КАК ЗАЩИТИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ИНТЕРНЕТЕ

28 января — Международный день защиты персональных данных.

Международным днём без интернета, празднование которого приходится на последнее воскресенье января.

День защиты персональных данных отмечается специально для того, чтобы пользователи сети, не забывали о соблюдении правил безопасности при пользовании интернетом, в частности использовании своих персональных данных. Не станем ходить кругами, и сразу перейдем к проблемам, с которыми наверняка встречался каждый из пользователей компьютера.

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Если вам на телефон приходят сообщения или звонки с рекламными предложениями, почта завалена «спамом» и рекламой, на которые вы не подписывались, и даже ваши соседи сверху, отказываются пользоваться вашей не запароленной Wi-Fi сетью, то, скорее всего, вы оказались жертвой собственной доверчивости к интернету. (Впрочем возможно у вашего соседа стоит еще более быстрый и также не запароленный интернет :))

Однако, вернемся к серьёзному. Сегодня вопрос защиты персональных данных стоит крайне актуально, ведь под ними понимается любая информация, относящаяся к человеку (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и любая другая информация.

Основная проблема заключается в том, что личная информация согласно требованиям международного и национального законодательства должна храниться

строго конфиденциально. На деле же – она часто попадает в руки третьих лиц, после чего вам начинают предлагать то, в чем вы не нуждаетесь, названивая и рассылая письма по несколько раз на дню.

Почему это происходит? Потому что чаще всего сам человек своими опрометчивыми действиями или элементарной неосторожностью способствует утечке собственных персональных данных.

КАК ОБЫЧНО ПРОИСХОДИТ УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ?

В большинстве случаев мы указываем свои персональные данные при регистрации на сайтах, оставляя заявки на заказы или даже просто набирая любой поисковый запрос. Обратите внимание, продолжая регистрацию на любом сайте, вы соглашаетесь с пользовательским соглашением, ставя «галочку» при заполнении его полей. Обычно этого достаточно, чтобы разрешить владельцам сайта использовать введенные вами данные при работе с его сервисами. Самые яркие примеры – поисковые системы. Google записывает, анализирует и сохраняет все вводимые поисковые запросы, а его модули, присутствующие на многих сайтах как подключенные компоненты, продолжают собирать информацию даже тогда, когда вы переходите из поисковой системы на другой сайт. Некоторые социальные сети, собирают информацию о пользователе, исходя из его действий и активности на самом сайте.

Подобные случаи можно перечислять долго, но суть их проста – пользуясь сайтом или услугой, вы соглашаетесь на передачу и хранение ваших данных, будь то дата рождения, номер мобильного, переписка и любые другие данные личного характера. Взамен, их обязуются хранить в конфиденциальности и ни в коем случае не разглашать третьим лицам. Однако, на деле, это не всегда так.

НАРУШЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЕЕ ПОСЛЕДСТВИЯ

Не всегда сторона, ответственная за хранение ваших данных, добропорядочно следует своему долгу, ведь персональные данные стоят денег и способны принести приличный доход!

Кроме того, никто не защищен от взлома баз данных, содержащих персональную информацию, или простых ошибок и человеческой опрометчивости. Например, регистрируясь или авторизуясь на сайте через социальную сеть, вы разрешаете сайту получить ваши личные данные и точно неизвестно, как он будет ими пользоваться. Точно также любой ваш звонок в магазин или салон автоматически вносит ваш номер в базу пользователей этой компании.

Сформулированное Википедией определение возможностей злоупотребления использованием персональных данных не потеряло актуальности: «Хотя концепция персональных данных довольно стара, развитие компьютерных сетей и автоматизированного анализа данных позволили красть, централизованно собирать и массово продавать данные о человеке. Эти данные помогают выследить человека, спланировать преступление против него или постороннему выдать себя за человека. Более мирное применение персональным данным — реклама».

Можно лишь согласиться с тем, что полученные третьими лицами данные, могут быть использованы очень разнообразно, вплоть до персонализированных и хорошо выстроенных афер и мошенничеств! Все зависит лишь от человеческой добропорядочности и сознательности.

ВОЗМОЖНАЯ СТРАТЕГИЯ ЗАЩИТЫ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Существует множество способов, как ваши данные могут попасть в чужие руки. Вопрос в том, как защитить себя от этого, в особенности при активном пользовании интернетом.

Во-первых, чтобы обезопасить себя, прежде всего, подумайте, стоит ли передавать свои данные, когда их запрашивают. Подумайте, доверяете ли вы приложению, которое устанавливаете себе на телефон или компьютер, и нужно ли оно вам.

Мы не предлагаем отказаться от всех современных услуг и сидеть в безопасном одиночестве. Однако, возможно не лишним будет, например, завести отдельную почту, используемую лишь для регистрации на сайтах, исключительно для этих целей.

Если вам нужно оставить объявление или контактные данные, то лучшим решением станет использование временной сим-карты и размещение этого объявления под чужим именем (ведь если вас зовут Дмитрий, а публикуете вы свой номер, указывая, что вы Игорь, то спустя месяцы, когда вам позвонят и спросят по телефону Игоря, вы поймете, откуда пошла утечка ваших данных).

Такой незамысловатый способ поможет защитить себя от постоянных рекламных звонков, понять, что вам звонят люди, взявшие ваш номер из интернета. Кстати, вместо покупки сим-карты можно использовать сервисы виртуальных номеров – с них точно так же можно звонить и писать сообщения, но при необходимости такой виртуальный номер легко удалить.

Отдельно следует сказать про личные фото и заметки – они публикуются людьми в открытом доступе и каждый может использовать их без ведома владельца — просто не забывайте об этом.

Во-вторых, защита и профилактика это хорошо, но что же делать, если ваши данные все-таки утекли к организациям, к которым вы не имеете никакого отношения?

Одно дело если вам звонят раз в неделю и совсем другое, когда звонки идут многократно в течении дня, например, от недобросовестных коллекторов, не удосужившихся выяснить, что вы не тот человек, который им нужен.

Кардинальным способом решить этот вопрос является смена телефонного номера. Однако, часто помогает и знание элементарных основ российского законодательства, регулирующего данную сферу.

Согласно Кодексу Российской Федерации об административных правонарушениях (статья 13.11) незаконное распространение и хранение персональных данных является правонарушением и влечет за собой административный штраф. Кроме того, потерпевший может обратится в суд за взысканием морального вреда причиненного постоянными звонками, особенно, если эти звонки происходят в нерабочее время.

Поэтому при наличии подобной ситуации потребуйте у звонящего представиться и назвать свою фирму. Очень часто звонки прекращаются уже на этом этапе.

Если предупреждения по телефону не помогли, вы всегда можете написать письмо на официальном сайте компании, потребовав удаления вашего номера и ваших данных из базы, пригрозив подать заявление на противозаконные действия в полицию и прокуратуру с ходатайством о проведении проверки по факту незаконного хранения и использования ваших персональных данных.

Подводя итог отметим, что защита собственных персональных данных исключительно в ваших собственных руках. Законодательство и практика его применения нацелены на обеспечение их сохранности, но, как и во всех других сферах, существуют различные способы обойти установленные законом рамки. По большей части это становится возможным при попустительстве самих собственников этих данных. Будьте осторожны и принципиальны в этом вопросе и ваши персональные данные останутся только вашими в течении долгих лет.

Автор — специалист АНО НИЦКБ Александр Роков.