

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

Большой Брат наблюдает за тобой

«Каждый, кто поиграл в FaceApp, на добровольной основе пополнил глобальную базу системы распознавания лиц. Каждый, кто собирал покемонов в Pokemon go, передал фото и видео посещенных территорий. Каждый, кто ведет учет состояния здоровья через мобильные приложения, пополняет биометрическую базу данных для аналитических исследований (а может, и донорскую базу органов). Каждый обладатель мобильного телефона носит с собой радиопередающее устройство, которое сообщает местоположение владельца в реальном времени. Список бесконечный...»

Так написал о тотальном контроле, использующем энтузиазм пользователей соцсетей, один из пользователей Facebook. И, возможно, он был не так уж далек от истины. Конечно, мы не призываем впадать в панику по поводу того, что все мы «под колпаком», но представлять себе возможные последствия виртуальной жизни все же не помешает



Поисковик – находка для шпиона

Наверное, вы и сами не раз замечали такую странность. Набрали в поисковике запрос про стоимость соковыжималки, и тут же какую страницу ни открой – везде в глаза бросается реклама соковыжималок. Зашел в интернет-магазин, торгующий саженцами, и – к гадалке не ходи! – пару недель реклама сельхозтоваров будет преследовать тебя по всей Всемирной паутине.

Объяснение тут простое. Реклама, что вы видели в Сети, ваши запросы, информация относительно ваших покупок, просмотров и оценки товаров в интернет-магазинах собираются и анализируются. А затем на основе сделанных выводов вам предлагаются аналогичные товары в виде рекламных блоков.

Более того, Google не так давно анонсировал интеграцию информации относительно того, какую рекламу пользователь просматривал в Сети и какую покупку совершил в реальном магазине. Даже это отслеживается – пока что в маркетинговых целях.

Собака лает? Получи рекламу корма!

Специалисты уверены, что изучать ваши предпочтения можно даже в том случае, если вы игнорируете поисковики и не бродите по виртуальным магазинам. Мобильные приложения по типу Facebook, Instagram, а

также тысячи мобильных игр из Google Play слушают информацию через микрофон на мобильном устройстве. В них запрограммирован код для распознавания телерекламы и других звуков, которые вас окружают. Даже если игра не запущена, звуки записываются, а статистика для рекламодателей собирается. И вот, поговорив с родственниками о ремонте обуви или покупке пылесоса, вы вдруг видите в Интернете рекламу нужных вещей. Не чудо ли?

Как сообщает Википедия, тревожный знак, обостривший теории о слежке Большого Брата, подала компания Google, получившая в 2012 году патент на «облачную» технологию, которая анализирует шум вокруг говорящего по телефону человека и предлагает рекламу на основе этого. К примеру, услышав музыку, Google предложит купить билеты на концерт; уловив лай собаки, покажет баннер магазина товаров для животных и так далее. Если добавить сюда еще и возможность считывать GPS-координаты, то простор для потенциальных сценариев использования этого механизма просто безграничен.

Ни минуты без присмотра

Есть теория, что некоторые соцсети (и уж точно многие смартфоны) отслеживают местоположение своих пользователей. Зачекинулись в кафе, где обедали, или просто на работе, а вам уже предлагают посетить интересное

место, мероприятие неподалеку.

Возможно, с точки зрения пользователя эта технология и работает во благо, помогая показывать рекламу наиболее востребованных в данный момент товаров или услуг. Однако стоит помнить о том, что распознавание личности человека по голосу аналогично распознаванию по лицу, так что компания в будущем может попробовать выстраивать социальные связи, определяя имена тех, кто в данный момент находится рядом с пользователем и слышен на фоне. А это уже реальный инструмент негласного тотального контроля практически за любым из нас.

В корыстных целях

Навязывание рекламы – не самая большая проблема. Информацию от Большого Брата с успехом используют и мошенники. В последнее время в СМИ часто пишут о звонках от якобы сотрудников банка, которые, оперируя персональными данными человека, пытаются узнать код его банковской карты. Откуда у мошенников эти данные? Конечно, проще всего заподозрить в продажности персонал банка. Но давайте вспомним, не оплачивали ли вы своей картой покупки в Интернете? Ведь в таком случае вы сами сообщили Большому Брату и номер карты, и свои имя-отчество. И если сайт, на котором вы совершали покупки, не вполне надежен или попросту взломан... Сами понима-

ете, какой Клондайк для преступников этот виртуальный мир.

Обезопасить себя

Чтобы обезопасить себя в Сети, просто держать язык за зубами недостаточно. Идеальный вариант – поменять многофункциональный смартфон на кнопочный телефон из 2000-х годов. Это, конечно, нереальная жертва. Но необходимый минимум, пожалуй, можно и нужно соблюдать.

Вот несколько несложных правил:

- Используйте телефон только для разговоров и не скачивайте сомнительные приложения. Не комментируйте, не ставьте лайки и не переходите по рекламным и подозрительным ссылкам.

- Выключайте передачу данных, геолокацию и Интернет, когда завершили поиск нужной информации.

- Помните: никакой тайны переписки сегодня уже не существует. Не сообщайте важную информацию, да и вообще любую, через мессенджеры и чаты.

- Для личной жизни, банковских карт и социальных сетей заведите отдельные телефонные карты.

- Помните: социальные сети – это вымышленный мир, в который нас пытаются затаскать. Ведь в нем очень легко управлять пользователями по своим, четко построенным алгоритмам. Больше общайтесь с реальными людьми и в реальном времени. И – думайте!

Инна НОВИКОВА

ЭТО ИНТЕРЕСНО

Навязчивая слежка за бывшими партнерами в социальных сетях приводит к серьезным психологическим отклонениям

Расставаясь, расставайтесь!

Навязчивое преследование человека носит название «сталкинг». Оно включает в себя нежелательные для жертвы звонки, домогательства или даже запугивания. А популяризация соцсетей серьезно облегчила злоумышленникам задачу слежки за человеком и его увлечениями.

Ученые из университета штата Огайо и Гавайского университета в Маноа провели анкетирование среди 431 активного пользователя Facebook в возрасте от 18 до 42 лет, которые ежедневно проводили около 100 минут в соцсети и пережили недавний разрыв в отношениях. Вопросы касались таких тем, как «вклад в отношения», «поиск альтернатив» и «стресс после расставания». И выяснили, что чем сильнее стресс, создаваемый этими факторами, тем более человек подвержен слежке за бывшим партнером в соцсети, что, в свою очередь, только усугубляет ситуацию. Постоянный стресс и неудовлетворенность влекут за собой психологические расстройства, которые порой выражаются в невозможности начать новые отношения и приводят к депрессии.

Сталкинг во многих случаях не является безобидной забавой. Как правило, у такой слежки есть цель: что-то показать или доказать бывшему партнеру и его окружению. Человек внимательно следит за всеми обновлениями в соцсетях бывшего партнера, активно комментирует друзей бывшего партнера, оставляя записи там, где бывший их точно увидит.

Еще деструктивнее активное участие, когда человек пишет что-то в ответ на публикации бывшего партнера, публикует что-то компрометирующее, выясняет отношения публично и скандалит.

Бывает, что дело доходит до взлома аккаунтов бывшего партнера. Здесь все гораздо сложнее и серьезнее, потому что речь уже идет о нарушении личных границ, вторжении в личную жизнь и даже о правонарушении.

В ряде западных стран особенно активные «сталкеры» числятся и подвергаются административной или даже уголовной ответственности, поскольку у людей есть право на защиту своей частной жизни. В России пока такой практики нет. Тем не менее в МВД уже серьезно озабочены данным вопросом.

Подготовлено с использованием материалов сайта gazeta.ru