Антикоррупционное поведение граждан: как каждый может внести вклад

Антикоррупционное поведение — это осознанные действия граждан, которые препятствуют возникновению и распространению коррупции. Оно строится на уважении к закону, личной ответственности и готовности противостоять коррупционным проявлениям.

Что может сделать гражданин

Каждый человек может внести свой вклад в борьбу с коррупцией, следуя простым правилам:

- Не давать взяток. Даже «мелкие» суммы, переданные для ускорения процесса или получения услуги, являются преступлением и подпитывают систему коррупции.

- Знать свои права. Если чиновник требует незаконное вознаграждение, важно понимать, какие услуги должны оказываться бесплатно и в какие сроки.

- Фиксировать нарушения. При столкновении с вымогательством взятки стоит зафиксировать факт правонарушения (например, сохранить переписку, записать разговор, если это не нарушает закон), чтобы предоставить доказательства правоохранительным органам.

- Обращаться в компетентные органы. О фактах коррупции можно сообщить в полицию, прокуратуру или на специализированные горячие линии и онлайн-сервисы.

Использовать механизмы общественного контроля. Участвовать в обсуждениях законопроектов, следить за госзакупками и расходованием бюджетных средств — многие данные доступны в открытых источниках.

- Распространять знания. Рассказывать окружающим о последствиях коррупции и о том, как правильно действовать в коррупционно опасной ситуации.

Правовой основой является Федеральный закон № 273-ФЗ «О противодействии коррупции», который закрепляет сотрудничество государства с гражданами как одно из ключевых направлений борьбы с этим явлением. Кроме того, Уголовный кодекс РФ предусматривает ответственность как за получение, так и за дачу взятки (ст. 290 и ст. 291 УК РФ).

Если вам требуют взятку за услугу, важно действовать последовательно и в рамках закона.

Вот основные шаги, которые следует предпринять:

Как вести себя во время разговора

Сохраняйте спокойствие и вежливость. Не проявляйте агрессии, но и не демонстрируйте готовность дать взятку. Внимательно выслушайте и запомните условия. Постарайтесь зафиксировать в памяти или записать (если это возможно без риска для себя) детали: размер суммы, наименование товаров или услуг, сроки и способ передачи взятки, должность и имя вымогателя, гарантии, которые он обещает.

Не берите инициативу в разговоре на себя.

Позвольте собеседнику высказаться, чтобы он сообщил как можно больше информации. Постарайтесь отложить вопрос о времени и месте передачи взятки до следующей беседы или предложите хорошо знакомое вам место для следующей встречи.

Поинтересуйтесь о гарантиях решения вопроса в случае дачи взятки.

Что делать после разговора

Прекратите контакты с вымогателем. Дайте понять, что вы отказываетесь от дачи взятки.

Немедленно обратитесь в правоохранительные органы. Устные и письменные заявления о преступлениях принимаются круглосуточно, независимо от места и времени совершения преступления. Вы можете обратиться: в прокуратуру, в органы Следственного комитета РФ; в органы внутренних дел;в органы безопасности.

Если взятку требует сотрудник правоохранительных органов, можно обратиться в подразделение собственной безопасности его ведомства или к руководителю органа.

Составьте заявление. В нём нужно указать: ФИО, должность, учреждение вымогателя; сумму и характер требуемой взятки; за какие действия (или бездействие) требуют взятку; время, место и способ предполагаемой передачи взятки.

Вы имеете право получить копию заявления с отметкой о регистрации или талон-уведомление.

Участвуйте в оперативно-розыскных мероприятиях. Если правоохранительные органы начнут расследование, важно точно выполнять их указания.

Важные нюансы

Не выполняйте требования вымогателя.

Если вы дадите взятку и не сообщите об этом в правоохранительные органы, вас могут привлечь к уголовной ответственности, если факт взятки будет выявлен.

Фиксируйте доказательства (если это возможно и безопасно): сохраняйте переписку, записывайте разговор (с соблюдением законодательства о защите персональных данных).

Помните о защите. Если есть угроза жизни или здоровью, действуйте максимально осторожно. В таких случаях можно рассмотреть возможность обращения в правоохранительные органы с объяснением ситуации.

Правовой основой является Федеральный закон № 273-ФЗ «О противодействии коррупции», который закрепляет сотрудничество государства с гражданами как одно из ключевых направлений борьбы с этим явлением. Кроме того, Уголовный кодекс РФ предусматривает ответственность как за получение, так и за дачу взятки (ст. 290 и ст. 291 УК РФ).

Мошенничество в социальных сетях — это противоправные действия, направленные на хищение денег, данных или имущества через обман или злоупотребление доверием с использованием платформ для общения и распространения информации. Такие преступления часто связаны с использованием IT-технологий, поддельных профилей, фишинга и социальной инженерии.

Основные виды мошенничества в социальных сетях

1. Взлом аккаунтов. Злоумышленники получают доступ к личной странице пользователя (например, через подбор паролей, использование слитых баз данных или фишинговые рассылки) и от имени владельца рассылают сообщения с просьбой о переводе денег или предоставлении реквизитов банковских карт.

2. Фейковые профили. Мошенники создают поддельные аккаунты, например, под видом знакомых, популярных людей или представителей организаций. От имени этих профилей они просят деньги, данные или пытаются втереться в доверие для последующего выманивания средств.

3. Романтические аферы («кэт-фишинг»). Злоумышленники оформляют личные страницы, публикуют привлекательные фотографии, вступают в общение, завоевывают доверие, а затем просят деньги на «билет домой», «срочную операцию родственнику» или под другим предлогом.

4. Фейковые интернет-магазины. В социальных сетях создаются страницы, где якобы продаются товары по выгодным ценам. Жертвы переводят деньги, но товар не получают либо получают некачественный.

5. Фишинг. Рассылки с поддельных аккаунтов или через мессенджеры с просьбой перейти по ссылке, где требуется ввести конфиденциальные данные (логины, пароли, данные карт).

Мошенничество с инвестициями. В соцсетях распространяется реклама с обещанием быстрого и высокого заработка от инвестиций. После внесения денег преступники исчезают.

6. Лотереи и конкурсы. Пользователи приглашаются зарегистрироваться на поддельных сайтах с указанием персональных данных, после чего деньги «выигрыша» требуют перевести на указанный счёт.

7. Фейковая благотворительность. Создаются аккаунты и сообщества якобы благотворительных проектов, от имени которых ведётся сбор средств на лечение детей, помощь животным и т. д.

8. Мошенничество с работой. Предлагается удалённая работа, но для начала требуется оплатить «обучение», «инструменты» или «гарантию».

Правовые последствия

Мошенничество в социальных сетях может квалифицироваться по нескольким статьям Уголовного кодекса РФ:

ст. 159 УК РФ — мошенничество (обман или злоупотребление доверием для хищения имущества);

ст. 159.6 УК РФ — мошенничество в сфере компьютерной информации (если использовались IT-технологии: поддельные сайты, фишинг, взлом аккаунтов);

ст. 272 УК РФ — неправомерный доступ к компьютерной информации при взломе аккаунтов);

ст. 273 УК РФ — создание и распространение вредоносных программ, если для совершения преступления использовались вирусы или трояны.

Наказание зависит от размера ущерба, обстоятельств дела и других факторов. Оно может включать штрафы, обязательные работы, исправительные работы, ограничение свободы, принудительные работы или лишение свободы — до 10 лет в случае особо крупного ущерба или действий организованной группы.

Как защититься

Не доверяйте просьбам о деньгах от незнакомых или малознакомых людей, даже если сообщение пришло от имени знакомого — проверяйте информацию через другие каналы связи.

Не предоставляйте личные данные, реквизиты карт, пароли и другую конфиденциальную информацию в ответ на сообщения в соцсетях.

Используйте надёжные пароли, включите двухфакторную аутентификацию.

Не переходите по подозрительным ссылкам, не скачивайте вложения от неизвестных отправителей.

Проверяйте информацию о благотворительных фондах и интернет-магазинах перед тем, как переводить деньги.

Если вы стали жертвой мошенничества, зафиксируйте все доказательства (скриншоты, переписки, реквизиты счетов) и обратитесь в полицию с заявлением.

Популярные способы мошенничества через звонки включают использование психологических приёмов, подмены номеров и технических ухищрений. Чаще всего злоумышленники стремятся получить доступ к личным данным, банковским счетам или вынудить жертву перевести деньги.

Основные схемы мошенничества

1. Звонок из банка или финансовой организации. Мошенники сообщают о «подозрительной операции», попытке взлома счёта или критическом уязвимости в системе банка. Они убеждают жертву назвать код из СМС, перевести деньги на «безопасный счёт» или установить приложение для «защиты», которое на самом деле даёт удалённый доступ к телефону. Иногда после первого звонка могут позвонить якобы из полиции или Центробанка.

2. Родственник в беде. Злоумышленники сообщают о ДТП, задержании или болезни родственника и требуют срочно перевести деньги на лечение, адвоката или урегулирование вопроса. Они стараются вызвать шок и не дать человеку времени проверить информацию. Иногда используются голосовые дипфейки.

3. Взлом аккаунта «Госуслуг». Жертве сообщают о подозрительном входе в аккаунт, попытке оформить кредит, доверенность или получить доступ к персональным данным. Далее её переводят на фальшивую службу безопасности и убеждают передать коды подтверждения или установить приложение.

4. Звонок от оператора связи. Мошенник представляется сотрудником мобильного оператора и говорит, что срок действия сим-карты якобы истекает. Нужно назвать код из СМС или подтвердить данные, иначе номер будет заблокирован. На практике этот код может использоваться для входа в банковское приложение, аккаунт «Госуслуг» или мессенджер. Также злоумышленники могут предложить «улучшить тариф», «подключить защиту от спама» или «перейти на 5G».

5. Посылка или доставка. Мошенники представляются сотрудниками маркетплейсов и служб доставки и просят подтвердить получение посылки кодом из СМС. Они могут уточнять адрес, имя или другие данные из утечек, чтобы вызывать доверие.

6. Инвестиционное мошенничество. Человеку предлагают выгодно инвестировать в акции или криптовалюту и обещают высокий доход. Убеждают установить приложение, которое на самом деле крадёт данные.

7. Звонок от имени правоохранительных органов. Мошенники представляются сотрудниками ФСБ, полиции или прокуратуры и утверждают, что жертва подозревается в госизмене, финансировании терроризма или других тяжких преступлениях. Для «закрытия дела» они требуют перевести деньги на «безопасный счёт» или передать данные банковской карты.

8. Неожиданные выплаты. Сообщают, что нужно получить подарок или деньги. Но для этого придётся сообщить данные карты, личных документов и СМС-код с телефона. Пожилых людей так могут обманывать с «выплатами» на День Победы.

9. Кража через NFC. Представляются сотрудником банка или госорганов и предупреждают, что мошенники получили доступ к личному кабинету на «Госуслугах» или банковскому счёту. Предлагают установить приложение, которое якобы позволит защитить деньги. Затем убеждают приложить банковскую карту к NFC на задней части телефона и ввести пин-код. Мошенническое приложение через NFC крадёт данные карты.

10. Допуск к сессии и экзаменам. Перед сессией студентам звонят якобы из деканата. Говорят, что нужно зарегистрироваться на образовательном портале, иначе к экзаменам не допустят. Сайт — поддельный. При регистрации студенту приходит одноразовый код, который требуется продиктовать мошенникам. На самом деле это код от «Госуслуг». Так взламывают личный кабинет, чтобы взять на имя студента кредиты или использовать информацию о нём в других преступных схемах.

Технические уловки, которые используют мошенники

- Подмена номера. С помощью IP-телефонии, специальных сервисов и программ мошенники редактируют Caller ID — технологию, которая определяет входящие вызовы. В результате на экране телефона может отображаться настоящий номер банка или полиции.

- Генерация голосов. Злоумышленники могут использовать алгоритмы для создания голосовых дипфейков.

- Звонки через мессенджеры. Мошенники используют разные мессенджеры и ставят на аватар логотип банка или организации.

Как распознать мошенника

Будьте внимательны, если собеседник просит предоставить личную или финансовую информацию; предлагает совершить платёж или перевести деньги с одного счёта на другой; спрашивает пароль, пин-код, одноразовый код из СМС-сообщения или другую информацию для аутентификации; просит данные банковской карты или реквизиты, чтобы оформить «возврат» или «переплату»; предлагает установить программное обеспечение или дать доступ к защищённому аккаунту; угрожает немедленным арестом и судом; заявляет, что ваши счета были взломаны или вовлечены в мошенническую схему; рассказывает о лёгком способе заработать без особого риска и усилий; говорит, что кто-то из ваших близких в опасности и нужны деньги, чтобы ему помочь.

Как защититься

Не сообщайте коды из СМС и банковские данные. Их нельзя передавать ни при каких обстоятельствах.

Не переводите деньги на «безопасные счета». Сотрудники банков никогда не предлагают переводить деньги для их «сохранности» или «страховки».

Проверяйте информацию самостоятельно. Если звонок вызывает сомнения, завершите разговор и проверьте информацию.

Используйте определители спам-звонков. Они помогут отсеять большинство нежелательных звонков.

Не устанавливайте приложения по инструкции звонящего.

Не переходите по ссылкам из сообщений, даже если они ведут на «официальный сайт».

Если вы стали жертвой мошенничества, зафиксируйте все доказательства (записи разговоров, скриншоты) и обратитесь в полицию с заявлением.