Защита персональных данных в социальных сетях

Введение

В современном обществе невозможно обойтись без социальных сетей. В настоящее время каждый человек, связанный с компьютером или с телефоном, зарегистрирован хотя бы в одной социальной сети. Социальные сети притягивают людей, так как в современном мире все люди общаются, обмениваются информацией и знакомятся. Проблема, связанная с утечкой персональных данных, стала одной из самых острых проблем последних лет. Поэтому социальные сети и другие электронные ресурсы постоянно совершенствуют свой функционал, чтобы предотвратить несанкционированный доступ к личным данным и контенту пользователя.

Кто имеет доступ к данным?

У кого же хранятся наши персональные данные, которые мы когда-то решили загрузить в интернет? Прежде всего, это компании, владеющие социальными сетями. В Пользовательском соглашении, которое многие пролистывают, не читая, обычно указано, кто именно имеет доступ к загруженной персональной информации, если она находится в закрытом аккаунте. Как правило, это только соцсеть, которая обязуется хранить и защищать данные, используя их только для «улучшения пользовательского опыта».

Тем не менее, как показал скандал с компанией Cambridge Analytica, в который оказался втянут Facebook, у некоторых социальных сетей предусмотрена специальная возможность для разработчиков сторонних приложений. Так, развлекательное приложение, работающее на базе Facebook и обещающее составить психологический портрет для каждого, кто пройдет тест, сумело завладеть данными почти 90 млн человек по всему миру.

Cambridge Analytica специализировалась на сборе личной информации пользователей интернета, чтобы потом использовать ее в своих целях. Таким же образом работают многие другие компании, в том числе российские.

Какие данные собирают?

Исследовательская компания Clario проанализировала приложения нескольких десятков крупных мировых брендов, чтобы выяснить, какие данные о пользователях они собирают и кто из них, как следствие, больше всего знает о

пользователях. Список собираемых данных получился внушительным. Наряду с электронным и почтовым адресом, именем, возрастом, полом и номером мобильного телефона в него вошли данные о друзьях, домашних животных, данные о весе и росте пользователя, предыдущих местах работы, интересах и увлечениях, религиозных убеждениях и даже об аллергиях. В общей сложности 32 категории.

По объему собираемой информации в абсолютных лидерах — социальные сети. Причем самой всеядной из них оказалась **Facebook**. По данным Clario, Facebook собирает 70,59% персональных данных (за 100% взят весь разрешенный к сбору массив) и из всех вошедших в исследование категорий. Ее не интересуют лишь вес и рост пользователя, девичье имя матери, номер банковского счета и размер зарплаты, а также место рождения и состояние здоровья. Все остальное Facebook использует в первую очередь для таргетированной рекламы.

При этом Facebook собирает личные данные еще и через принадлежащий ей **Instagram**, который в этом списке стоит на втором месте. Причем Instagram как раз и интересны вес и рост пользователя, без которых обходится Facebook. Но дочерний сервис Facebook не хранит у себя информацию из многих других категорий и в целом собирает только 58,82% персональных данных.

На третьем месте расположился сервис знакомств **Tinder**, который собирает 55,88% всей доступной информации о пользователе, чтобы на основе этих данных подобрать идеальный вариант партнера. Tinder хочет знать имя, возраст и пол пользователя, его рост (но не вес), должность, хобби, список друзей, наличие или отсутствие домашних питомцев, а также данные банковского счета, чтобы можно было предложить пользователю платный вариант приложения с большим числом опций.

Кроме того, Tinder хранит всю романтическую переписку пользователей (что отражается на предлагаемой им рекламе) и следит за тем, какими еще социальными сетями они пользуются.

Как отмечают авторы исследования:

- 93% компаний запрашивают и хранят адреса электронной почты пользователей,
- 20% компаний имеют доступ к списку друзей пользователя в социальных сетях,
- 18% компаний известен вес пользователей,
- 16% компаний собирают данные об интересах,

- 10% компаний знают о домашних питомцах пользователей.

Эксперты отмечают, что одна из причин, по которым у соцсетей оказывается столько персональных данных, — сами пользователи, которые позволяют эти данные собирать.

Выгода из данных

Что же происходит с собранными данными, и в каких целях они используются? Главным образом, для настройки таргетированной рекламы. Если рекламодатель будет знать, какой доход у покупателя, где он живет и чем интересуется, ему будет гораздо проще показывать пользователю релевантные объявления, которые с большей долей вероятности его заинтересуют.

Рекламная прибыль — это основная статья доходов крупных компаний, чьи сервисы являются бесплатными, во многом благодаря монетизации платных объявлений.

Есть и те организации, которые зарабатывают на продаже больших массивов данных, включающих в себя телефонные номера.

Я думаю, многие сталкивались с такой ситуацией, что вам звонят из клиники или из образовательных учреждений и предлагают свои услуги.

Защита личной информации

Стоит запомнить некоторые правила, позволяющие сделать жизнь как можно безопаснее:

1. Пароль. Придумывайте как можно более сложный и длинный пароль.
2. Меньше личной информации. В своем профиле пишите как можно меньше о себе, ваших поездках, номерах телефонах и др. В такой социальной сети, как Instagram, пользователи рассказывают о своем распорядке дня, своем местоположении, личной информации о себе и так далее.
3. Фотография. Перед тем как выложить фотографию, внимательно посмотрите на каждую деталь: на свой внешний вид, на окружающую местность, людей, находящихся рядом с вами, и многое другое.
4. Конфиденциальность. Установите параметры конфиденциальности. Незнакомые вам люди не должны видеть важные сведения о вас, которые могут быть расположены на странице.

5. Безопасные браузеры. Используйте только надежные и проверенные браузеры, не забывайте про брандмауэр и антивирусную программу.
6. Никогда не переходите на незнакомые ссылки, которые присылают неизвестные вам люди.
7. Общаясь с друзьями в сетях, будьте внимательны. Их страницы могут быть взломаны
8. Не используйте файлообменные сайты для получения пиратских программ, ведь вместо них может быть вирус.
9. Wi-Fi. Будьте осторожны при использовании Wi-Fi. Обычно почти каждый человек, увидев то, что нашлась бесплатная точка доступа, сразу подключаются к ней. А это может подвергнуть вас опасности.

Подводя итог, можно сказать: социальные сети — это способ всегда быть на связи с друзьями и семьей, но также их можно использовать со злыми намерениями. Поэтому нужно быть более внимательным и ответственным по отношению к себе, осознавать необходимость распространения персональных данных.

https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/

https://nris.ru/blog/zashita-v-socialnyh-setyah/

https://www.kommersant.ru/doc/4556804

https://www.tadviser.ru

https://www.gazeta.ru

https://elar.urfu.ru/bitstream/10995/65634/1/978-5-7996-2404-0_2018-67.pdf