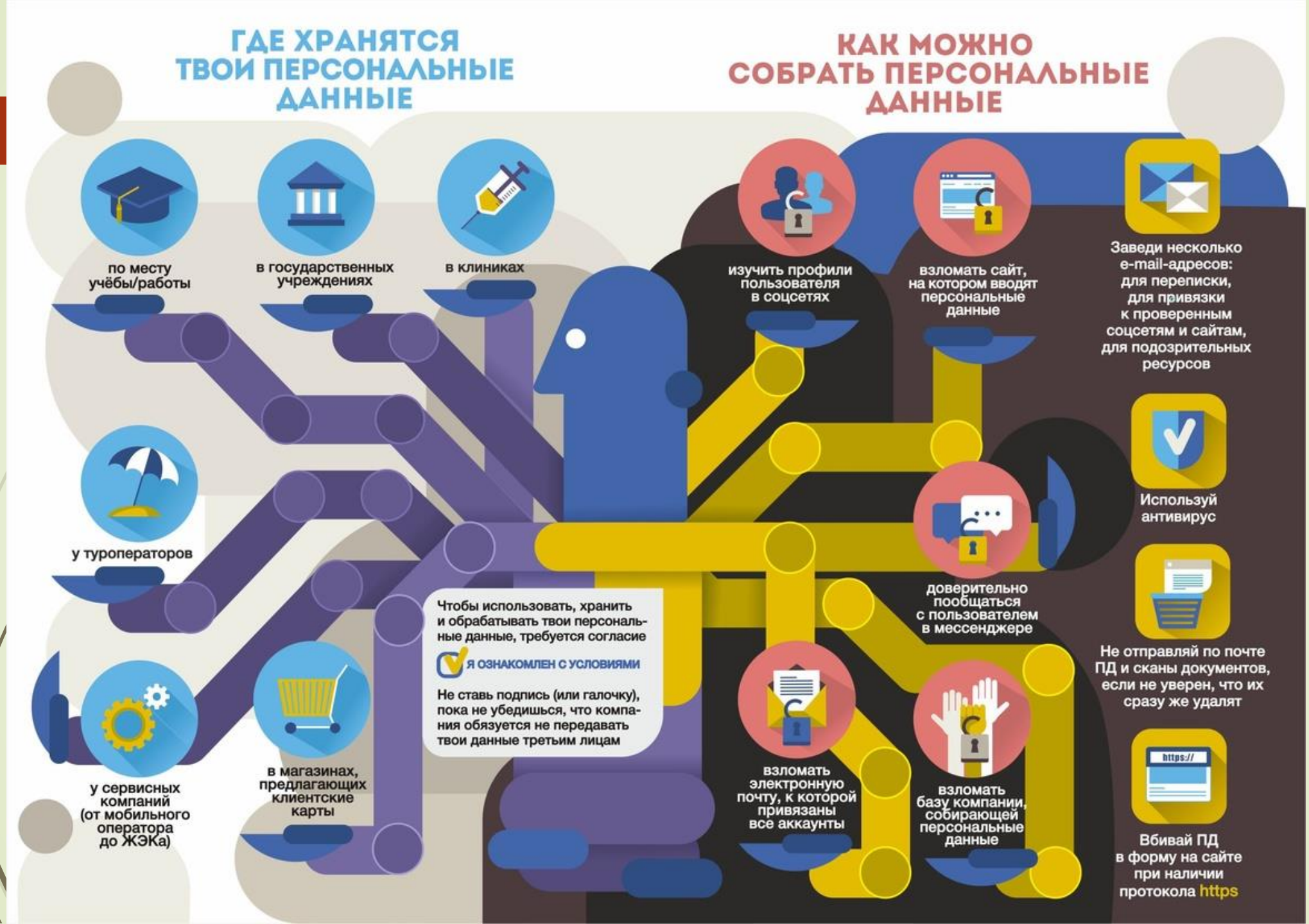
Установи НАСТРОЙКИ ПРИВАТНОСТИ для своего профиля в социальной сети

ЗАПРЕЩАЙ ДОСТУП мобильных приложений к информации, хранящейся в твоем телефоне

Заведи ВТОРОЙ АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ для видеохостингов и т.д.

Если ты прокладывал маршрут при помощи google-карт, не забудь по прибытию в пункт назначения , ОТКЛЮЧИТЬ ПЕРЕДАЧУ ГЕОДАННЫХ в настройках телефона




ГДЕ ХРАНЯТСЯ ТВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ
по месту учёбы/работы
в государственных учреждениях
в клиниках
у туроператоров
у сервисных компаний (от мобильного оператора до ЖЭКа)
в магазинах, предлагающих клиентские карты
Чтобы использовать, хранить и обрабатывать твои персональные данные, требуется согласие
Я ОЗНАКОМЛЕН С УСЛОВИЯМИ
Не ставь подпись (или галочку), пока не убедишься, что компания обязуется не передавать твои данные третьим лицам
КАК МОЖНО СОБРАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ
изучить профили пользователя в соцсетях
взломать сайт, на котором вводят персональные данные
доверительно пообщаться с пользователем в мессенджере
взломать электронную почту, к которой привязаны все аккаунты
взломать базу компании, собирающей персональные данные
Заведи несколько e-mail-адресов: для переписки, для привязки к проверенным соцсетям и сайтам, для подозрительных ресурсов
Используй антивирус
Не отправляй по почте ПД и сканы документов, если не уверен, что их сразу же удалят
https://
Вбивай ПД в форму на сайте при наличии протокола https

ПРОГРАММЫ «РОДИТЕЛЬСКОГО КОНТРОЛЯ»

ЧТО ЭТО ТАКОЕ:

Специальные программы (модули), с помощью которых можно контролировать использование ребенком компьютера и работу в сети интернет.

КОНТЕНТНАЯ ФИЛЬТРАЦИЯ:

Поиск и выявление контента, содержащего нежелательную или опасную информацию, как правило по списку «плохих» и «запрещенных» слов. Далее данная информация корректируется или ресурсы, содержащие такую информацию блокируются.

НЕДОСТАТКИ:

- Необходима отдельная учетная запись для ребенка, иначе ребенок легко отключает программу контроля.
- Родители не всегда могут справиться с настройкой программы.
- Обновление списков всегда «запаздывает».
- Контентная фильтрация требует значительных ресурсов компьютера или быстрого интернет-соединения

Лига безопасного интернета

ВАРИАНТЫ РЕАЛИЗАЦИИ

ФУНКЦИИ

- ОГРАНИЧЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЯ-РЕБЕНКА
- КОНТРОЛЬ ВРЕМЕНИ РАБОТЫ ЗА КОМПЬЮТЕРОМ
- СБОР СТАТИСТИКИ, УВЕДОМЛЕНИЕ РОДИТЕЛЕЙ
- БЕЛЫЕ И ЧЕРНЫЕ СПИСКИ
  - **черные списки:** запрещен доступ к ресурсам по списку
  - **белые списки:** доступ только к тому, что разрешено
- КОНТЕНТНАЯ ФИЛЬТРАЦИЯ
  - фильтрация по ключевым словам
  - фильтрация изображений

Безопасный Интернет

С осторожностью добавляйте незнакомцев в «друзья» и отказывайтесь от личных встреч с людьми, с которыми вы познакомились в Интернете. Обязательно расскажите взрослым и своим друзьям о запросе на такую встречу. Виртуальные друзья могут на самом деле быть не теми, за кого они себя выдают.

Клевета, оскорбление, незаконное копирование продуктов труда других людей и другие противоправные действия, совершенные в виртуальном мире, влекут за собой реальное привлечение к административной, гражданской правовой или даже уголовной ответственности.

Заведите отдельный почтовый адрес для регистрации в социальных сетях, форумах и прочих сервисах - придумайте к нему сложный пароль.

Относитесь с подозрением к сайтам, где запрашивают пароль, адрес, данные паспорта и т.д., просят прислать sms, фотографию, ввести номер телефона.

Если у вас есть вопросы по безопасности в сети Интернет, позвоните на телефон «горячей линии» 8 800 25 000 15

Незнакомые сайты и письма от неизвестных адресатов могут содержать вредоносные программы.

Всё, что вы сообщите о себе в социальных сетях, чатах или форумах, может быть использовано с мошенническими намерениями.

Подумайте прежде, чем разместить фотографии или рассказать о чем-нибудь в онлайн-среде. Фотография, размещенная несколько лет назад, может стать причиной отказа принять вас на работу в будущем.

Оставляйте в сети минимум информации о себе и своих близких, используйте логины и сложные пароли – новые для каждого сайта - чаще их меняйте!

Помните, что в безопасных играх и квестах никогда не предлагается выполнять задания в реальной жизни или в ночное время. Избегайте таких игр.

Если у вас есть вопросы по безопасности в сети Интернет, зайдите на сайт «Дети России онлайн» www.detionline.com