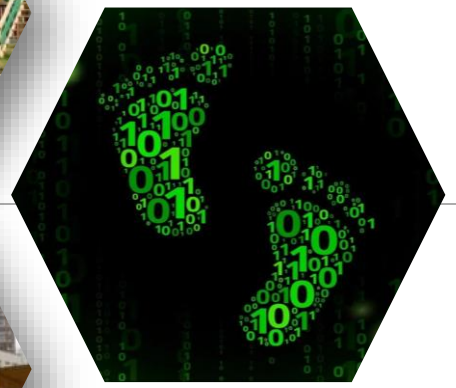
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 35 НЕВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

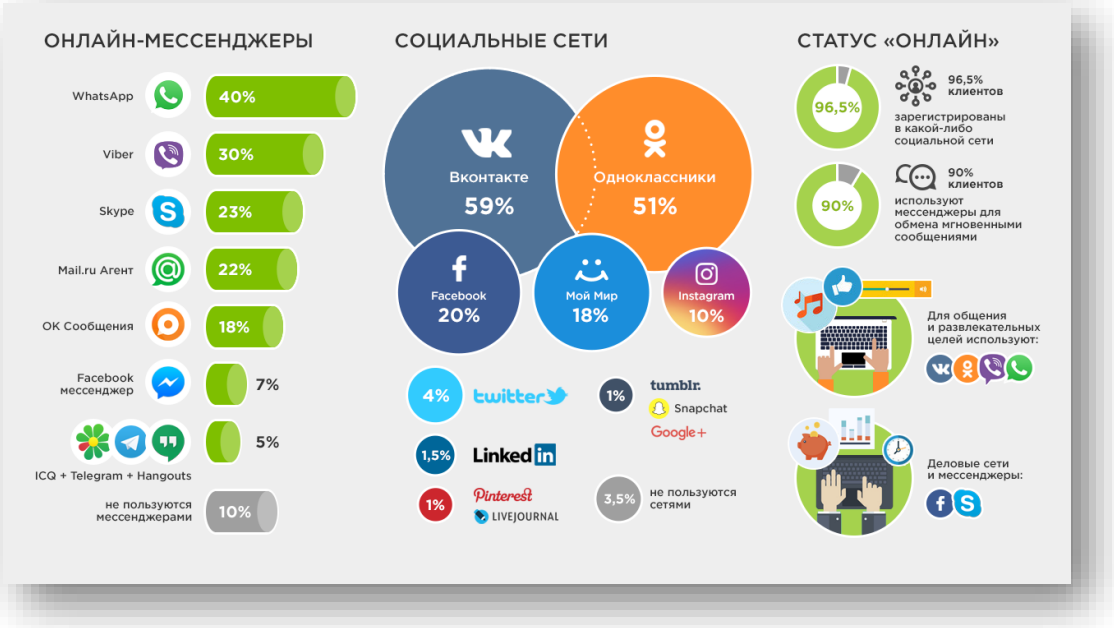
Опасности чрезмерного обмена личной информацией о детях в Интернете



МАТВЕЕВА ТАЛЛИЯ ИЛЬДАРОВНА

ВОСПИТАТЕЛЬ

Цифровой след — это весь массив данных, которые люди оставляют в интернете



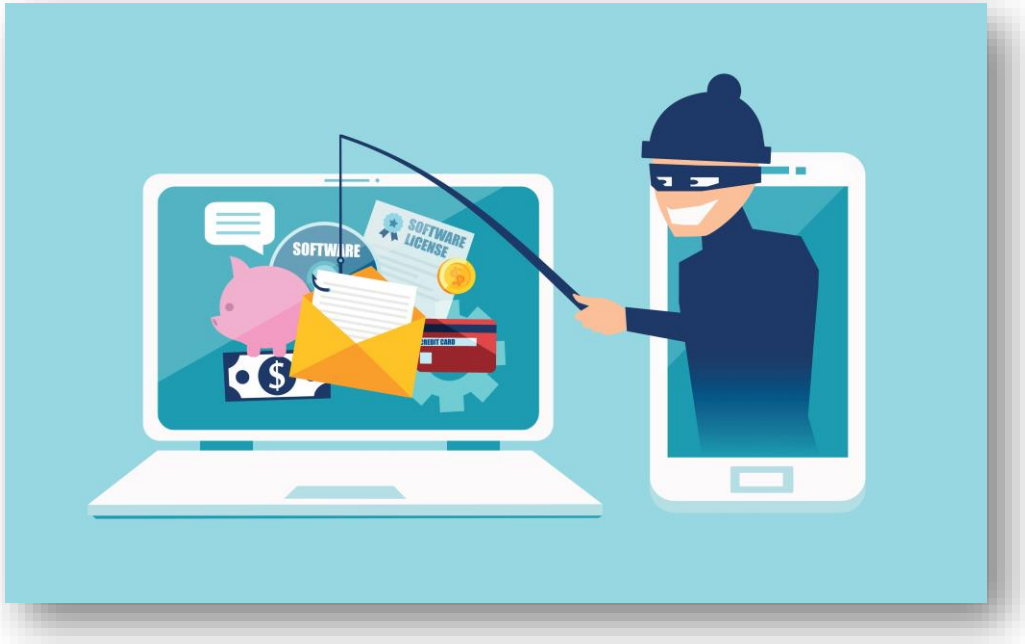
Файлы cookie — это фрагменты данных сайта, на который зашел пользователь. Они помогают лучше понимать поведение пользователей, настраивать предложения под них и оптимизировать бизнес-процессы.

Цифровой след, какой он?

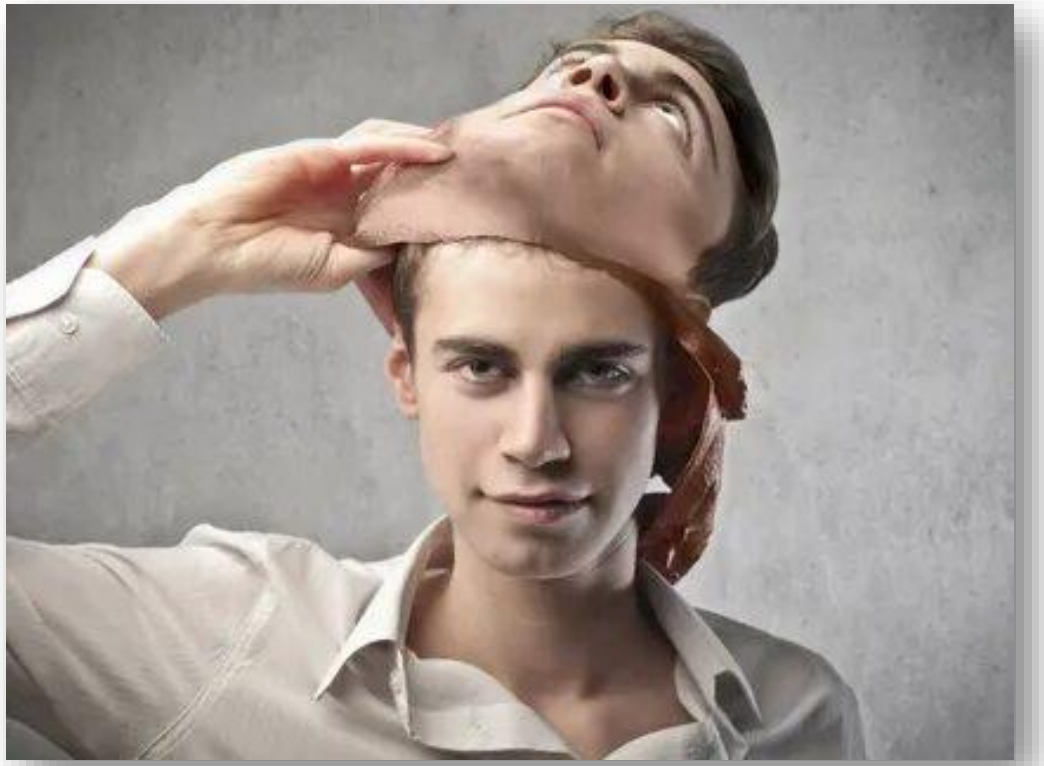
- Покупки: в интернет-магазинах, приложениях, на маркетплейсах и др.
- Банковские операции: получение и переводы денег, оплата кредитов, инвестиции и вклады и др.
- Путешествия и деловые поездки: изменение геолокации, покупки на сайтах железнодорожных и авиакомпаний и др
- Здоровье: сведения в фитнес-приложениях, личные кабинеты на сайтах клиник, электронные медицинские карты и др
- Профили в социальных сетях, отзывы на товары и услуги, сообщения на форумах и др.

Что такое фишинг?

Фишинг-
вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей



Чем опасна кража личных данных?



Из-за хакерских атак на организации, личные данные могут оказаться
у мошенников.
В зависимости от полученных данных (логин, паспортные данные или личные фото) мошенники могут использовать их несколькими способами

Скомпрометировать вас? Легко!

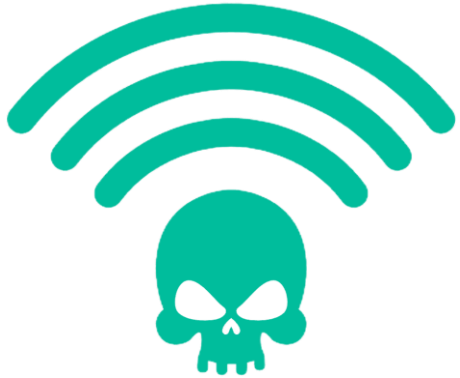
- Оформить на имя жертвы кредит «повесить» долги или оформить фирму-однодневку;
- Совершить незаконные сделки с недвижимостью;
- Подобрать или перехватить пароль от вашего банковского приложения;
- Открыть на ваше имя электронный счет, который впоследствии может быть использован в личных целях

Чем опасна открытая WI-FI сеть?

Ответ: кражей данных

Передача данных через открытую WI-FI точку – это в каком то смысле разговор в полный голос в людном месте!

Пользуясь Интернетом, вы передаете много ценной информации — платежные данные, логины и пароли от всевозможных сервисов, документы и переписку. Если она попадет в руки преступника, он сможет перевести все ваши банковские накопления на свой счет, украсть ваши аккаунты и распространять через них спам или выпрашивать у ваших знакомых деньги.



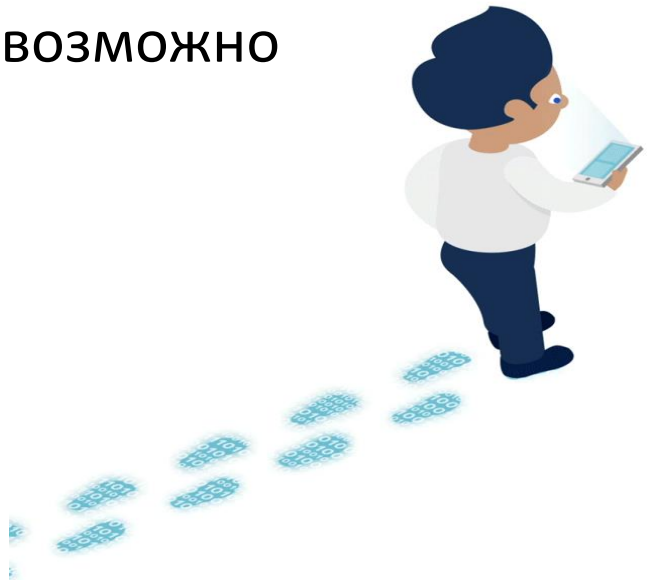
Чем опасно использование VPN ?

При пользовании VPN-сервисами важно понимать, что ты кому-то предоставляешь информацию о себе, и этот кто-то не обещал хранить ее в тайне.

VPN не защищает от хакерских атак, которые приходят извне: фишинговых писем, вредоносных ссылок или звонков мошенников. Получив доступ к устройству, хакеры могут получать любые данные, даже если вы пользуетесь VPN.

Способы защиты при использовании общественного WI-FI :

- Всегда дважды проверяйте имя сети WiFi
- Отключите обмен файлами при подключении к любому общедоступному WiFi
- Включите двухфакторную аутентификацию везде, где это возможно
- Прочитайте условия в общедоступном WiFi
- Не доверяйте никаким бесплатным сетям, на которые вы наткнулись.
- Используйте разные пароли для ваших учетных записей
- Просматривайте только безопасные сайты
- Придерживайтесь веб-сайтов и приложений, которые не раскрывают никакой личной информации
- По завершении использования сети Wi-Fi отключите настройку Wi-Fi на телефоне.



Способы защиты при использовании VPN и обменом личными данными в сети интернет :

- Не стоит обращаться к неизвестному поставщику услуг VPN
- Не оставляйте его включенным на постоянной основе
- Меняйте пароли и избегайте слабых комбинаций
- Не выкладывайте в соцсетях фотографии документо
- Проверяйте личный компьютер на наличие вирусо
- Закройте свои аккаунты в соцсетях