

Тема: «Актуальные способы совершения мошенничеств в отношении граждан и меры по их предупреждению»

Уважаемые участники!

Сегодня мы поговорим о теме, которая касается практически каждого: о современных способах мошенничества и о том, как не стать потерпевшим.

Сразу хочу обратить внимание: современные мошенничества – это уже не только история про пожилого человека, которому позвонили по телефону. Это проблема, с которой сталкиваются люди разных возрастов, разных профессий, с разным уровнем образования и разным опытом пользования интернетом. Мошенники работают не только с теми, кто плохо разбирается в технологиях. Очень часто они обманывают активных пользователей смартфонов, банковских приложений, социальных сетей, интернет-магазинов и мессенджеров.

Главный расчет мошенника – не на то, что человек ничего не знает. Главный расчет – на эмоции: страх, спешку, доверие, желание помочь, желание заработать, купить дешевле, получить выгоду, избежать неприятностей или сохранить свои деньги.

По имеющимся аналитическим сведениям, только в мае 2026 года было учтено 2 347 инцидентов, связанных с мошенническими операциями. Общая сумма ущерба составила более 3,5 миллиона рублей. За январь–май 2026 года количество таких инцидентов составило почти 12 тысяч, а сумма ущерба превысила 19 миллионов рублей.

Это означает, что мошенничества – не редкость и не исключение. Это ежедневная реальность. Каждый день преступники звонят, пишут, создают поддельные сайты, используют мессенджеры, социальные сети, торговые площадки, банковские переводы, криптовалюту, подставные счета и чужие банковские карты.

Важно понять одну простую вещь: в большинстве случаев мошенник не взламывает телефон, не вскрывает квартиру и не получает доступ к деньгам силой. Он делает так, чтобы человек сам выполнил нужное действие: сообщил код, перешел по ссылке, ввел данные карты, оформил кредит, перевел деньги, установил приложение или передал доступ к аккаунту.

Поэтому главная защита – не только антивирус, пароль или сложные технические настройки. Главная защита – умение вовремя распознать ситуацию, остановиться и не выполнять указания неизвестного человека.

Сегодня мы разберем основные способы мошенничества, которые сейчас наиболее актуальны: звонки от имени банков и должностных

лиц, обман при покупках в интернете, фишинговые ссылки, мошенничества в социальных сетях, инвестиционные схемы, обман при аренде жилья, вымогательство и вовлечение граждан в движение похищенных денег.

Начнем с наиболее опасного способа – **звонков и сообщений от имени должностных лиц**.

Этот способ часто называют **вишингом**. Проще говоря, это мошенничество через телефонный разговор или голосовое общение в мессенджере. Вам может позвонить человек, который представится сотрудником банка, милиции, следственного органа, службы безопасности, оператора связи, Национального банка, прокуратуры или другой организации.

Сценарии могут быть разными, но смысл почти всегда один: вас пытаются напугать и заставить действовать быстро.

Например, вам говорят: «На ваше имя пытаются оформить кредит». Или: «С вашего счета пытаются похитить деньги». Или: «Ваши данные попали к преступникам». Или: «По вашей карте проходят подозрительные операции». Или: «Вы проходите по делу, необходимо срочно помочь следствию». Или: «Нельзя никому рассказывать, идет секретная операция».

После этого мошенник начинает руководить вашими действиями. Он может попросить назвать код из SMS, установить приложение, зайти в банковское приложение, оформить кредит, снять деньги, перевести их на «безопасный счет», передать деньги курьеру, купить криптовалюту или включить демонстрацию экрана.

Самое важное правило: никаких «безопасных счетов» для граждан, на которые нужно срочно переводить деньги по указанию звонящего, не существует.

Если вам говорят перевести деньги на «безопасный», «резервный», «защищенный», «специальный» или «транзитный» счет – это мошенничество.

Если вам говорят оформить кредит, чтобы якобы не дать мошенникам оформить кредит на вас, – это мошенничество.

Если вам говорят не класть трубку, не звонить родственникам, не обращаться в банк, не идти в милицию и никому ничего не рассказывать, – это мошенничество.

Если вам говорят, что вы участвуете в секретной операции, и поэтому должны выполнять указания по телефону, – это мошенничество.

Ни сотрудник банка, ни сотрудник милиции, ни следователь, ни прокурор, ни работник Национального банка не будет требовать у гражданина сообщить код из SMS, перевести деньги на другой счет,

оформить кредит по телефону или установить приложение удаленного доступа.

Отдельно нужно сказать про коды из SMS и push-уведомления. Код подтверждения – это фактически ключ к операции. Когда вы называете код, вы можете подтверждать перевод, вход в личный кабинет, изменение настроек, оформление услуги или другое действие. Мошенник может говорить: «Это код отмены операции», «Это код безопасности», «Это код регистрации заявления», «Это код для проверки». Но если код пришел вам от банка или сервиса, его нельзя сообщать никому.

Еще один опасный прием – установка приложений. Мошенники могут убеждать установить программу для защиты телефона, проверки счета, видеосвязи, помощи сотруднику банка или удаленной консультации. На самом деле это может быть приложение удаленного доступа. Через него преступник видит экран телефона, получает возможность подсказывать действия или фактически контролировать устройство.

Поэтому правило простое: если неизвестный человек по телефону просит установить приложение, включить демонстрацию экрана, зайти в банковское приложение или выполнить финансовую операцию – разговор нужно прекратить.

Что делать в такой ситуации?

Первое – положить трубку. Не спорить, не доказывать, не пытаться переиграть мошенника. Просто завершить разговор.

Второе – самостоятельно перезвонить в банк по номеру, указанному на официальном сайте, на банковской карте или в официальном приложении. Не по номеру, который продиктовал звонящий.

Третье – если вам угрожали уголовным делом, проверкой, ответственностью или требовали срочно совершить действия, можно обратиться по телефону 102 либо лично в ближайший орган внутренних дел.

Четвертое – предупредить близких. Особенно пожилых родителей, детей, супругов, коллег. Очень часто мошенники продолжают звонить другим людям из окружения.

Теперь перейдем к **мошенничествам при покупке товаров в интернете.**

Это один из самых распространенных способов обмана. Человек находит товар на торговой площадке, в социальной сети, в мессенджере, в группе объявлений или на сайте. Это может быть одежда, обувь, телефон, техника, мебель, автозапчасти, бытовые товары, детские вещи, билеты, животные, строительные материалы – фактически что угодно.

Обычно мошенник создает привлекательные условия. Цена ниже рыночной. Фотографии хорошие. Описание убедительное. Продавец отвечает быстро. Может говорить, что товар почти новый, срочно продается, много желающих, нужно внести предоплату, чтобы он никому другому его не отдал.

Именно на этом этапе многие теряют осторожность. Человек думает: «Сумма небольшая», «Выгодное предложение», «Не хочу упустить», «Продавец вроде нормальный», «Он даже скинул фото паспорта», «У него есть отзывы». Но все это может быть частью схемы.

Основные признаки опасности при покупке онлайн:

- продавец требует предоплату на карту физического лица;
- продавец торопит и говорит, что товар заберет кто-то другой;
- продавец отказывается от безопасной сделки на площадке;
- продавец просит перейти по ссылке для оплаты или доставки;
- продавец предлагает продолжить общение в другом мессенджере;
- аккаунт новый, с малым количеством информации;
- цена заметно ниже обычной;
- условия слишком выгодные;
- продавец избегает личной встречи или проверки товара.

Особенно часто используется схема с доставкой. Вам могут сказать: «Я оформлю доставку, вот ссылка для оплаты». Или наоборот: «Я покупатель, хочу оплатить ваш товар через доставку, перейдите по ссылке и получите деньги». Ссылка может выглядеть похожей на настоящую страницу почты, службы доставки или торговой площадки.

На такой странице вас просят ввести данные банковской карты: номер, срок действия, CVV-код, имя держателя, а потом еще и код из SMS. При этом человеку могут объяснять: «Это нужно для получения денег», «Это подтверждение доставки», «Это безопасная сделка», «Это возврат», «Это проверка карты».

Нужно запомнить: для получения денег на карту не нужно вводить CVV-код и подтверждать операцию кодом из SMS. Если вы вводите полный набор реквизитов карты и подтверждаете действие кодом, вы можете не получать деньги, а подтверждать списание.

Если вы покупаете товар, безопаснее пользоваться официальными механизмами площадки, проверять историю продавца, отзывы, дату создания аккаунта, не переводить предоплату неизвестным лицам и не переходить по платежным ссылкам из переписки.

Если вы продаете товар, также будьте осторожны. Мошенники часто представляются покупателями. Они говорят: «Я уже оплатил через доставку», «Получите деньги по ссылке», «Нужно подтвердить карту», «Вам придет код, продиктуйте его курьеру». Это тоже обман.

Правило для покупателя и продавца одно: все действия по оплате и доставке выполняются только через официальный сайт или официальное приложение сервиса. Не через ссылку, которую прислали в личном сообщении.

Следующий важный способ – **фишинг**.

Фишинг – это использование поддельных сайтов, страниц, сообщений и форм, которые имитируют настоящие сервисы. Внешне страница может быть очень похожа на официальный сайт банка, службы доставки, государственной организации, торговой площадки, почтового сервиса или социальной сети. На ней могут быть логотипы, цвета, знакомые кнопки, текст на русском языке, даже значок защищенного соединения.

Но цель такой страницы – похитить ваши данные или заставить вас подтвердить операцию.

Фишинговые ссылки могут приходить через SMS, электронную почту, Viber, Telegram, WhatsApp, социальные сети, комментарии, рекламные объявления. Темы бывают разными: оплата штрафа, доставка посылки, получение перевода, возврат денег, подтверждение аккаунта, голосование, выигрыш, акция, проверка безопасности, отмена списания, получение выплаты, продажа товара.

Например, человеку приходит сообщение: «У вас неоплаченный штраф. Оплатите по ссылке». Или: «Ваша посылка задержана, оплатите доставку». Или: «Покупатель оплатил товар, получите деньги». Или: «Ваш аккаунт будет заблокирован, подтвердите данные». Или: «Вы выиграли приз, заполните форму».

В таких ситуациях нельзя оценивать сайт только по внешнему виду. Мошенники умеют копировать дизайн. Нужно смотреть на адрес сайта. Поддельный домен может отличаться одной буквой, лишним дефисом, цифрой, странной доменной зоной, дополнительным словом или переставленными символами.

Важно понимать: значок замка в браузере и наличие HTTPS не доказывают, что сайт официальный. Это означает только то, что соединение с этим сайтом зашифровано. Мошеннический сайт тоже может открываться с замком. Поэтому главное – не замок, а правильный официальный адрес.

Лучшее правило против фишинга: не открывать платежные и учетные ссылки из сообщений. Если вам нужно оплатить штраф, проверить доставку, зайти в банк, получить услугу или проверить аккаунт – откройте официальный сайт самостоятельно или используйте официальное приложение.

Если вы получили ссылку от знакомого, это тоже не гарантия безопасности. Его аккаунт могли взломать. Особенно если сообщение

выглядит необычно: «Проголосуй за меня», «Посмотри фото», «Получи подарок», «Мне срочно нужна помощь», «Перейди и подтверди».

Если после перехода по ссылке у вас просят ввести логин, пароль, данные карты, CVV-код или код из SMS – остановитесь. Сначала проверьте, куда вы попали.

Следующий способ – **мошенничества в социальных сетях и мессенджерах.**

Здесь преступники используют доверие. Социальная сеть – это среда, где мы общаемся с друзьями, родственниками, знакомыми, коллегами. Поэтому сообщение от знакомого человека воспринимается иначе, чем звонок от неизвестного номера.

Одна из распространенных схем – просьба о переводе денег от имени знакомого. Вам пишет друг, родственник или коллега: «Срочно нужны деньги», «Переведи до вечера», «Проблемы с картой», «Потом верну», «Не могу сейчас звонить». Аккаунт может быть взломан, либо мошенник может создать похожий профиль с фотографией и именем знакомого.

Если вы получили просьбу о деньгах через мессенджер или социальную сеть, обязательно перепроверьте ее по другому каналу связи. Не пишите в тот же чат: «Это точно ты?» Если аккаунт взломан, вам ответит мошенник. Позвоните человеку по известному вам номеру, задайте вопрос, ответ на который знает только он, свяжитесь через другой канал.

Еще одна схема – фейковые сборы денег. Например, якобы на лечение, помощь пострадавшему, благотворительность, срочную операцию, поддержку семьи. Сами по себе благотворительные сборы могут быть настоящими, но мошенники активно используют сострадание людей. Поэтому перед переводом денег нужно проверять источник: кто организатор, есть ли официальные реквизиты, подтверждающие документы, известна ли организация, публикуются ли отчеты.

Также распространены схемы с конкурсами, подарками и голосованиями. Вам может прийти сообщение: «Проголосуй за моего ребенка», «Поддержи в конкурсе», «Получи подарок», «Ты выиграл». После перехода по ссылке вас просят авторизоваться через социальную сеть или мессенджер. В результате мошенники получают доступ к аккаунту и начинают рассылать сообщения уже от вашего имени.

Чтобы защитить аккаунты, используйте двухфакторную аутентификацию, сложные пароли, не вводите логины и пароли на страницах, открытых по ссылкам из сообщений, и не передавайте коды подтверждения.

Отдельно нужно поговорить о предложениях работы и быстрого заработка.

Мошенники часто обращаются к молодым людям, студентам, людям, которые ищут подработку или хотят заработать в интернете. Предложения звучат привлекательно: работа без опыта, свободный график, высокая оплата, простые задания, быстрый доход. Но затем появляются условия: оплатить регистрацию, обучение, страховку, доступ к платформе, доставку оборудования, оформление документов. После оплаты связь прекращается.

Есть и более опасный вариант. Человеку предлагают принимать деньги на свою карту и переводить их дальше, оформлять банковские карты, открывать счета, передавать реквизиты, регистрировать SIM-карты, создавать электронные кошельки или криптокошельки. Ему говорят, что это обычная работа: «оператор платежей», «помощник менеджера», «финансовый агент», «транзитный сотрудник», «курьер», «дроп», «арбитраж», «обработка заявок».

На самом деле такие действия могут быть связаны с движением похищенных денег. Человек может думать, что просто подрабатывает, но фактически его карта или счет используется в преступной схеме. Это может повлечь серьезные последствия.

Запомните: если работа заключается в том, чтобы принимать деньги от неизвестных лиц и переводить их дальше, передавать карту, счет, SIM-карту или доступ к банковскому приложению, – это не нормальная работа. Это признак противоправной схемы.

Нельзя передавать свою банковскую карту другим лицам. Нельзя продавать или сдавать в аренду банковские карты. Нельзя открывать счета по просьбе неизвестных лиц. Нельзя передавать логин, пароль, SMS-коды и доступ к банковскому приложению. Деньги, которые проходят через ваш счет, могут быть похищенными у других граждан.

Следующее направление – **инвестиционные мошенничества**.

Такие схемы часто выглядят убедительно. Человеку предлагают заработать на бирже, криптовалюте, акциях, валюте, нефти, золоте, международных рынках или инвестиционной платформе. Реклама обещает высокий доход, быстрый результат, помощь личного аналитика, обучение с нуля, гарантированную прибыль.

Сначала человеку предлагают внести небольшую сумму. Затем показывают в личном кабинете красивый график и якобы рост прибыли. Потерпевший видит, что баланс увеличивается, и начинает доверять. Ему звонит «аналитик», объясняет, какие сделки выгодные, советует внести больше денег. Потом человек пытается вывести прибыль, но ему говорят: «Нужно оплатить комиссию», «Нужно заплатить налог»,

«Нужно пройти верификацию», «Нужно внести страховой депозит», «Нужно разблокировать счет».

Это один из главных признаков инвестиционного мошенничества: чтобы вывести якобы заработанные деньги, от вас требуют внести еще деньги.

Нормальная инвестиционная деятельность не строится на переводах на карты физических лиц, личных сообщениях в мессенджере и обещании гарантированной прибыли. На финансовых рынках не бывает высокой доходности без риска. Если вам обещают быстрый доход без опыта, без риска и с гарантией – это повод остановиться.

Особенно осторожно нужно относиться к ситуациям, когда вам предлагают установить приложение, включить демонстрацию экрана, передать доступ к телефону, зарегистрироваться по ссылке, купить криптовалюту под руководством неизвестного человека или перевести деньги на иностранные реквизиты.

Перед любыми инвестициями задайте себе несколько вопросов. Вы понимаете, кому переводите деньги? Есть ли у организации лицензия? Есть ли официальный договор? На чье имя открыт счет получателя? Почему общение идет через мессенджер? Почему решение нужно принять срочно? Почему вам гарантируют прибыль? Почему для вывода денег нужно снова платить?

Если хотя бы на часть этих вопросов нет ясного ответа, деньги переводить нельзя.

Следующий распространенный способ – **обман при аренде жилья**.

Особенно часто с ним сталкиваются молодые люди, студенты, граждане, которые переезжают в другой город, ищут квартиру на короткий срок или хотят снять жилье по выгодной цене.

Схема обычно такая: размещается объявление с хорошими фотографиями, удобным расположением и привлекательной ценой. Когда человек пишет арендодателю, ему отвечают, что желающих много, квартира хорошая, нужно срочно внести задаток или бронь. Могут прислать паспорт, договор, видео квартиры, геолокацию, дополнительные фотографии. Все это создает видимость надежности.

После перевода денег объявление исчезает, телефон отключается, аккаунт удаляется.

Главное правило при аренде жилья: не переводить задаток до реальной проверки объекта и документов. Фотографии, переписка, сканы паспорта и договор в мессенджере не гарантируют, что квартира существует и что собеседник имеет право ее сдавать.

Если жилье нужно снять дистанционно, используйте проверенные сервисы, обращайте внимание на отзывы, историю аккаунта,

возможность официального оформления, не соглашайтесь на срочную оплату без проверки. Если цена заметно ниже рынка, это не всегда удача. Часто это приманка.

Теперь поговорим о **вымогательстве в интернете**.

Это особенно чувствительная тема, потому что потерпевшие часто испытывают стыд, страх и не хотят обращаться за помощью. Мошенники этим пользуются.

Один из вариантов – угрозы распространить интимные фотографии, видео или переписку. Человек знакомится в интернете, вступает в доверительное или интимное общение, отправляет материалы или участвует в видеочате. После этого ему начинают угрожать: «Заплати, иначе отправим всем твоим друзьям», «Разошлем родственникам», «Опубликуем на работе», «Сольем в интернет».

Иногда преступник действительно получил материалы. Иногда он только делает вид, что получил. Но в обоих случаях цель одна – заставить человека платить.

Важно знать: оплата не гарантирует, что требования прекратятся. Наоборот, если человек заплатил один раз, мошенник понимает, что на него можно давить дальше. Суммы могут расти, угрозы продолжаться.

Если вы столкнулись с такой ситуацией, не нужно оставаться один на один с преступником. Сохраните переписку, скриншоты, номера, ссылки, данные аккаунта, не удаляйте доказательства. Не переводите деньги. Обратитесь за помощью. Если ситуация касается несовершеннолетнего, очень важно, чтобы ребенок или подросток не боялся сказать взрослым. Задача родителей – не обвинить, а помочь.

Еще один опасный сценарий связан с учетными записями Apple ID, iCloud, Google и другими сервисами. Под предлогом вакансии, тестирования приложения, бесплатного получения товара, участия в акции или настройки телефона человека могут попросить ввести чужие учетные данные на своем устройстве. После этого устройство блокируется, а за разблокировку требуют деньги.

Нельзя вводить чужие учетные данные на своем телефоне. Нельзя передавать свои учетные данные другим лицам. Нельзя выполнять инструкции неизвестных людей, связанные с аккаунтами, облачными сервисами и настройками безопасности.

Теперь остановимся на том, почему мошенникам удастся убеждать людей.

Многие потерпевшие после случившегося говорят: «Я сам не понимаю, как поверил». Это важный момент. Мошенник не просто сообщает информацию. Он управляет состоянием человека.

Первый прием – срочность. Вам говорят, что решение нужно принять немедленно: деньги исчезнут, кредит оформят, аккаунт

заблокируют, товар уйдет другому покупателю, штраф увеличится, операция пройдет через несколько минут. Спешка мешает думать.

Второй прием – страх. Вас пугают потерей денег, уголовной ответственностью, проблемами с банком, родственниками, работой, публикацией личных данных.

Третий прием – авторитет. Мошенник представляется сотрудником банка, милиции, следователем, работником службы безопасности, специалистом технической поддержки. Он может говорить уверенно, использовать профессиональные слова, присылать поддельные документы и удостоверения.

Четвертый прием – секретность. Вам говорят никому не рассказывать. Это очень опасный признак. Настоящая помощь не требует изолировать человека от семьи, банка или правоохранительных органов.

Пятый прием – выгода. Дешевый товар, быстрый заработок, высокий доход, подарок, выигрыш, компенсация, выплата. Желание получить выгоду снижает критичность.

Шестой прием – доверие. Сообщение приходит от знакомого, продавец вежливый, «аналитик» долго общается, арендодатель присылает документы, покупатель кажется убедительным.

Как только в ситуации появляются срочность, страх, секретность, деньги и неизвестный собеседник – нужно остановиться.

Есть хорошее универсальное правило: сделать паузу. Не на час, не на день, а хотя бы на несколько минут. Положить трубку. Закрывать ссылку. Не вводить данные. Не подтверждать операцию. Позвонить близкому человеку. Позвонить в банк. Перепроверить информацию.

Мошенники боятся паузы, потому что во время паузы человек возвращает контроль над ситуацией.

Теперь поговорим о том, что делать, если вы уже сообщили данные или перевели деньги.

Первое – немедленно связаться с банком. Чем быстрее вы сообщите о мошеннической операции, тем выше шанс заблокировать карту, счет, личный кабинет или приостановить дальнейшие операции.

Второе – заблокировать карту или доступ к банковскому приложению, если есть риск компрометации.

Третье – сменить пароли от банковских, почтовых, социальных и иных аккаунтов, если вы вводили данные на подозрительном сайте.

Четвертое – сохранить все доказательства: номера телефонов, переписку, скриншоты, ссылки, чеки, квитанции, данные получателя, объявления, аккаунты, адреса сайтов.

Пятое – обратиться в органы внутренних дел. Не нужно думать, что сумма слишком маленькая или что «сам виноват». Обращение

важно не только для конкретного случая, но и для выявления связанных эпизодов, счетов, номеров, сайтов и иных элементов схемы.

Шестое – предупредить родственников и знакомых, если мошенники получили доступ к вашему аккаунту или контактам. Они могут начать писать от вашего имени.

Очень важно не пытаться «договориться» с мошенником. Не переводить дополнительные суммы за возврат денег, разблокировку, комиссию, налог, удаление материалов, отмену операции. Часто после первого платежа следует второй, третий и так далее.

Теперь несколько слов **о безопасности банковских карт и аккаунтов.**

Нельзя сообщать никому PIN-код, CVV-код, срок действия карты, коды из SMS, пароли, логины, одноразовые коды, данные для входа в интернет-банкинг. Даже если человек представляется сотрудником банка. Даже если он знает ваше имя. Даже если он называет часть номера карты. Даже если номер похож на официальный.

Карта – это не просто кусок пластика. Это доступ к деньгам. А банковское приложение – это фактически ваш финансовый кабинет. Если вы передаете доступ, вы передаете контроль.

Используйте отдельную карту для интернет-покупок, если есть такая возможность. Держите на ней ограниченную сумму. Устанавливайте лимиты на операции. Включайте уведомления о списаниях. Регулярно проверяйте операции. Не храните фотографии карты в мессенджерах и галерее. Не отправляйте реквизиты карты в переписке.

Для аккаунтов используйте разные пароли. Если один и тот же пароль стоит в почте, социальной сети, интернет-магазине и другом сервисе, взлом одного аккаунта может привести к доступу ко всем остальным. Включайте двухфакторную аутентификацию. Но помните: код двухфакторной аутентификации также нельзя никому сообщать.

Отдельно обращаюсь к родителям.

Дети и подростки могут стать потерпевшими в схемах с играми, скинами, подарками, голосованиями, конкурсами, подработкой, интимным вымогательством, фейковыми аккаунтами, покупками через интернет. Важно не только запрещать, но и объяснять. Ребенок должен знать, что если он ошибся, перешел по ссылке, отправил фото, сообщил код или столкнулся с угрозами, он может прийти к взрослым без страха наказания.

Мошенники часто удерживают подростков именно страхом: «Если расскажешь родителям, будет хуже». Поэтому дома должно быть правило: в сложной ситуации сначала обращаемся за помощью, а потом разбираемся.

Также обращаюсь к тем, у кого есть **пожилые родственники**.

Пожилым людям нужно не просто сказать: «Не разговаривай с мошенниками». Этого мало. Лучше заранее обсудить конкретные фразы: «На ваше имя оформляют кредит», «Ваш счет под угрозой», «Нужно перевести деньги на безопасный счет», «Идет секретная операция», «Не говорите родственникам». Нужно договориться: если поступает звонок о деньгах, кредитах, карте или уголовном деле – человек прекращает разговор и звонит родственнику.

Можно записать на бумаге и положить рядом с телефоном короткую памятку: «Коды не называю. Деньги не перевожу. Кредиты по телефону не оформляю. При подозрительном звонке звоню родственнику или в банк». Простые правила в стрессовой ситуации работают лучше, чем длинные объяснения.

Теперь давайте разберем **несколько типичных ситуаций**.

Ситуация первая. Вам звонят и говорят: «На вас оформляют кредит. Чтобы остановить операцию, нужно самому оформить встречный кредит и перевести деньги на безопасный счет». Правильное действие: положить трубку. Самостоятельно позвонить в банк. Никаких кредитов не оформлять. Никаких переводов не делать.

Ситуация вторая. Вам пишет знакомый: «Срочно переведи деньги, потом объясню». Правильное действие: позвонить этому знакомому по обычному номеру. Не переводить деньги, пока не убедитесь, что просьба настоящая.

Ситуация третья. Вы продаете товар, покупатель присылает ссылку: «Я оплатил доставку, получите деньги». Правильное действие: не переходить по ссылке из переписки. Проверить заказ только в официальном приложении или на официальном сайте площадки.

Ситуация четвертая. Вам приходит сообщение о штрафе или доставке. Есть ссылка на оплату. Правильное действие: не переходить по ссылке. Самостоятельно открыть официальный сайт соответствующего сервиса.

Ситуация пятая. Вам предлагают инвестировать, обещают высокий доход и личного аналитика. Деньги нужно перевести на карту физического лица или криптокошелек. Правильное действие: не переводить деньги. Проверить организацию, лицензию, договор, официальный сайт. Не принимать решение в телефонном разговоре.

Ситуация шестая. Вам угрожают публикацией личных материалов и требуют деньги. Правильное действие: не платить. Сохранить доказательства. Обратиться за помощью. Заблокировать контакт после фиксации данных.

Ситуация седьмая. Вам предлагают работу: принимать деньги на карту и переводить дальше за процент. Правильное действие: отказаться. Не передавать карту, счет, SIM-карту, логины и пароли.

Ситуация восьмая. Арендодатель просит срочно перевести задаток за квартиру, которую вы не видели. Правильное действие: не переводить деньги до проверки жилья и документов.

Теперь сформулируем основные правила, которые стоит запомнить каждому.

Первое. Не сообщайте коды из SMS и push-уведомлений никому и никогда.

Второе. Не переводите деньги по указанию человека, который сам вам позвонил или написал.

Третье. Не оформляйте кредиты под диктовку по телефону.

Четвертое. Не существует «безопасных счетов», на которые гражданин должен перевести свои деньги.

Пятое. Не устанавливайте приложения по просьбе неизвестных лиц.

Шестое. Не включайте демонстрацию экрана при разговоре с неизвестным человеком.

Седьмое. Не переходите по ссылкам для оплаты, доставки, получения денег или входа в аккаунт из сообщений.

Восьмое. Проверяйте просьбы о деньгах от знакомых через другой канал связи.

Девятое. Не переводите предоплату неизвестным продавцам на личные карты.

Десятое. Не передавайте свои банковские карты, счета, SIM-карты и аккаунты другим лицам.

Одиннадцатое. Не верьте обещаниям гарантированного высокого дохода.

Двенадцатое. При любом сомнении сделайте паузу и перепроверьте информацию.

Хочу подчеркнуть: жертвой мошенника может стать любой. Образование, возраст, профессия и опыт не дают стопроцентной защиты. Защищает не самоуверенность, а привычка проверять.

Мошенник часто звучит уверенно. Он может знать ваши фамилию, имя, номер телефона, адрес, банк, часть реквизитов, данные из утечек или открытых источников. Это не доказывает, что он сотрудник банка или государственного органа. Сегодня персональные данные могут попадать к преступникам разными путями. Поэтому нельзя доверять только потому, что звонящий что-то о вас знает.

Также нельзя доверять номеру телефона только потому, что он похож на официальный. Номера могут подменяться, а звонки могут

поступать через мессенджеры. Безопаснее завершить разговор и самостоятельно набрать официальный номер.

Не нужно бояться показаться невежливым. Если человек действительно сотрудник банка или организации, он поймет ваше желание перепроверить информацию. А если это мошенник, именно пауза разрушит его сценарий.

В завершение хочу сказать следующее.

Современные мошенничества построены на том, чтобы заставить человека действовать быстро, эмоционально и без проверки. Поэтому наша главная линия защиты – спокойствие, пауза и самостоятельная проверка.

Если вам звонят по поводу денег – остановитесь.

Если вас торопят – остановитесь.

Если вас пугают – остановитесь.

Если вам запрещают кому-либо рассказывать – остановитесь.

Если просят код – остановитесь.

Если дают ссылку для оплаты или получения денег – остановитесь.

Если обещают легкий заработок – остановитесь.

Если требуют предоплату без проверки – остановитесь.

Почти всегда нескольких минут достаточно, чтобы не потерять деньги.

Запомните простую формулу безопасного поведения: не сообщать, не переводить, не переходить, не устанавливать, не спешить, а проверять.

Если каждый из нас будет соблюдать эти правила и объяснит их своим близким, особенно детям и пожилым родственникам, количество успешных мошенничеств станет меньше. Преступники рассчитывают на нашу спешку и доверчивость. Наша задача – не дать им управлять нашими действиями.

Спасибо за внимание.