**Как защитить себя от желающих похитить деньги**

Согласно статистике, в первом полугодии 2023-го года число краж с банковских счетов выросло на треть по сравнению с первой половиной 2022-го года. Разберемся в самых популярных схемах мошенников и в том, как от них защититься.

За первую половину 2023-го года мошенники украли у россиян более 8 млрд руб., это на 33% больше того же периода год назад, следует из отчета ЦБ. Из них 1,3 млрд руб. было похищено через Систему быстрых платежей (СБП). Вернуть удалось только 4,39% от всей суммы — около 356,6 млн руб. Всего ЦБ зафиксировал 531,8 тыс. инцидентов.

Почти половина хищений (48,4%) совершается с использованием социальной инженерии – то есть случаев с психологическим воздействием на людей. В 2021 и 2022 годах показатели были выше — 51,6% и 49% соответственно.

В то же время за период с января по июнь 2023 года банки не допустили более 9 млн краж средств на 1,6 трлн руб. В деньгах это в 200 раз больше объема потерянных россиянами средств за тот же период.

Самыми частыми видами мошенничества в первом полугодии 2023 года стало снятие преступниками денежных средств с банковских карт — за полгода ЦБ зафиксировал 441,1 тыс. таких случаев на сумму чуть более 3 млрд руб. Из них вернуть удалось в I квартале лишь 5,6% (почти 76,4 млн руб.), а во II квартале — 7,2% (почти 122,5 млн руб.).

На втором месте по числу — кражи со счетов. К примеру, с помощью взлома мобильных приложений. За январь — июнь произошло 51,3 тыс. случаев. Именно таким образом мошенники похищают больше всего средств — 3,5 млрд руб. Доля возврата в таких случаях в разы ниже: в I квартале — 1,5% (37,3 млн руб.), а во II квартале — 1,7% (17,5 млн руб.).

С электронных кошельков Банк России зафиксировал 6 тыс. случаев операций без согласия клиента на общую сумму почти 48,9 млн руб., но доля краж методами социальной инженерии здесь одна из самых высоких — 92,4% случаев в I квартале и 99% случаев во II квартале. Вернуть украденные средства граждане не смогли.

Во II квартале возросла активность телефонных мошенников, отмечает ЦБ: количество звонков увеличилось в 2,5 раза за три месяца — до 276 775. Наиболее распространенной практикой остаются звонки от лжесотрудников Банка России или якобы работников банков.

При этом активность злоумышленников в интернете немного сократилась. Если в I квартале ЦБ выявил 1489 ресурсов, предлагающих различные финуслуги, но не имеющих лицензии на такую деятельность, то во II квартале их количество сократилось примерно на 8%, до 1365. Число фишинговых сайтов уменьшилось по итогам апреля — июня почти на 10%, до 4924 ресурсов. Единственная категория, показавшая рост, — финансовые пирамиды. Их стало больше на 31% (1767 ресурсов).

**Мошенники в Забайкальском крае**

На сегодняшний день в Забайкальском крае растет число мошенничеств, связанных с использованием сотовой связи и сети Интернет. Количество таких преступлений в Забайкалье к июлю 2023 года выросло почти на 46%, а раскрываемость снизилась. Однако уровень раскрываемости мошеннических преступлений в Забайкальском крае выше, чем в целом по России. Об этом 30 июня во время брифинга сообщил начальник управления по надзору за уголовно-процессуальной и оперативно-розыскной деятельностью прокуратуры Забайкальского края Александр Захаров. По его словам, в Забайкалье раскрывают 33,4% интернет-мошенничеств, по России этот показатель около 31%. Прирост количества мошенничеств в информационной среде за первые 3 месяца 2023 года составил 44,4% в Забайкальском крае, сообщили на сайте прокуратуры региона.

Чаще всего, кража происходит под предлогом перевода денежных средств на безопасный счет из-за возникшей угрозы незаконного списания суммы или подозрительной транзакции. В этом случае мошенники представляются работниками банков».

 Так, например, в УМВД России по городу Чите обратился 37-летний читинец и сообщил о хищении крупной суммы денег. Сотрудники полиции установили, что мужчине позвонили неизвестные. Они представились работниками службы безопасности банка, сообщили о попытках снятия денег с его банковской карты. Мужчине предложили перевести средства на безопасные счета, чтобы их обезопасить. Под диктовку мошенников потерпевший осуществил несколько переводов на номера счетов, указанных злоумышленниками. В результате доверчивый забайкалец лишился свыше 1,3 миллиона рублей.

В апреле 2023 года житель Читы перевел мошенникам 4 миллиона рублей, поверив, что его подозревают в госизмене. Пострадавшему позвонил неизвестный и, представившись сотрудником внутренних органов из Москвы, сообщил, что его подозревают в госизмене. По словам лжеполицейского, со счета забайкальца якобы зафиксированы переводы в адрес запрещенных организаций. Затем к разговору подключились подставные сотрудники ФСБ и Центробанка. Они предложили обезопасить имеющиеся деньги, а также исчерпать кредитный лимит, оформив максимально возможные суммы, и перевести средства на «безопасные счета».

Под диктовку злоумышленников гражданин перечислил свои накопления, занял деньги у родственников, а также оформил три кредита на общую сумму больше 3 миллионов рублей. Кроме того, мошенники убедили его купить новый телефон, установить на него программу удаленного доступа к счетам и «личным кабинетам» банков. Мошенники были на связи с потерпевшим на протяжении пяти дней. Всё это время он ходил по отделениям банков и оформлял кредиты. При этом злоумышленники категорически запретили читинцу сообщать кому-либо о ситуации, в которой он оказался, а целью получения кредитов называть ремонт дома или покупку автомобиля.

По факту мошенничества, совершенного в особо крупном размере, возбуждено уголовное дело.

С октября 2022 года по август 2023 года в Забайкалье задержали 11 курьеров, которые помогали забирать деньги у пенсионеров после обмана мошенниками. Все задержанные работали в составе организованных преступных групп. Во всех случаях мошенники сообщали забайкальцам, что их родственники попали в беду. Задания курьеры получали по телефону или в мессенджерах — там им писали адреса жертв, как правило, пожилых людей. Потом через банкоматы курьеры переводили деньги на счета, которые диктовали им заказчики.

Так, в октябре 2022 года был задержан курьер, который забрал у обманутых 2,7 миллиона рублей, у него успели изъять 145 тысяч из них. Сейчас на его квартиру наложили арест, проводится расследование.

Также в июне этого года задержали двух жителей Амурской области 1992 и 1995 года рождения. Они приехали в Читу на поезде, чтобы забрать деньги под предлогом того, что родственники читинцев попали в ДТП, — успели совершить 7 преступлений на 2,9 миллиона рублей. Из них удалось изъять 930 тысяч рублей. 20-летний читинец совершил пять таких преступлений в Чите, Краснокаменске и в Читинском районе на 2,4 миллиона рублей.

Не менее распространены случаи хищения денежных средств посредством известных сайтов по продажам товаров и услуг. В данном случае потерпевшие называют все реквизиты карты либо переходят по интернет-ссылкам, которые им присылают потенциальные покупатели. В результате граждане оказываются на «фишинговых» сайтах и позволяют мошенникам получить удаленный доступ к онлайн-банку и похитить денежные средства.

В настоящее время получают распространение преступления, совершенные в социальных сетях. Сотрудники правоохранительных органов рекомендуют тщательно проверять представленную рекламную информацию, читать отзывы о той или иной фирме, у которой намереваетесь приобрести товар и убедиться в порядочности продавца.

По мнению специалистов, практически во всех случаях причиной хищения денежных средств, каким бы способом они не были совершены, является доверчивость граждан. Единственная и главная защита от мошенников – это бдительность и разумность.

**Что делать если вас пытаются обмануть мошенники**

|  |  |
| --- | --- |
|  | **Вариант 1. Человеку позвонили мошенники, представились сотрудниками банка, убедили назвать данные карты. Что делать в таком случае?** |

Если вы уже сообщили посторонним конфиденциальную информацию по карте и только потом спохватились, необходимо срочно заблокировать карту любым доступным способом. Быстрее всего сделать это можно через мобильное приложение вашего банка. Найдите заранее в приложении опцию «заблокировать карту», чтобы не тратить время на ее поиски в экстренной ситуации.

Если у вас на телефоне приложение не установлено, звоните в банк по телефону горячей линии. Номер для экстренной связи обычно указан на оборотной стороне карты. Лучше заранее сохранить этот номер в телефон. Оператор горячей линии попросит назвать паспортные данные, кодовое слово или код из СМС-сообщения, которое он вам вышлет. Только после этого сотрудник банка заблокирует карту.

Также некоторые банки позволяют блокировать карты по СМС. Информацию о наличии такой опции и ее активации лучше узнать заранее при оформлении карты. Обычно для этого надо отправить на короткий номер банка кодовое слово (например, «блокировка») и через пробел последние четыре цифры номера карты.

|  |  |
| --- | --- |
| **Вариант 2. Мошенники убедили установить на телефон приложение с удаленным доступом или человек предоставил пароли и явки от мобильного банка. Что делать в такой ситуации?** |  |

Попав в мобильный банк, мошенники получают возможность опустошить все ваши счета за считаные минуты. Поэтому успех в такой ситуации зависит от скорости действий. Предлагаю следующий алгоритм действий:

* Срочно позвонить по номеру горячей линии, чтобы заблокировать движение средств по счетам или попробовать отменить транзакции;
* Смените пароль для входа в мобильный банк в личном кабинете;
* Проверьте все личные данные на привязку к другому номеру телефона;
* Обратитесь в отделение банка с заявлением на возврат незаконно списанных средств. Сделать это необходимо в течение суток. Может возникнуть ситуация, когда средства уже списаны со счета клиента, но еще не зачислены на счет мошенников. По закону у банков есть три дня для проведения транзакций. И если банк поторопить, то транзакцию можно аннулировать и вернуть деньги безболезненно.
* Поскольку кража денег — это уголовное преступление, напишите заявление в полицию. Возможно, ваша информация поможет быстрее вычислить и поймать преступников.

Однако помните, что банки не обязаны возвращать деньги, если клиент нарушил правила обслуживания и сам передал третьим лицам пароли, коды подтверждения и прочие данные, которые позволили мошенникам украсть деньги со счетов. Такие переводы будут считаться добровольными и банк не будет списывать средства со счета получателя. Банки не имеют права вмешиваться в договорные отношения клиентов.

Кстати, в суде такому клиенту скорей всего тоже откажут: практика российских судов свидетельствует о том, что суды чаще всего принимают сторону банков, поскольку понимают вину самих граждан в раскрытии персональных данных для доступа к счетам.

Помните, что в арсенале банков сегодня большой комплекс средств и механизмов защиты от кибермошенников, от взломов приложений, но банки не могут отвечать за то, какие программы загружает клиент на свой телефон. Важно помнить, что сотрудник банка никогда не запросит назвать персональные данные, в том числе информацию по банковским картам и счетам, коды подтверждения из СМС, а также установить на ваше устройство какие-либо программы, например, антивирус или программы для удалённого доступа.

|  |  |
| --- | --- |
|  | **Вариант 3. Мошенники убедили человека, что нужно перевести деньги на резервный/безопасный счет. Человек перевел – что делать?** |

В этом случае в первую очередь нужно звонить не на горячую линию в банк, а в полицию. Заявление в полицию нужно подать как можно скорее. Сделать это проще онлайн на сайте МВД через страницу управления в своем регионе. В заявлении необходимо описать все максимально подробно: все известные вам данные мошенников, сколько денег и за что вы перечислили. Приложите банковские выписки о переводах. Чем больше информации вы дадите о преступниках, тем больше вероятность, что полицейские найдут нарушителей.

Расскажите о действиях мошенников и в своем банке. Деньги банк вам не вернет, поскольку вы их перевели добровольно, но ваше обращение может помочь другим людям не стать жертвами аферистов. Чем больше жалоб поступит на счет мошенника, тем быстрее их реквизиты окажутся в специальной базе Банка России, к которой имеют доступ все банки.

**Как защитить себя от мошенничества**

* Не сообщайте никому паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Тем более нельзя публиковать такие сведения в интернете.
* Не храните данные карт и ПИН-коды на компьютере или в смартфоне.
* Покупки в интернете стоит делать только на проверенных сайтах. И лучше завести для этого отдельную карту, которая будет пополняться исключительно на сумму покупки. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).
* По возможности установите антивирус на все устройства и обновляйте его.
* Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах («Яндекс», Mail.ru) помечены цветным кружком с галочкой.
* Если с неизвестного номера звонит якобы сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или запугиваниями с требованием каких-либо быстрых действий, положите трубку. Самостоятельно позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.
* Не совершайте каких-либо действий по счету, если звонят с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет Центробанка, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с обычными гражданами, его клиенты — коммерческие банки.
* Делиться QR-кодом, который по сути является поручением банку на выдачу денег без ввода ПИН-кода, нельзя ни с кем. Сам QR-код тоже не стоит хранить на телефоне или в распечатанном виде.

**Что делать, если стал жертвой мошенника**

Если вы стали жертвой мошенников, необходимо срочно обратиться в банк по телефону (номер горячей линии банка указан на обратной стороне карты) или через официальное мобильное приложение и заблокировать карту.

Не позднее дня, следующего за днем поступления информации о совершении подозрительной операции, подайте в банк заявление о несогласии с операцией. Банк проверит сообщали ли вы ПИН-код, код безопасности или срок действия карты посторонним. Если вы нарушили правила безопасности, банк не компенсирует потери.

Подайте заявление в полицию. Чем быстрее вы это сделаете, тем выше вероятность того, что преступников найдут и привлекут к ответственности, поэтому выберите самый быстрый в вашем случае способ.

Вы можете подать заявление:

* по телефону 102 или 112;
* с помощью специальной формы на официальном [сайте](https://xn--b1aew.xn--p1ai/request_main) МВД России;
* в ближайшем [отделении полиции](https://77.xn--b1aew.xn--p1ai/Kontakti) по месту жительства.

Автор: Васько Галина Борисовна