Что делать при утечке персональных данных: пошаговый план защиты

Утечка персональных данных — это не абстрактная угроза, а реальная проблема, с которой мы сталкиваемся. Например, только в прошлом году в открытый доступ попало свыше 16 миллионов записей с личной информацией: ИИН, адресами, номерами телефонов и другими данными.

Что такое персональные данные

Персональные данные — это любая информация, с помощью которой можно установить личность человека. Они делятся на общедоступные и ограниченного характера. К первым относятся те, на которые не распространяются требования конфиденциальности, т.е. данные, указанные самим человеком в соцсетях, или размещенные в адресных базах, открытых интернет-источниках и СМИ.

К данным ограниченного доступа относятся фамилия, имя, отчество, дата и год рождения, национальность, адрес проживания или регистрации, ИИН, данные удостоверения личности и другие сведения. Данные ограниченного доступа охраняются законом «О персональных данных и их защита», и именно они чаще всего становятся целью мошенников и недобросовестных компаний, которые хотят через слитую информацию навязывать свои услуги. Да, утечка данных не всегда приводит к тому, что человек станет жертвой аферистов, но в любом случае риски сохраняются. И нужно знать, как себя защитить и вовремя заметить неладное.

Главные признаки утечки данных

1. Спам-звонки, сообщения и электронные письма от компаний или сервисов, которым вы никогда не предоставляли свои данные.
2. Подтверждение регистрации и SMS-уведомления, хотя вы нигде не регистрировались и не заказывали какие-либо услуги.
3. Звонки с незнакомых номеров от людей, которые представляются знакомыми или коллегами. Нередко, чтобы вы им поверили, они оперируют вашей личной информацией. В последнее время технологии резко продвинулись вперед, и можно подделать даже голос, поэтому будьте бдительны.
4. Частые звонки от якобы сотрудников банков или государственных органов - один в звонок в месяц это нормально, но, если на вас выходят несколько раз за короткий срок, это признак того, что ваши данные ушли третьим лицам.
5. Уведомления о подозрительной активности в аккаунтах - запросы кодов, попытки входа в почту или соцсети, а также попытка войти с новых устройств или из зарубежных стран.

Что делать при утечке данных

Шаг первый: выясните, какие именно данные украли

К сожалению, выяснить это удается не всегда — банки, компании или владельцы баз данных редко раскрывают, какие именно сведения оказались у третьих лиц. Однако даже если вы узнали об утечке из новостей или получили уведомление без уточнений, какие данные были скомпрометированы, уже стоит принимать меры. Обычно в таких случаях злоумышленникам становятся доступны электронные и почтовые адреса, пароли, имена, номера телефонов и данные банковских карт.

Шаг второй: измените слитые данные

Конечно, менять место жительства не нужно, но вы можете изменить и дополнительно защитить учетные записи в социальных сетях, сайтах, которыми регулярно пользуетесь *(например, для получения госуслуг или маркетплейсах).* Если у вас раньше была привычка использовать один пароль

везде, сделайте для каждого сервиса отдельный. В мессенджерах, например, можно ввести функцию по запросу пин-кода – это дополнительно вас защитит, а в приложениях банков — биометрию.

Шаг третий: настройте двухфакторную аутентификацию

Не пренебрегайте этой мерой — она может уберечь ваши данные, деньги и нервы. Включите двухфакторную аутентификацию везде, где это возможно. Можно выбрать удобный способ подтверждения: код из приложения-аутентификатора, через номер телефона, по электронной почте или в сообщении. В результате, даже если ваши пароли попадут к злоумышленникам, они не смогут получить доступ к аккаунтам.

Шаг четвертый: регулярно проверяйте все свои учетные записи

В первые дни после того, как стало известно об утечке данных, регулярно проверяйте аккаунты во всех важных сервисах и приложениях. В дальнейшем тоже не прекращайте контроль: отслеживайте подозрительные входы, неизвестные устройства и необычную активность. Кроме того, раз в три–шесть месяцев обновляйте пароли, PIN-коды, программное обеспечение и антивирусные программы.

Шаг пятый: обсудите ситуацию со своим банком

Даже если злоумышленники получили доступ только к вашей электронной почте, этого уже достаточно, чтобы попытаться добраться до ваших счетов. Почта часто связана с номером телефона, а он, в свою очередь, используется в интернет-банкинге — в таком случае риск для ваших средств значительно возрастает. Чтобы этого избежать, важно выполнить все предыдущие меры, а также связаться с банком и его службой безопасности: они так же заинтересованы в защите ваших данных, поскольку от этого зависит и их репутация.

Как еще можно защитить свои персональные данные

1. **Не открывайте письма от незнакомых отправителей** и не переходите по подозрительным ссылкам — это простое правило поможет избежать множества проблем.
2. **Регулярно обновляйте программное обеспечение на своих устройствах:** обновления устраняют уязвимости и усиливают защиту от киберугроз.
3. **Используйте надежные пароли и двухфакторную аутентификацию** — это один из ключевых элементов цифровой безопасности. Подключайте 2FA везде, где возможно, а пароли делайте длинными, сложными и не связанными с личной информацией вроде даты рождения.
4. **Защищайте домашний Wi-Fi и избегайте открытых сетей**: недостаточно защищенное соединение может стать точкой доступа для злоумышленников. В общественных местах через открытые сети также есть риск перехвата данных.
5. **Правильно утилизируйте старые жесткие диски:** на устройствах хранится много чувствительной информации, а простое форматирование не гарантирует её полного удаления, поэтому лучше физически уничтожать носители перед утилизацией.
6. **Отключайте Bluetooth, когда он не используется:** включенное соединение облегчает обнаружение устройства и может повысить риск несанкционированного доступа.
7. **Шифруйте данные:** на первый взгляд это может показаться сложным, но современные инструменты делают процесс доступным. Например, в macOS есть встроенное решение FileVault, которое позволяет зашифровать весь диск.