МОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ УКРАЛИ. ЧТО ДЕЛАТЬ?

Андрей прочитал, что в сеть утекли данные тысяч людей. И даже было написано, какая компания их продает. Он зашел на ее сайт и увидел демофрагмент из базы, где были его имя и номер карты. Теперь Андрей боится, что мошенники смогут украсть все деньги с его счета. Рассказываем, чем грозят утечки персональных данных и как обезопасить свои деньги, если информация о вашем счете попала к преступникам.

Зачем преступникам мои данные?

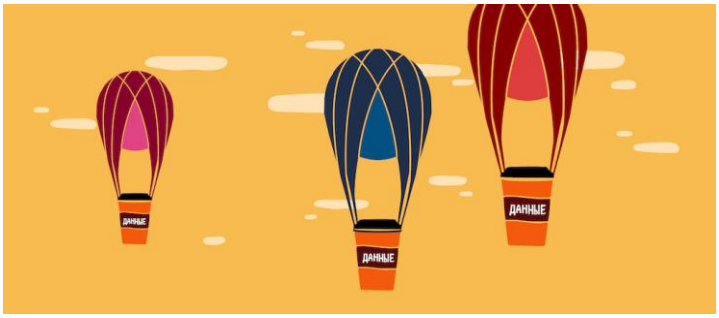
Как правило, информации, которая утекает в сеть из баз данных финансовых организаций и других компаний, недостаточно, чтобы украсть деньги без вашего ведома. Но персональные данные в открытом доступе привлекают мошенников. С помощью социальной инженерии они пытаются раздобыть недостающую информацию, которая позволит добраться до ваших сбережений. Мошенники рассчитывают на то, что источником необходимых им данных станут сами владельцы карт и счетов.

Обманщики звонят и представляются сотрудниками банковской службы безопасности, присылают сообщения «о блокировке карты». Пишут по электронной почте, что «вам положена компенсация, нужно лишь заплатить небольшую комиссию за ее перевод на ваш счет». А иногда даже стучатся в дверь и предлагают «сдать анализ на коронавирус», потому что «у соседей тест показал положительный результат».

Легенды бывают самые разные. Но задача всегда одна: махинаторы играют на эмоциях, чтобы люди добровольно перевели им свои сбережения или сообщили секретные данные, которые позволят списать деньги с банковских карт. А в случае очной встречи, могут просто обчистить квартиру.

Чтобы завязать разговор, втереться в доверие и подтолкнуть к необдуманным действиям, преступникам нужно знать не так много. Для их целей вполне достаточно имени, адреса, номеров телефона и карты.

Когда клиенты сами выдают секретную информацию мошенникам или по их инструкции переводят деньги на чужие счета, банки не компенсируют потери. И в абсолютном большинстве случаев люди лишаются сбережений из-за собственной доверчивости, а не потому, что их счета взломали хакеры.



Как персональные и платежные данные оказываются в сети?

За последние годы несколько раз данные клиентов сливали сотрудники банков, микрофинансовых организаций, коллекторских бюро и кредитных брокеров.

Иногда хакерам удается взломать базы интернет-магазинов и сервисных компаний, отелей и перевозчиков.

Но нередко люди сами делятся номерами своих карт или даже публикуют их фотографии в соцсетях и мессенджерах. Киберпреступники взламывают аккаунты и собирают такие данные в собственные базы, чтобы затем выставить их на продажу.

Некоторые пользователи вводят свои имена, номера телефонов и реквизиты карт на страницах псевдоконкурсов, лотерей и опросов или на сайтах-двойниках настоящих финансовых организаций, магазинов и других компаний. Такие фишинговые сайты мошенники создают специально, чтобы собирать персональные и платежные данные.

Я слышал, что мошенники могут получить дубликат сим-карты с моим номером телефона — и СМС-коды будут приходить им.

Такая схема мошенничества действительно существовала. По поддельным документам и фальшивой доверенности преступники получали дубликат сим-карты с чужим номером и перехватывали СМС-сообщения. Эта схема была трудоемка и опасна для самих махинаторов. Им приходилось лично обращаться в офис оператора связи. Из-за этого резко возрастала вероятность, что их вычислят и поймают.

Сейчас подобная схема встречается редко. Многие банки и мобильные операторы заключили соглашения об обмене информацией при замене сим-карты. В таких случаях банки приостанавливают СМС-информирование на один-два дня.

Если преступникам все же удастся завладеть вашим номером, вы сразу узнаете об этом — сим-карта в вашем телефоне перестанет работать. В таком случае стоит немедленно связаться с банком и отключить от номера все услуги. Тогда преступникам не удастся ничего украсть.

Если вы сами решите заменить сим-карту или перейти со своим номером к другому сотовому оператору, стоит предупредить об этом свой банк, чтобы он не отключал СМС-сервис. Банки всегда проводят идентификацию клиентов, в том числе при звонке на горячую линию. Вероятность, что мошенник пройдет проверку банка и продолжит получать СМС-сообщения для подтверждения операций, очень мала.

Вдруг и мои данные попадут к обманщикам? Как от них защититься?

Полностью предотвратить утечки данных вы не можете. Но свести риск потери денег к минимуму — в ваших силах. Важно всегда соблюдать правила финансовой безопасности.

- Никому не сообщайте полные реквизиты своей карты и не выкладывайте ее фотографии в сети. Если кто-то хочет перевести вам деньги, ему достаточно знать только номер карты или даже просто номер телефона.
- Вводите данные карты только на защищенных сайтах надежных компаний. Официальные сайты финансовых организаций, а также многих онлайн-магазинов и сервисов в поисковых системах «Яндекс» и Mail.ru помечены галочками. Защищенное соединение легко узнать по значку закрытого замка и адресу, который начинается с https:/.
- Платежи лучше проводить через безопасные шлюзы платежных систем: они перекидывают вас на сайт банка, который для подтверждения операции присылает код подтверждения в СМС-сообщении.
- Подключите СМС-оповещения или push-уведомления об операциях. Так вы сразу же узнаете, если по карте кто-то проведет платеж без вашего согласия.
- Если вам звонят или присылают сообщения от банка с тревожными или радостными новостями о балансе вашего счета, лучше не поддерживать разговор и сразу положить трубку, не отвечать на сообщение. Стоит набрать официальный телефон горячей линии — он указан на обратной стороне карты и на сайте банка. Объясните ситуацию специалисту, он подскажет, что в действительности происходит с вашим счетом и как лучше поступить в таком случае.
- Используйте сложные пароли для своей электронной почты и личных кабинетов на сайтах. Пароли типа 12345 или Password не смогут вас защитить. В идеале все пароли должны быть разными, длинными, с прописными и строчными буквами, цифрами и специальными символами. При этом желательно, чтобы для вас пароль имел смысл и вы могли его запомнить. Как и реквизиты карты, пароли нужно хранить в тайне.