Профилактика

Борьба с интернет-аферистами

Как сообщает сайт Объясняем.РФ, государственным органам, банкам и операторам запретят общаться с клиентами через мессенджеры.

Предполагается, что в скором времени информационные технологии защитят россиян от кибермошенников. По поручению правительства Минцифры вместе с Банком России и правоохранительными органами разработан пакет законопроектов для борьбы с телефонными и интернет-аферистами.

– Мы детально проанализировали наиболее распространённые мошеннические схемы, включая обман через звонки и сообщения, взломы личных кабинетов и оформление кредитов на чужие паспорта. На основе этого анализа разработаны меры для защиты граждан от таких угроз. В результате гражданам станет доступен широкий набор инструментов, который поможет им обезопасить себя от телефонного и интернет-мошенничества, – сообщают в правительстве РФ.

Комплексный план действий включает около 30 мер. Благодаря им:

– россияне смогут удалённо запретить оформлять кредиты и займы онлайн на своё имя – через портал госуслуг или банковские приложения. Снять это ограничение можно будет лично в МФЦ или отделении банка;

– кредитные организации будут тщательнее проверять заёмщиков: анализировать кредитную историю и банковский счёт, на который переводят деньги;

– если человек изменил данные, например, номер телефона, или его персональная информация «утекла» в интернет, будет срабатывать временная «заморозка» на выдачу займов онлайн;

– госорганы, банки и цифровые платформы смогут обмениваться информацией онлайн. Это позволит моментально выявлять подозрительные действия, блокировать их и сообщать о потенциальных преступлениях в правоохранительные органы;

– появятся новые обязательные правила по идентификации и проверке личности пользователей;

– введут обязательную маркировку звонков: на экране телефона будет отображаться название организации, из которой вам звонят. Так человек сможет понять, кто с ним пытается связаться – банк или мошенник;

– госорганам, банкам и операторам запретят общаться с клиентами через мессенджеры. Все официальные уведомления будут приходить только через проверенные каналы связи.



Не паниковать и быстро действовать

Инструкция. Что нужно делать, если вы перевели деньги мошенникам

К сожалению, стать жертвой обмана может любой – и неопытный человек, и специалист в банковской сфере. Разбираемся с экспертами, как быть, если человек перевёл деньги мошенникам. Реально ли вернуть средства и куда обратиться за помощью?



Обязанности банка

Кибермошенники очень изобретательны и придумывают всё новые способы похищения средств у доверчивых граждан. Чтобы нечистым на руку людям было труднее добраться до ваших сбережений, в банках работает антифрод (от английского выражения anti-fraud – борьба с мошенничеством). Это система мер, направленная на предотвращение сомнительных транзакций. Рассказываем, как обычно происходит возврат средств, что нужно сделать пострадавшему и велики ли шансы на успех.

Но сначала давайте разберёмся, по каким признакам банк (служба безопасности) считает перевод сомнительным:

• если деньги переведены на счёт, которым владеет лицо из базы дропперов (Дропперы – это люди, которые, используя свои банковские счета или карты, помогают мошенникам обналичивать деньги или скрывать их следы. Владельцы, так сказать, «безопасных счетов». Потом эти деньги проходят через цепочку переводов и впоследствии обналичиваются);

• если перевод сделан с устройства, уже использованного мошенниками;

• если необычная для клиента сумма или частота переводов, подозрительное место отправки или используемое устройство;

• если по данным операторов связи, накануне отправитель получал подозрительные сообщения или звонки.

Банк обязан возместить ущерб, если:

• перевод сделан получателю, связанному с мошенничеством, а клиент не получил уведомление о рисках;

• если банк не задержал операцию на два дня;

• перевод был сделан после того, как клиент уведомил банк об утере личных данных или потере карты.

Банк не должен возмещать ущерб, если выполнены все требования безопасности, подозрительный перевод был задержан на 2 дня, клиент получил уведомления о рисках, но сам принял решение о переводе.

Сроки возврата средств: для банков – 30 дней при переводе внутри страны, при переводе за рубеж – 60 дней.

Обязанности банка-получателя мошеннического перевода – свериться с базой данных дропперов и прекратить банковское обслуживание мошенников.

Не верьте обещаниям

Как вернуть деньги, которые вы перевели мошенникам? Специалисты рекомендуют не паниковать и действовать быстро. Алгоритм действий зависит от обстоятельств, суммы ущерба и времени совершения мошенничества.

Срочно свяжитесь с вашим банком! Заблокируйте карту или учётную запись в онлайн-банке, попробуйте отменить транзакцию. Ваш банк в срочном порядке свяжется с банком-получателем и попросит заблокировать счёт подозрительного лица. Если вы среагировали в течение суток, есть шанс, что деньги вернут.

Напишите заявление в правоохранительные органы. Заявление о мошенническом переводе можно подать в отделение полиции по месту жительства или на сайте МВД. К заявлению обычно просят приложить выписку о движении средств на карте и счёте, которую делают в банке. Чем больше подробностей о случившемся вы опишите, тем выше вероятность, что правоохранительные органы отыщут преступника.

Составьте иск в суд. При сумме ущерба до 50 тысяч рублей иск будут рассматривать в мировом суде, а свыше 50 тысяч – в районном. Если сумма значительная, стоит обратиться в прокуратуру. В этом случае заявление подают лично или отправляют заказным письмом. Как показывает практика, рассмотрение дела о мошеннических схемах не бывает быстрым. Разбирательство может занять от двух месяцев до нескольких лет.

При массовом мошенничестве – найдите других пострадавших. В случае массового обмана через социальные сети и тематические форумы поищите других жертв мошенничества. Коллективный иск обычно привлекает больше внимания и помогает снизить расходы на юридическое сопровождение.

Желательно сообщить о случившемся в ЦБ. Такое обращение может помочь в расследовании, особенно, если вас обманула компания. Тогда регулятор проведёт проверку и отправит результаты следователям.

Помните, дропперы всегда делают расчёт на панику. Если вы заподозрили обман, не верьте их обещаниям вернуть деньги, это очередная попытка обмана. Сохраняйте спокойствие и действуйте последовательно. Имейте в виду, если вы сами поделились с мошенниками личной информацией – данными своей карты, счёта, паролем, ПИН-кодом, или заметили пропажу денег со счёта не сразу, а спустя некоторое время, шанс вернуть деньги невелик.

Федеральным законом от 24.07.2023 № 369-ФЗ добавляется ряд превентивных мер, направленных на недопущение перевода денег гражданина злоумышленникам. В частности, банк отправителя должен проверить операцию на наличие согласия клиента, и если оно есть, то определить, не получено ли оно под влиянием обмана, и приостановить исполнение распоряжения клиента вплоть до отказа в переводе. Новый закон также устанавливает критерии анализа операции: нужно учесть и бэкграунд действий клиента, и изучить базы данных о попытках мошенничества. При этом банк должен уведомить обо всём клиента, дать рекомендации, как не допустить подобного в будущем, а также переспросить, точно ли совершать операцию. Закон даёт гражданам два дня на подтверждение, что выглядит разумным.

Законом предусмотрена двойная проверка – операцию проверяет не только банк отправителя, но и банк получателя. Эффективность такой двойной заслонки вызывает вопросы – насколько ценной и новой будет информация от принимающей стороны и как именно ее использовать...

Не забыть про чёрный список

При каких условиях банк вернёт деньги, если сам перевёл их мошенникам?

Со вступлением в силу с 25.07.2024 ФЗ № 369 «О внесении изменений в Федеральный закон «О национальной платёжной системе», банк обязан возвратить деньги клиенту, если платёж был осуществлен на получателя, находящегося в «чёрном списке» ЦБ РФ. Для этого нужно, чтобы перевод соответствовал определённым критериям:

• платёж был проведен при наличии информации о хищении (утрате) электронного средства платежа клиентом.

Какие переводы банк может посчитать подозрительными и заблокирует?

Подозрительными переводами могут считаться:

• платежи на получателя из чёрного списка ЦБ РФ;

• платежи, проведённые с устройства, параметры которого не совпадают с устройствами, обычно используемыми клиентом;

• платёж на получателя, в отношении которого имеется информация о возбуждённом уголовном деле;

• платёж при наличии информации от сторонних организаций о мошеннической операции;

• несоответствие характера, параметров и объёма проводимой операции, то есть учитывается накопленная статистика по ранее осуществлённым платежам клиента, которая анализируется и обрабатывается по определенным алгоритмам, используемым в банке.

Когда банк обязан вернуть деньги, которые перевели мошенникам?

Возврат обязателен, если платеж был осуществлён на получателя, находящегося в «чёрном списке» ЦБ РФ.

• клиент не дал подтверждения перевода;

• нарушен «период охлаждения», составляющий два дня с момента подтверждения операции;

▸ Комментарии

Иван ЛАЗАРЕВ, руководитель антифрод-системы, управление безопасности и взыскания задолженности, ПАО «Норвик Банк»:

«Первое, что нужно сделать для возврата средств, если есть подозрение о перечислении мошенникам, уведомить банк о перечислении денежных средств с расчётного счёта без добровольного согласия, либо под действием обмана. Банки по межбанковским каналам могут взаимодействовать между собой, есть возможность приостановить дальнейшее перечисление денежных средств. После оповещения банка, клиенту нужно обратиться в правоохранительные органы. Они проведут по заявлению проверку, возбудят уголовное дело и, возможно, наложат арест на денежные средства, находящиеся на счёте злоумышленника. Также можно вернуть денежные средства в рамках гражданско-правового законодательства: обратиться в суд с иском о неосновательном обогащении в отношении лица, на чьё имя открыт банковский счёт, с ходатайством о принятии обеспечительных мер по иску.

Евгения БОДНАР, юрист по банкротству физических лиц компании «Финансово-правовой альянс»:

«К сожалению, мошенникам до сих пор удаётся убедить потенциальную жертву самостоятельно передавать конфиденциальную информацию, например, о реквизитах карты или счёта, однако не всегда именно они являются целью. Ещё одна задача – убедить клиента в том, что он должен перевести деньги самостоятельно. Аферисты вводят жертв в заблуждение, играют на человеческих слабостях, они умеют правильно выстроить диалог и надавить на самые чувствительные места. Схем и приёмов множество, а в их сети всё чаще попадают не только доверчивые обыватели всех возрастов, но и вполне осведомлённые и даже юридически подкованные граждане. «Секрет успеха» преступников – в одновременном использовании современных технологий и психологических манипуляционных методов, в том числе элементов нейролингвистического программирования. Отметим, что, увы, раскрываемость подобного рода преступлений оставляет желать лучшего: мошенники идут на разнообразные ухищрения, чтобы не попасться правоохранителям.

Пока механизм по возврату средств банками только набирает обороты, а значит вернуть украденные деньги сложно. Даже если дело доходит до суда, он не всегда встаёт на сторону жертв мошенничества, ведь потерпевший сам подтверждал операции по своему счёту. В случае если человек уже пострадал от подобного обмана, необходимо обратиться в правоохранительные органы, как и при любом другом мошенничестве.

На заметку



Следственный комитет предостерегает граждан от действий телефонных мошенников

По всей стране продолжают фиксироваться случаи телефонного мошенничества. Граждане сообщают о противоправных действиях со стороны лиц, которые представляются сотрудниками правоохранительных органов, банков и склоняют переводить им деньги.

Одним из видов мошенничества являются случаи, когда абонентам звонят якобы сотрудники Следственного комитета России. Они сообщают о наличии возбужденных уголовных дел и даже присылают в мессенджеры копии поддельных процессуальных документов, пытаясь запугать человека и заставить поверить в происходящее. Для прекращения «уголовного преследования» мошенники требуют перевести им денежные средства.

Другая мошенническая схема связана с попыткой убедить человека, что в рамках расследуемого уголовного дела выяснился факт использования его персональных данных злоумышленниками и поэтому деньги нужно срочно перевести на «безопасный счёт».

Зачастую мошенники представляются высокопоставленными сотрудниками Следственного комитета, в том числе руководителями главных следственных и следственных управлений. Они агрессивно и грубо обшаются с абонентом, пытаясь оказать на него эмоциональное воздействие, запугать и заставить нервничать. Кроме того, мошенники используют должности и фамилии сотрудников ведомства, которые нередко выступают по телевидению с комментариями по уголовным делам.

Следственный комитет России призывает граждан быть бдительными и не дать себя обмануть. Для этого достаточно помнить ряд простых рекомендаций:

Следователи СК России дистанционно не совершают никаких процессуальных действий. Допрос и опрос граждан сотрудниками правоохранительных органов посредством телефонной связи не предусмотрены нормами закона.

Для проведения следственных действий граждане не вызываются повесткой или телефонограммой к следователю. При этом адрес расположения следственного органа можно проверить на официальном сайте.

Должностное лицо не имеет права требовать предоставления информации по счетам и картам, а также кодов из смс. Ни по телефону, ни в ходе очной беседы сотрудники СК России не заявляют требований о переводе денежных средств на какие-либо счета.

Любые предложения о содействии правоохранительным органам, например, в поимке преступников путем перечисления денежных средств на указанные «собеседником» счета либо с целью обезопасить сбережения от противоправных действий третьих лиц – явный признак мошенничества.

Следует помнить, что в случае, когда потерпевший сообщает злоумышленнику о том, что сам перезвонит в государственные органы и финансовые организации для уточнения всей информации по данному вопросу, он может натолкнуться на провокации. Мошенники зачастую путём угроз и недостоверной информации пытаются убедить абонента не делать этого, поскольку якобы может произойти «разглашение определённых сведений, за что действующим законодательством предусмотрена ответственность».

Данные заявления не являются правомерными и рассчитаны на запугивание абонента, чтобы он отказался проверить поступившую информацию и достоверность документов.

Ещё раз обращаем внимание граждан: не поддавайтесь уговорам, угрозам и влиянию телефонных мошенников. Незамедлительно сообщайте о таких фактах в правоохранительные органы.