# Кто торгует нашими данными

В прошлом году в нашей стране утекли в сеть **около 100 миллионов** записей персональных данных россиян и их платежной информации. Об этом говорится в исследовании компании InfoWatch.

***Чем опасны утечки персональных данных? Мы беседуем с координатором направления интернет-безопасности регионального общественного центра интернет-технологий (РОЦИТ) Урваном Парфентьевым.***

**— Урван Урванович, кто и зачем сливает наши персональные данные?**

— Как правило, сотрудники компаний и финансовых организаций. Например, менеджеры банков и операторы сотовой связи, которые на конфиденциальной информации просто зарабатывают. Кстати, по данным аналитиков InfoWatch, общая доля утечек в стране, связанных с действиями персонала, за год возросла примерно на три четверти.

Простой пример: вы пришли в поликлинику — не важно, платную или муниципальную.

Вам поставили определенный диагноз. И вдруг через какое-то время звонят из другой клиники или медицинского центра — разумеется, частного, и предлагают пройти обследование или полечиться. Причем именно с вашим диагнозом. Они угадали? Нет, просто ваши данные слили конкурентам.

**— Неприятно, но не страшно. Можно заблокировать номер и забыть.**

— Да, но у вас могут и деньги украсть. Простой пример: вы создали в соцсетях страничку. И ваши персональные данные тут

же стали всеобщим достоянием. Кто-то, допустим, решил снять деньги с вашего счета. Оператор в банке спрашивает кодовое слово. Мошенник его не знает. Оператор подсказывает: кличка вашей собаки. И жулик тут же отвечает, потому что ваша собака – на десятке снимков, а в подписи хоть под одним из них кличка указана! Вообще, знание персональных данных может быть настоящим оружием против вас. В России было немало случаев, когда преступник, выйдя из тюрьмы, быстро обзаводился фальшивым паспортом, который тем не менее содержал сведения о вполне реальном, существующем в природе человеке. И с этим паспортом он совершал аферы, а полиция приходила к ничего не подозревающему обывателю.

**– В свое время были очень популярны фейковые аккаунты в соцсетях – когда появлялись двойники страничек известных людей с их фотографиями. И потом со «звезд» требовали деньги, чтобы такие аккаунты закрыть.**

**Эта история по-прежнему актуальна?**

– Мошенники пошли гораздо дальше. Берутся ролик какого-нибудь дебоша и видео с реальным человеком – с его же странички в соцсети. Дальше идет накладывание одного ролика на другой. Получается, что в ролике действуете непосредственно вы! Бьете посуду в ресторане или, скажем, колотите в пьяном виде жену. Это называется дипфейк. Затем к вам обращаются мошенники, присылают видео и поясняют, что готовы отправить его вашему работодателю. Разумеется, появление такого ролика грозит полным разрушением репутации, увольнением и прочими ужасами. Чтобы их избежать, вы готовы заплатить требуемую мошенниками сумму.

**– Футболиста Артема Дзюбу, как известно, тоже шантажировали, требуя пять миллионов долларов.**

**Но платить он не стал. Хотя ролик с его участием был реальным.**

– За вымогательство в крупном размере преступнику может грозить до семи лет колонии.

За нарушение неприкосновенности личной жизни – еще до двух лет! Но Дзюба мог и без денег избежать скандала. Самый простой

вариант защиты для публичных персон — списывать подобные вещи на монтаж. Дескать, это не я — видео смонтировано в целях вымогательства! Думаю, вам поверят, потому что мошенников действительно развелось очень много.

**— Многие боятся скандала и наверняка предпочтут заплатить.**
— И зря. Если вы пойдете на поводу и переведете деньги, это не дает никакой гарантии, что вымогатель не распространит видео или фото или это не всплывет позже где-то еще. Ведь шантажист может это видео или фото перепродать в том же даркнете, «темном» сегменте интернета, особенно если это контент с известной персоной.

**— Сейчас персональные данные пытаются защитить с помощью биометрии.**
**Ведь, например, отпечаток твоего пальца невозможно подделать, а значит, и, скажем, снять с твоего счета деньги.**
— Согласен. Есть одно «но» — биометрические данные можно продать, как и любые другие! И вот представим ситуацию: ваши паспортные данные известны мошенникам, и они, скажем, берут на ваше имя кредиты. Вы идете и меняете паспорт. Или, например, жулики взломали ваш аккаунт в соцсети. Тогда вы просто меняете пароль. Если кто-то сделал клон вашей симки и перехватывает мобильный трафик, вы пошли и поменяли СИМ-карту. На какое-то время это поможет. А вот отпечатки пальцев и лицо вы никак не поменяете! Это работает только в фантастических книгах и голливудских фильмах. В итоге получается, что вы становитесь заложником биометрии.
Вашими данными может пользоваться кто угодно, и поделать с этим ничего нельзя!

**— И что же делать?**
— Это вопрос к законодателям. С моей точки зрения, единственный выход — минимизация сбора и оборота персональных данных.
Нужно просто менять государственную политику в этой области. Ведь сейчас персональные данные собирают буквально все: от госструктур до магазинов у дома. Причем под откровенно

надуманными предлогами. Друзья, мне кажется, мы зарываем под собой мину. Данные потому и персональные, что они должны быть не для всех.

**СПРАВКА**

По данным исследования компании InfoWatch, в России в 2020 году чаще всего обнаруживали утечки информации в хайтек-индустрии, сфере финансов и госсекторе. При этом в общемировом рейтинге на месте финансов находится сфера здравоохранения. Всего, согласно исследованию, за прошлый год в мире утекло около 11 миллиардов записей персональных данных и платежной информации.

ВЕЧЕРНЯЯ МОСКВА

***Наталия Покровская, Никита Миронов***