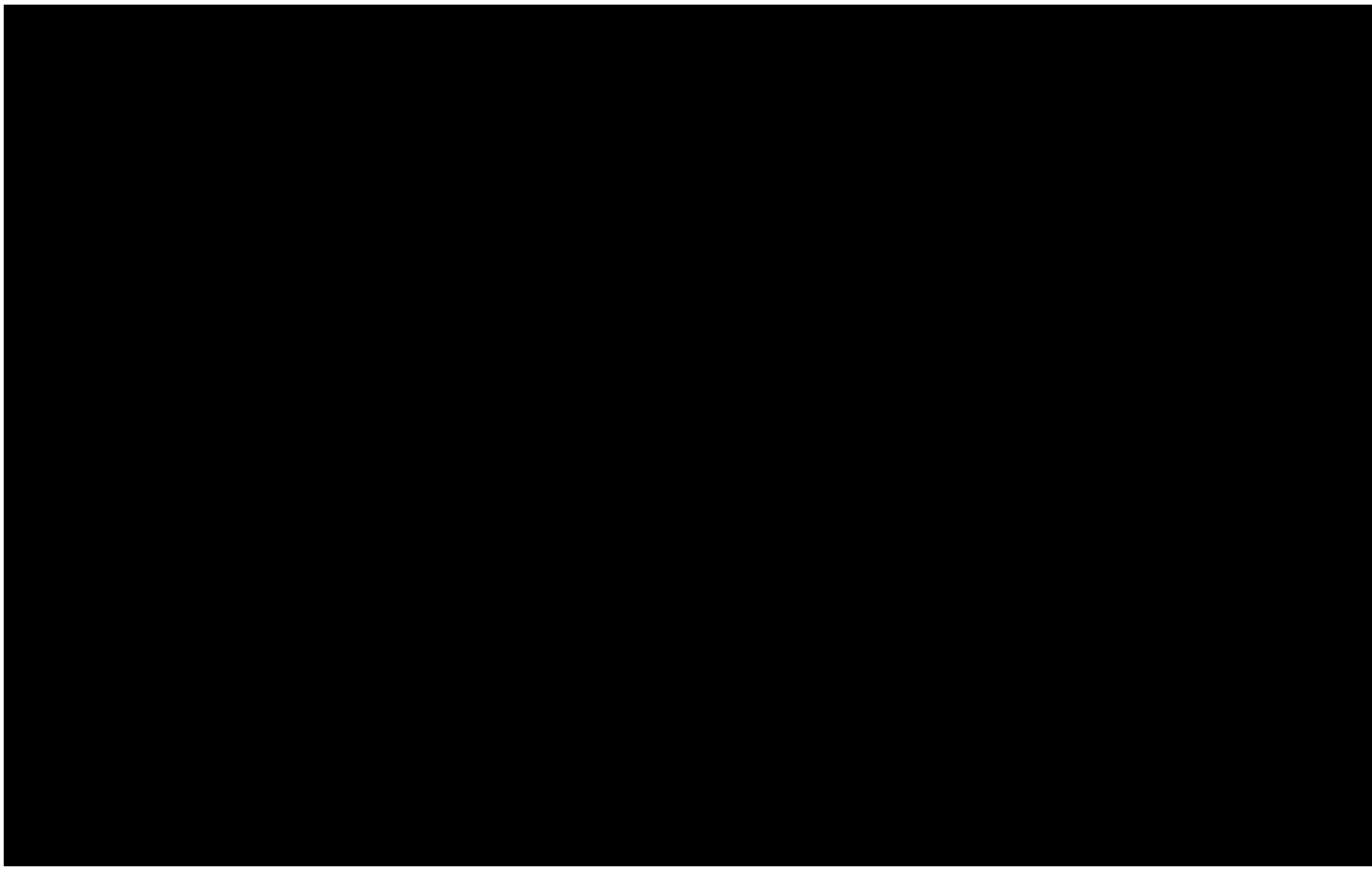
Что будет, если ваша SIM-карта окажется в чужих руках? Воры не будут звонить бабушке в Саратов. Они просто украдут все ваши деньги.



Зачем вообще красть SIM-карту?

Во многих онлайн-сервисах используется двухфакторная авторизация. Вводишь пароль, получаешь SMS с кодом, вводишь код — входишь. Но есть один нюанс: если забудешь пароль, то восстановить его зачастую можно тоже через SMS.

То есть, стоит кому-либо получить доступ к вашей SIM-карте, как все сервисы, где используется двухфакторная авторизация — от мессенджеров (включая архив) до интернет-банка — перейдут под контроль злоумышленника.

Как воруют SIM-карты

Можно, конечно, просто украсть у вас телефон, но тогда вы, скорее всего, оперативно заблокируете «симку». Хотя и за эти несколько минут преступники могут успеть сделать то, что им нужно.

Однако красть сам аппарат довольно сложно и рискованно. Поэтому одним из наиболее распространенных видов кражи стало получение дубликата SIM-карты у вашего оператора.

Происходит это так: зная ваши ФИО и номер телефона, преступник делает липовую доверенность и с ней приходит в офис оператора. Там ему выдают новую «симку» с вашим номером.

Обращаем внимание, что такое может произойти только тогда, когда сотрудник оператора состоит в сговоре с мошенником, потому что обычно ксерокопии для восстановления «симки» недостаточно.

Итак, в тот момент, когда делается дубликат вашей «симки», ваш телефон отключается, а новый хозяин получает возможность принимать ваши звонки, сам звонить кому-либо с вашего номера. И, конечно, принимать SMS-сообщения.

Получается, аппарат-то все время при вас и включен, и даже показывает, что он в сети. Просто в какой-то момент вам перестают поступать входящие звонки и сообщения, и вы тоже не можете никуда позвонить. Сначала вы грешите на оператора, потом на аппарат, перезагружаете его, потом пытаетесь вставить другую SIM-карту, в итоге звоните в колл-центр, чтобы разобраться, и тут... Тут выясняется, что номер больше вам не принадлежит.

Так, у одного из пострадавших мошенник переоформил SIM-карту на себя по поддельной доверенности. Жертва написала претензию оператору и заявление в полицию. Претензию приняли, попросили подождать, но через день мошенник переоформил абонентский номер снова, теперь на юрлицо.

Вот уже почти месяц жертва ждет ответа от оператора, пишет претензии, но тот ссылается на то, что на ответ у них есть 60 дней. SIM-карта заблокирована, и по номеру, который знают все клиенты и который указан в рекламе, никто не может дозвониться. Турагент теряет клиентов и деньги и подозревает, что это могут быть происки конкурентов.

Защититься от кражи SIM-карты можно двумя способами

- ***Не публикуйте свой основной номер нигде в интернете — ни в соцсетях, ни в формах регистрации интернет-магазинов, ни на***

сайтах бесплатных объявлений.

- ***Заведите для двухфакторных авторизаций еще одну SIM-карту, номер которой будете знать только вы. Вставьте ее во второй слот «двухсимочника» или купите под нее простенький телефон за 500 рублей.***

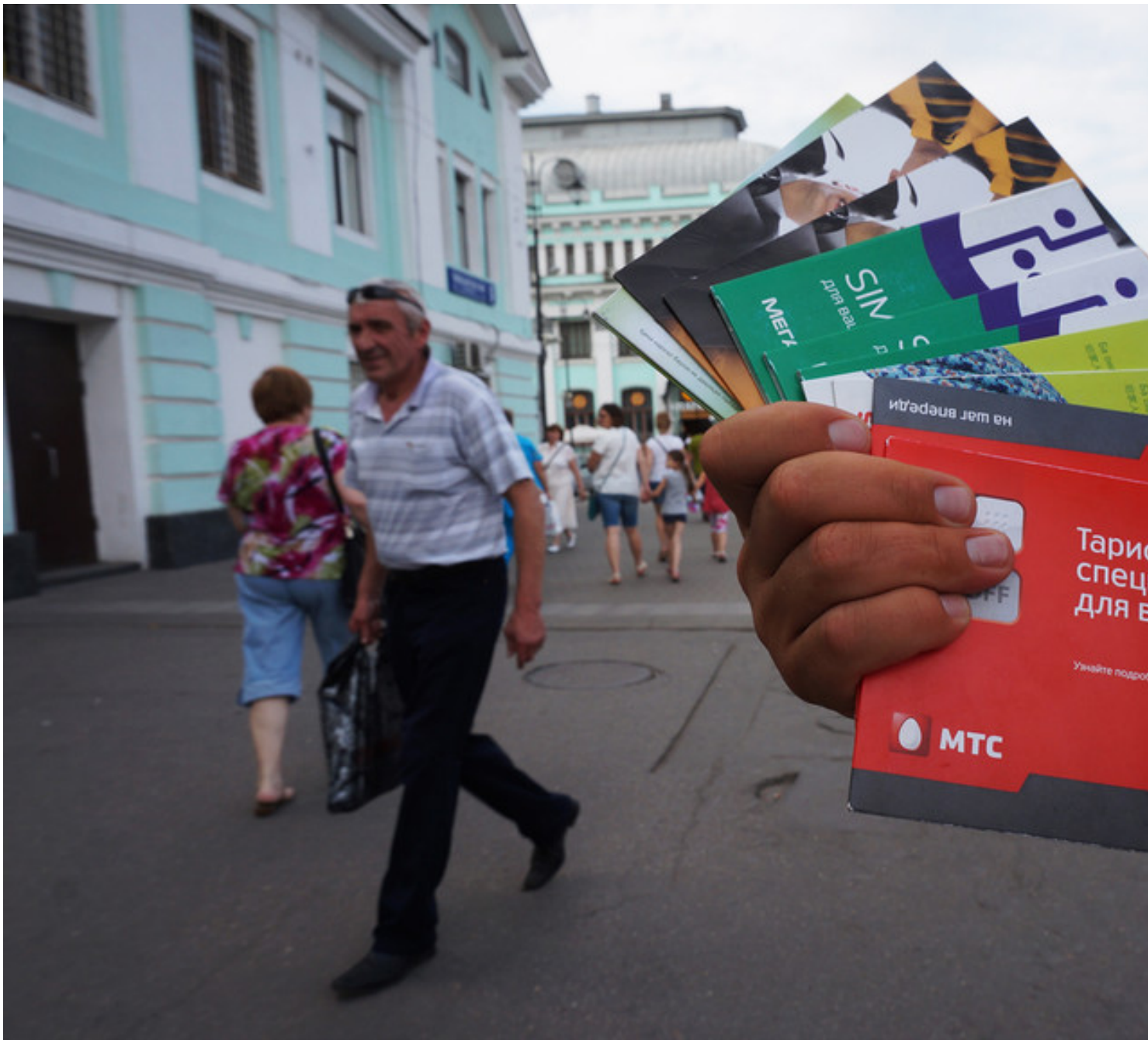
«Левая» SIM-карта на ваше имя — это к долгам

Вы не задумывались, на кого оформлены все эти SIM-карты, которые продаются на улицах? Нелегальные продавцы в переходах реализуют в месяц по 1,5-2 миллиона SIM-карт, оформленных на украденные паспортные данные. Как это происходит: сообщники мошенников из салонов сотовой связи вводят в форму регистрации паспортные данные реальных людей, ведь если придумывать такое просто «из головы», очень быстро вычислят. А так создается впечатление, будто действительно приходил человек с таким паспортом. И да, купил сразу два десятка номеров.

То есть, вы покупаете одну SIM-карту, а на ваши же данные «вешают» еще несколько. Это называется «дилерским фродом». Дело в том, что дилер получает вознаграждение за каждую проданную «симку», поэтому не гнушается реализовывать их любыми способами.

Преступники используют эти «левые» SIM-карты для разных махинаций. Одна из них — знаменитое «Положите деньги на этот номер». Второй способ — загнать балансы этих карт в минус (например, роумингом или организацией подпольного переговорного

пункта для гастарбайтеров), после чего оператор, найдя вас по паспортным данным, списывает задолженность с вашего основного номера. Да и в случае чего, все претензии правоохранительных органов будут адресованы вам.



Не приобретайте SIM-карты у уличных торговцев

Так, например, на одну из известных нам жертв мошенников была зарегистрированна SIM-карта, о существовании которой он узнал, когда владелец «липовой» SIM-карты загнал ее в небольшой минус, а оператор предупредил о задолженности. Выяснить ничего не удалось, а вот долг пришлось погасить.

Защититься от переоформления SIM-карты можно так:

- ***Не оставляйте нигде в интернете свои паспортные данные, особенно при регистрациях на разных сайтах. Исключение — покупка электронных билетов на поезд и самолет на доверенных сайтах (например, авиакомпаний и РЖД) и регистрация в финансовых сервисах.***

- ***Покупайте SIM-карты только в фирменных офисах операторов.***

Если на ваше имя уже оформлена «левая» сим-карта, нужно обратиться с заявлением в полицию и в офис оператора. Однако будьте морально готовы к тому, что дело «спустят на тормозах», потому что вы вряд ли сможете доказать, что не приходили такого-то числа в такой-то салон связи.

Профилактика: 3 правила безопасности

- ***Не отключайте запрос PIN-кода SIM-карты. Конечно, неудобно его вводить при каждом включении телефона. Зато у злоумышленников будет меньше шансов, если к ним попадет ваша SIM-карта.***

- ***Установите пароль, графический ключ или отпечаток пальца для разблокировки смартфона. Это не позволит украсть ваши данные.***

- ***Нет ничего зазорного в том, чтобы раз в несколько месяцев заходить по дороге в офис оператора и узнавать, какие номера оформлены на ваш паспорт. Если появились новые — их лучше сразу от греха подальше заблокировать.***

Тэги: если , через , многих , зачем , тоже , пароль , ваша , используется , вводишь , получаешь
,
кодом
,
авторизация
,
онлайн-сервисах