«Потерял телефон — отдавай миллион»

Игорь, Владивосток

Больше года назад у меня украли смартфон. На нем были установлены «Госуслуги» и банковские приложения. С карты одного из банков воры успели вывести небольшую сумму – пару тысяч рублей, а остальные карты я быстро заблокировал. Я написал заявление в полицию, но уголовное дело так и не завели, ведь ущерб был небольшой. Купил новый телефон, установил на него все приложения, поменял пароли и поскорее забыл об этом инциденте. А зря – я не понял, что неприятности у меня только начинаются.

Месяц назад я попытался войти в «Госуслуги», но мне это не удалось – ни с телефона, ни с ноутбука, ни с других гаджетов. Пароль не подходил, а восстановить его не получалось. Позвонил на горячую линию «Госуслуг», но сразу вернуть доступ к моей учетной записи они не смогли.

Я сразу подумал, что это может быть не техническая ошибка, а взлом моего аккаунта, и пошел писать заявление в полицию. Но на него не обратили особого внимания, так как никакого материального ущерба на тот момент еще не было.

Тем временем у меня неожиданно сменился номер мобильного, которым я пользовался почти всю жизнь. Видимо, это тоже как-то организовали преступники, чтобы я не получал сообщения от банков. Номер удалось вернуть на следующий день – после того, как я написал оператору заявление о мошенничестве. Но пока я этим занимался, воры в моем банке оформили от моего имени кредитную карту и вывели с нее почти полмиллиона рублей.

Неделю я ходил по разным инстанциям – ПФР, МФЦ, звонил на горячую линию «Госуслуг» и банка… Быстро мне нигде не могли помочь: срок рассмотрения заявок везде от 10 до 30 дней.

На заведение уголовного дела в полиции ушло больше двух недель – разбирались с моим материальным убытком, передавали между разными отделами, ждали решения прокуратуры.

Затем пришло СМС от еще одного банка с предложением взять кредит. Дел с этим банком до этого я не имел, и такое предложение меня насторожило. Я отправился к ним в офис, и опасения подтвердились – в банке сообщили, что на мое имя оформлена дебетовая карта и оставлен запрос на кредит наличными. Карту получил в другом городе человек по поддельному паспорту. В банке мне показали его скан: все указанные данные – мои, кроме фотографии и подписи.

Я тут же подал заявление о выдаче нового паспорта. Но на его получение внесение старых паспортных данных в реестр недействительных на портале МВД тоже нужно около недели.

Тут мне пришло в голову, что, возможно, на меня оформили и другие кредиты. Обратился в бюро кредитных историй и узнал, что мошенники оформили на меня несколько микрозаймов в разных МФО и еще один большой кредит в банке. Таким образом за пару недель я оброс долгами больше чем на миллион рублей.

Выяснилось, что последний кредит был оформлен не по липовому паспорту, а удаленно через электронную цифровую подпись, которая была получена с помощью данных с Портала госуслуг (ИНН и СНИЛС). Отозвать сертификат на эту подпись можно только в том удостоверяющем центре, где он был выпущен. А выяснить, что это за центр, так и не удалось, и теперь с этим вопросом придется разбираться через Минкомсвязи. Сколько это займет времени и сколько за это время у меня появится новых кредитов, выданных через ЭЦП, – никто не знает.

Пока только две из пяти МФО ответили на мои обращения и согласились признать займы недействительными. С банками, выдавшими крупные кредиты, видимо, предстоит разбираться в судах.

Совет эксперта по противодействию мошенничеству:

Мошенники провели многоуровневую сложную операцию. Получив доступ к учетной записи Игоря на Портале госуслуг, они сменили его контактную информацию. Именно поэтому не работали обычные способы восстановить пароль – по номеру мобильного или через электронную почту. После замены данных письма со ссылками и проверочные СМС приходили мошенникам.

Параллельно они подключили Игорю другой номер, чтобы он временно не мог получать коды от банков и вообще не знал, что ему приходят запросы на оформление кредитов и займов и на другие операции. Сотовые операторы позволяют клиентам менять номер на своей сим-карте дистанционно – и аферисты этим воспользовались. А пока Игорь разбирался, в чем дело, и пытался вернуть свой номер, мошенники указали свои контакты во всех его аккаунтах, в том числе в банковских приложениях.

Игорь правильно сделал, что немедленно обратился в полицию. Так ему будет проще оспорить незаконно оформленные на него кредиты и займы и доказать, что брал их не он. По каждому кредитному договору, в том числе заключенному с помощью электронной цифровой подписи, правоохранители должны будут провести отдельное расследование.

Как защитить свои личные и платежные данные?

Если у гаджета есть функция распознавания лица или отпечатка пальца, лучше настроить биометрическую идентификацию. Сымитировать биометрию гораздо сложнее, чем подобрать символьный код.

Не стоит сохранять в гаджетах логины и пароли к Порталу госуслуг, электронной почте и банковским приложениям. Нужно придумать сложные пароли, для каждого сервиса свой, и лучше вводить их заново при каждом входе.

Не храните в телефоне фотографии паспорта и других документов. Если устройством завладеют мошенники, у них в руках окажутся важные данные, которых может оказаться достаточно, например, для оформления кредита на ваше имя.

Если на украденном или потерянном смартфоне установлено приложение Портала госуслуг, помимо блокировки карт и смены паролей в мобильных банках, нужно сразу же сменить пароль к своей учетной записи и обязательно отвязать от нее утраченное устройство. Для этого надо зайти в раздел «Настройки и безопасность» и во вкладке «Связанные приложения» изменить список устройств, с которых возможен доступ.

Преступники оказались расторопнее и успели добраться до Портала раньше вас? Дистанционно вернуть себе доступ к аккаунту уже

не удастся. Обратитесь с паспортом в МФЦ и попросите выдать новый пароль для входа в личный кабинет.

В случае кражи или потери телефона надо как можно скорее сменить пароли ко всем почтовым ящикам, социальным сетям, личным кабинетам во всех приложениях, а также при возможности воспользоваться опцией удаленного выхода со всех мобильных устройств. Получив доступ к вашим пользовательским данным, злоумышленники могут собрать дополнительную информацию и устроить мошеннические атаки на ваших друзей, родственников и коллег.

Чтобы исключить ситуацию с кражей номера телефона, обязательно договоритесь с оператором связи о дополнительном способе идентификации вашей личности, когда вы обращаетесь за помощью удаленно. К примеру, им может стать кодовое слово. Ведь действительно по просьбе абонента оператор может дистанционно заблокировать его текущий номер и привязать к сим-карте новый. Для этого потребуются только личные данные, прописанные в договоре: ФИО, паспортные данные, дата рождения и адрес регистрации. Но вы можете попросить оператора связи добавить к этому списку кодовое слово – оно будет дополнительным уровнем защиты от мошенников.