Здравствуйте, я Иванов Михаил и большую часть моего дня я провожу за компьютером. Я занимаюсь программированием, графическим дизайном, видеоредактированием и многим другим, что связано с мониторам.

Просто посмотрите на место, где я каждый день провожу большую часть моего времени!

Как вы можете представить, мне далеко не наплевать на состояние интернета и его пользователей.

Бывало такое, что Фонарик просит доступ к телефону? Или пользовательское соглашение в социальной сети кажется «Войной и миром»? Вы знали, что почти все компании, чьими сайтами вы пользуетесь собирают о вас информацию? А знаете какую?

Я предлагаю поиграть в мою любимую игру – викторину паранойи!

Правила такие - просто поднимите руку, если считаете, что у компании есть определённая информация о своих пользователях. Начнём.

Знает ли Facebook расу своих пользователей? Знает.

Знает ли он уровень доходов? Знает.

А религиозные взгляды?

Что насчёт ВКонтакте? Хранятся ли где-то ваши удалённые сообщения? Да.

А знает ли он где вы живёте? Знает.

А как насчёт того, когда и откуда вы заходили на сайт? Знает!

Последний раунд – Google. Хранится ли информация о всех ваших устройствах? Да.

Когда и что вы открывали на телефоне? Да.

А может быть у них и записи вашего голоса до и после фразы «Окей Google»? Абсолютно.

Все места, где был ваш телефон? Да. Вот примеры моих интересных мест:

Дом дорога дача ярославль аэропорт анапа музей

Возможно после этой маленькой игры вам не по себе, а может даже и страшно.

Такие и многие другие архивы можно запросить у любой компании, которая как либо собирает данные. Так что советую сегодня покопаться в настройках конфиденциальности вашего любимого сайта или приложения и найти такую опцию. А теперь представьте, что кто-нибудь заполучает все эти данные о вас.

Кстати, а как это можно сделать?

У крупных сайтов почти всегда работает эффективная защита от перебора, которую можно обойти, лишь имея очень крупную сеть ботов и растягивая атаку на многие месяцы, так что такой способ неэффективен.

Но есть лучший способ. Фишинг – заполучение пароля используя не настоящую ссылку на сайт, где пользователь «заходит» в свой аккаунт. Таким образом, с точки зрения пользователя ничего страшного не происходит: он вводит пароль и оказывается в своей привычной ленте друзей или в почтовом ящике, но данные для входа оказываются в руках злоумышленников.

А как используются эти так называемые «Большие данные»?

Первое и самое очевидное – целевая реклама.

Целевая реклама это реклама, которая основана на больших данных. Намного вероятнее, что пользователь купит продукт, если этот продукт рекомендуют ему, основываясь на его привычках и действиях. К примеру, если вы изменили свой статус отношений с «не женат» на «помолвлен», вы увидите больше рекламы ювелерии. Профессионалы в сфере рекламы способны манипулировать желаниями определённой целевой аудитории, пока эта аудитория не купит товар. Подобные стратегии могут быть использованы для рекрутизации, скажем, террористов.

Целевая аудитория террористических организаций – молодые люди, иммигранты, бедные люди, прошедшие через утрату любимых. Как раз для поиска таких людей идеально подходят стандартные инструменты целевой рекламы.

Самый главный аргумент за сбор данных это защита от терроризма.

Страх стать жертвой террористической атаки испытывают 65% опрашиваемых, и этот процент растёт.

Так как Россия находится на втором месте по числу погибших в терактах в 1994—2004 годах можно было бы сделать вывод, что терроризм – серьёзная угроза безопасности гражданина. Однако, я представляю информацию, выводы из которой напрашиваются сами. За 2016 год в России:

56 тысяч человек умерли от алкоголя.

23 тысячи человек совершили самоубийство.

21 тысячи человек погибли на транспорте.

8,5 тысяч человек умерли, просто неудачно упав на ровном месте.

В результате терактов за тот же год в России погибли 62 человека.

Как программист могу заверить, что за пол часа можно наладить двухстороннюю связь с математически непреодолимой шифровкой.

И вот мы подошли к самой главной проблеме на сегодняшний день. Так называемые “Пузыри фильтров”.

Пузыри фильтров - негативная сторона персонализированного поиска, явления, при котором веб-сайты определяют, какую информацию пользователь хотел бы увидеть, основываясь на больших данных. В результате веб-сайты показывают только информацию, которая согласуется с прошлыми точками зрения данного пользователя. Илай Парайзер в своей книге «The Filter Bubble» предупреждает, что проблемой фильтрации поисковых запросов является то, что она «закрывает нас от новых идей, предметов и важной информации». Это приносит потенциальный вред как для личности, так и для общества в целом.

Дам пример. В последние пять лет во всём мире были зафиксированы рекордные количества случаев смерти от Кори и Оспы.

19 января 2018 года всемирная организация здоровья назвала «движение против вакцинации» одной из самых больших мировых опасностей на данный момент.

Сейчас в социальных сетях таких как Facebook существует множество групп, в которых пропагандируются (конечно же неправильные) факты об опасностях вакцинации. Пользователи, которые ставят в таких группах лайки, нажимают на ссылки и т.д. попадают в пузырь фильтров, который не показывает им настоящую статистику о вакцинации и рекомендует всё больше пропаганды опасного движения.

Так что мы сегодня узнали?

1. Вся наша информация хранится и обрабатывается большими компавниями
2. Алгоритмы социальных сетей поощряют заключение информации в маленьких кругах людей, что приводит к дизинформации.