ПРОКУРАТУРА ИРКУТСКОГО РАЙОНА РАЗЪЯСНЯЕТ:

КАК НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА: ПРОСТЫЕ ПРАВИЛА И ЧТО ДЕЛАТЬ, ЕСЛИ УЖЕ ОБМАНУЛИ

Телефонное мошенничество остаётся одной из самых распространённых угроз: люди добровольно переводят деньги злоумышленникам, поверив в убедительную легенду.

Мошенники действуют по отработанной схеме. Сначала они собирают данные о человеке — могут знать имя, последние цифры карты или даже паспортные данные за счёт утечек. Это создаёт иллюзию достоверности: кажется, что звонит действительно представитель банка или госоргана. Затем злоумышленник выдаёт себя за сотрудника «службы безопасности», следователя, оператора связи или специалиста Госуслуг.

Следующий шаг — изоляция жертвы: «никому не говорите, это секретное расследование». Дальше идёт давление: «деньги уйдут через 10 минут», «на вас оформляют кредит», «ваш родственник попал в беду». Паника отключает критическое мышление, и человек совершает действия, которые приводят к потере денег: называет код из СМС, переводит средства на «безопасный счёт», устанавливает вредоносное приложение или включает демонстрацию экрана. Среди популярных схем 2026 года — звонки о «взломе Госуслуг», «продлении симкарты», а также использование голосовых дипфейков и вредоносных APKфайлов.

Распознать мошенника можно по нескольким характерным признакам. Если собеседник просит код из СМС, пароль или CVV-код — это точно мошенник: ни банк, ни полиция, ни Госуслуги никогда не запрашивают такие данные. Требование перевести деньги на «безопасный счёт» или в криптовалюту — ещё один однозначный признак обмана: безопасных счетов не существует. Опасным сигналом является просьба установить приложение или включить демонстрацию экрана — так злоумышленники получают доступ к банковским приложениям и СМС-кодам.

Наконец, если звонок поступает через мессенджер и на экране виден логотип банка или полиции — это почти наверняка обман: официальные организации не используют мессенджеры для таких звонков. Самый надёжный способ проверить собеседника — положить трубку и самостоятельно перезвонить в организацию по официальному номеру.

Чтобы не стать жертвой, стоит заранее принять несколько мер.

С 1 марта 2025 года можно оформить самозапрет на кредиты через Госуслуги (с сентября — также через МФЦ). Снять такой запрет получится только лично или с электронной подписью «Госключ», поэтому даже при взломе аккаунта мошенники не смогут оформить на вас заём.

С 1 сентября 2025 года вводится период охлаждения по кредитам: деньги по займам от 50 до 200 тысяч рублей выдают не раньше чем через 4 часа, а свыше 200 тысяч — через 48 часов. Этого времени обычно хватает, чтобы опомниться и не поддаться на уговоры.

Полезно также установить запрет на сделки с недвижимостью без личного участия — его можно оформить в МФЦ или через Госуслуги. В личном кабинете Госуслуг стоит проверить список симкарт, зарегистрированных на ваше имя, и везде включить двухфакторную аутентификацию. Для дополнительной защиты можно подключить сервис «вторая рука»: по договорённости с банком доверенное лицо будет получать уведомления о крупных переводах — это особенно актуально для пожилых родственников.

Если деньги уже переведены мошенникам, действовать нужно максимально быстро: у злоумышленников есть примерно 30 минут, чтобы вывести средства через цепочку счетов. Первым делом следует немедленно позвонить в банк по номеру, указанному на карте или в приложении, сообщить о мошенничестве и попросить заблокировать карты, а также попытаться приостановить перевод — если транзакция ещё не завершена, её реально остановить. Затем нужно заблокировать номер мошенника и сообщить о нём своему оператору связи. После этого обязательно написать заявление в полицию — лично в отделении или онлайн на сайте МВД. К заявлению стоит приложить скриншоты переписки, выписку по счёту и номера телефонов, с которых поступали звонки. Важно получить талон уведомление о приёме заявления. Параллельно следует подать письменную претензию в банк и приложить к ней копию заявления в полицию.

По закону № 161-ФЗ «О национальной платёжной системе» банки обязаны проверять переводы на признаки мошенничества и могут приостанавливать подозрительные операции на два дня — это так называемый период охлаждения, в течение которого клиент может отказаться от перевода. Банк обязан возместить ущерб, если получатель уже числился в базе мошеннических счетов ЦБ, а банк не предупредил клиента и не задержал операцию; если клиент сообщил об утере карты или о мошенниках, а банк всё равно провёл перевод; либо если банк нарушил период охлаждения. Срок возврата составляет 30 дней для внутренних переводов и 60 дней для международных. Однако если человек сам продиктовал код из СМС после предупреждения банка, прямой возврат от банка невозможен — в этом случае остаётся рассчитывать на работу полиции и последующее взыскание ущерба через суд.

Если банк отказал в возврате средств, нужно запросить письменный мотивированный отказ — он понадобится как доказательство. Далее следует направить досудебную претензию на юридический адрес банка. При ущербе до 500 тысяч рублей перед обращением в суд обязательно нужно обратиться к финансовому уполномоченному — его решение имеет силу судебного акта. Также можно подать жалобу в Банк России через интернетприёмную. Если эти меры не помогли, остаётся подать иск в суд — либо к банку за ненадлежащее оказание услуги (включая неустойку и компенсацию морального вреда), либо к получателю денег по иску о неосновательном обогащении.