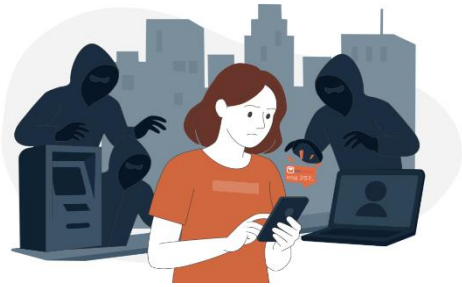
Самые распространенные схемы мошенничества в 2025 году



В ушедшем году мошенники действовали изощрённее. Они умело адаптировали технологии и законодательные изменения под свои преступные схемы, а также активнее прежнего использовали детей для доступа к деньгам семьи. Распознать обман стало сложнее. Но какими бы ни были их легенды, виды мошенничества остаются почти неизменны. А значит, неизменным остается главное средство защиты - критическое мышление. На примерах мошеннических схем - 2025 расскажем, как защитить свои финансовые активы в 2026 году.

«Спасти родителей» Мошенники ни перед чем не останавливаются в погоне за легким и незаконным заработком. В 2025 году получили распространение циничные преступные схемы, которые рассчитаны исключительно на детей.

В чем суть: ребенку звонят «полицейские» и сообщают, что его родителям грозит тюрьма за «финансовые преступления». Чтобы спасти их, ребенок должен показать на камеру деньги и ценности в доме, а затем передать их курьеру. Объясните детям, что сотрудники полиции не требуют передачи денег через курьера. Научите их в подобных ситуациях сразу звонить вам.

«Электронный дневник». Родители тоже не остаются без внимания злоумышленников. Одна из популярных схем 2025 года связана с электронными дневниками. Мошенники под прикрытием школьных работников или специалистов техподдержки пишут в мессенджерах (иногда звонят) и сообщают, что дневник работает некорректно. Чтобы это исправить, нужно выполнить одно или несколько действий:

подтвердить номер телефона

обновить информацию

активировать учетную запись

Цель злоумышленников - разузнать код из СМС, который откроет доступ к онлайн-банку или Госуслугам. Также мошенник может заманить свою жертву на фишинговый сайт, который крадет данные. Дальше может последовать схема со звонком из правоохранительных органов и «спасением» средств на «безопасных счетах» – подробнее о ней ниже.

Официальные представители учебных заведений никогда не запрашивают по телефону или в мессенджере коды из СМС, пароли и подобную информацию. При появлении малейших сомнений стоит прекратить такой разговор. Правильным решением будет позвонить в школу для уточнения информации.

Мошенничество с Пушкинской картой. В чем суть: преступники находят подростков в соцсетях и предлагают им обналичить средства с карты. Схема обмана строится на обещании быстрого и легкого перевода средств в кэш. Для этого злоумышленники просят предоставить полные реквизиты уже не Пушкинской, а банковской карты, включая секретные трехзначные коды, а также пароли из смс. Получив эту информацию, мошенники моментально опустошают карты, после чего бесследно исчезают, предварительно заблокировав контакты и удалив свои аккаунты в соцсетях.

Разговаривайте с детьми о новых схемах мошенничества. Донесите до подростка, что нельзя ни при каких условиях никому передавать конфиденциальные данные карты. Номер, срок действия, трехзначный код карты и коды из смс – персональная информация, которая не должна быть известна третьим лицам.

Подробно о том, какие банковские реквизиты можно сообщать, а какие – ни в коем случае, читайте здесь.

Налоговый вычет. В 2025 году получили распространение схема мошенничества с налоговыми вычетами. В большинстве случаев интерес представляет имущественный вычет при покупке недвижимости. Эта льгота позволяет вернуть 260 000 рублей и предоставляется всего лишь один раз в жизни.

Преступники, зная об этом, стремятся опередить законного владельца. Они составляют фиктивный договор купли-продажи или ДДУ на несуществующий объект недвижимости. На имя жертвы открывается счет по поддельным документам. Затем в налоговую инспекцию подается декларация 3-НДФЛ с указанием ложных данных о сделке и реквизитов счета для перечисления средств. В итоге пострадавший не только лишается денег, но и безвозвратно теряет право на законный вычет при реальной покупке жилья в будущем.

Чтобы обезопасить себя, не выкладывайте в открытый доступ сканы документов: фото паспорта, ИНН, СНИЛС, свидетельство о собственности и др. Передавайте документы только проверенным лицам и организациям (работодателю, риелтору, банку). Установите сложный пароль от Госуслуг и личного кабинета налогоплательщика, регулярно его меняйте и включите двухфакторную аутентификацию для доступа к этим

«Безопасный счет» Эта схема распространена уже несколько лет и по-прежнему остается популярной.

В чем суть: мошенники всеми возможными предлогами убеждают потенциальную жертву перевести деньги на “безопасный/защищенный счет”, который, конечно же, таким не является. Поддаваясь на манипуляции, доверчивый гражданин собственноручно перечисляет деньги мошенникам, которые представляются сотрудниками полиции, Центробанка, прокуратуры и других ведомств. Они сообщают, что счет “взломали”, либо говорят, что обнаружили по нему “нелегальные операции” - например, финансирование ВСУ. Запуганный владелец счета готов следовать любой инструкции, чтобы сохранить деньги. Министерство финансов, от имени которого мошенники тоже частенько звонят, на своем сайте так рассказывает об этой схеме мошенничества: злоумышленники обещают компенсировать часть денег на покупку лекарств, биологических добавок, лечение у экстрасенсов и парапсихологов, по вкладам в банках и другим банковским продуктам. Предлагая получить какую-либо компенсацию, мошенники просят предварительно оплатить: «госпошлину», «страховку», «налог», «страховые взносы» или иные платежи для разблокировки операций по переводу денежных средств.

Мошенники даже высылают гражданам копии фейковых документов с их личными данными и суммой компенсации, ссылаются на вымышленные статьи законов и приказы Минфина России. И все это может быть оформлено на поддельных бланках с недействительной печатью с подписью. Для пущей убедительности гражданам звонит «сотрудник» министерства и требует незамедлительного перечисления на счет подставных «доверенных» лиц крупных сумм денег якобы в качестве «госпошлины» или других «обязательных» платежей.

Минфин России не наделен полномочиями блокировать операции с денежными средствами, а также выплачивать какие-либо компенсации физическим лицам. Настоящие ведомства никогда не требуют перевода денег. Положите трубку и при возникновении сомнений перезвоните для уточнения вопроса самостоятельно по официальному номеру, который всегда можно найти на сайте соответствующего ведомства.

«Инвестиции» в криптовалюту». В чем суть: «успешный брокер» находит потенциальную жертву в соцсетях и предлагает вложить деньги в высокодоходные активы, часто криптовалюту. Для обмана злоумышленники создают фиктивные онлайн-платформы, которые не имеют ничего общего с настоящими криптобиржами. В личном кабинете «инвестора» искусственно формируется видимость успешных торговых операций и растущей прибыли. Увидев мнимый доход, человек соглашается внести дополнительные средства для увеличения своего «инвестиционного портфеля». Иногда мошенники даже разрешают вывести небольшую сумму, чтобы усыпить бдительность. Однако стоит жертве ввести относительно крупную сумму, доступ к кабинету блокируется, а все контакты с «брокером» обрываются. Не верьте в доходность выше рынка, которую предлагают в соцсетях. Вкладывайте деньги исключительно в те финансовые инструменты, принцип работы которых понимаете. В погоне за легким и высоким заработком можно потерять все имеющиеся деньги.

Фишинговые ссылки. В 2025 году по-прежнему в топ-3 наиболее распространенных схем обмана входили фишинговые атаки. При этом мошенники стали работать более точечно и изощренно.

В чем суть: мошенники рассылают ссылки на сайт-копию интернет-магазина, банка, почтового сервиса или страницы входа в соцсеть. При попадании на поддельный сайт пользователя просят авторизоваться, ввести данные банковской карты, номер телефона, паспортные данные и т.д. После ввода информации пользователь может увидеть сообщение об «успешном входе» или «подтверждении заказа», но это всего лишь отвлекающий маневр. Если злоумышленниками удалось завладеть данными карты, они моментально совершают несанкционированные платежи или переводы.

Логины, пароли и другие персональные данные продаются в даркнете. Также мошенники могут использовать доступ к почте или соцсетям для шантажа или мошенничества против друзей и коллег жертвы.

Не переходите по ссылкам из писем и сообщений. Если пришло уведомление от банка или магазина, лучше самостоятельно введите адрес сайта в браузере или откройте официальное приложение.

Взлом Госуслуг через демонстрацию экрана. В чем суть: мошенник, представляясь сотрудником правоохранительных органов, сообщает о взломе аккаунта. Под предлогом ускорения процедуры и защиты от мошенников (вот ирония!) он убеждает пользователя зарегистрироваться на определенном сайте и предлагает свою «помощь», для чего просит включить демонстрацию экрана. Если человек соглашается, то мошенник получает полный визуальный доступ к конфиденциальной информации. Используя полученные персональные данные, он инициирует восстановление доступа к аккаунту на портале Госуслуги, после чего блокирует его для законного владельца. А на Госуслугах, как мы знаем, хранится чувствительная личная информация о нас и персональные данные.

Никогда не включайте демонстрацию экрана незнакомцам. Госорганы никогда не попросят об этом. Если же подобная ситуация произошла, значит перед вами мошенники. Важно срочно прекратить контакт.

Запись к врачу. Запись в поликлинику или больницу тоже в некоторых случаях не обходятся без мошенников. Аферисты, действуя от имени сотрудников больниц или страховых организаций, обзванивают людей, предлагая «запланировать визит к специалисту» или «актуализировать информацию по записи». Главная задача злоумышленников – заполучить контроль над Госуслугами и завладеть деньгами потенциальной жертвы. В ходе беседы злоумышленники пытаются выведать конфиденциальные сведения: логины, пароли, коды из СМС для подтверждения операций или номер телефона, привязанный к учетной записи.

Еще один распространенный метод: рассылка смс с фальшивыми уведомлениями о записи. В таких письмах часто содержится ссылка, которая ведет на сайт-двойник поликлиники или больницы. Ввод персональных данных на таких ресурсах может привести к потере данных или денег.

Для защиты от подобных схем никогда не передавать третьим лицам данные для входа в аккаунты, включая одноразовые коды доступа! Нельзя верить на слово абоненту на другом конце трубки. Всегда перепроверяйте актуальную информацию по записи к врачу через официальные сайты медицинских учреждений или региональные сервисы онлайн-записи. Также можно позвонить в регистратуру для уточнения вопроса.

Голосовые дипфейки. В чем суть: с помощью искусственного интеллекта (ИИ) мошенники создают голосовые копии близких. Потенциальной жертве поступает звонок или голосовое сообщение в мессенджере, где «сын» или «внук» взволнованно сообщает, что попал в аварию, срочно нужны деньги и перевести их нужно как можно скорее и только так можно избежать «ужасных последствий». В некоторых случаях мошенники для убедительности даже создают видеоизображение. Злоумышленники рассчитывают на то, что человек в состоянии аффекта сразу не поймет, что перед ним продукт ИИ, а уже затем, когда переведет деньги, будет поздно.

Перезвоните близкому на его основной номер, чтобы удостовериться. Задайте уточняющий вопрос, ответ на который не известен посторонним.

Вирусы в поздравительных открытках. В чем суть: перед Новым годом, Рождеством, 23 февраля, 8 марта и другими праздниками мошенники спешат «поздравить» доверчивых граждан. В популярных мессенджерах они

рассылают красочные открытки, которые на самом деле содержат вредоносные ссылки или файлы (часто с расширением. apk) – стоит открыть такое поздравление и устройство окажется заражено вирусом. Далее пользователь смартфона, ноутбука или планшета может потерять доступ к гаджету, зато мошенники возьмутся за похищение личных данных, а иногда и денег через установленное на устройстве приложение банка.

Еще одна вариация разводки: фейковые опросы и вакансии. Злоумышленники предлагают пройти оплачиваемый опрос или устроиться на простую работу. Для этого нужно скачать задание или анкету, которая оказывается вредоносной программой.

Не открывайте файлы и ссылки от неизвестных отправителей. Если же желание велико, то перезвоните своему контакту и поинтересуйтесь у него, действительно ли он что-то присылал.

Афера с квартирой. Схема обмана построена следующим образом: злоумышленники под психологическим давлением принуждают человека (чаще всего пенсионера) продать квартиру, а полученные деньги передать наличными через курьера. Когда потерпевший осознает факт мошенничества, он обращается в суд с иском о возврате жилья. Суд, как правило, удовлетворяет требование, признавая, что продажа была совершена владельцем в состоянии аффекта. С формальной точки зрения, пенсионер обязан компенсировать покупателю сумму сделки, однако на практике эти средства уже растворились в карманах мошенников. В результате добросовестный покупатель лишается и квартиры, и денег, а в случае покупки в ипотеку — еще и остается с непогашенным кредитом.

Поговорите со своими пожилыми родственниками, расскажите им о мошеннической схеме и попросить в случае возникновения подобных ситуаций сразу звонить вам. Если же вы планируете покупку жилья на вторичном рынке, то помните 100% защиты в настоящее время от последующего оспаривания сделки нет, но снизить риски можно, застраховав титул.

Материал подготовлен с использованием информации со страницы: https://xn--80apaohbc3aw9e.xn--p1ai/article/ostorozhno-moshenniki-samye-rasprostranennye-shemy-v-2025-godu/

По вопросам соблюдения требований законодательства о защите прав потребителей можно обращаться:

- в Управление Роспотребнадзора по Новгородской области по адресу: В. Новгород, ул. Германа, д.14, тел.971-093; 971-106;

- в Центр по информированию и консультированию потребителей по адресу: г. Великий Новгород, ул. Германа 29а, тел. 77-20-38, 73-06-77;

- в отдел МФЦ по г. Великому Новгороду (адрес: 173000, г. Великий Новгород, ул. Большая Московская, д. 24) консультации можно получить каждый первый четверг месяца с 10-00 до 17-00.

Работает Единый консультационный центр, который функционирует в круглосуточном режиме, по телефону 8 800 555 49 43 (звонок бесплатный), без выходных дней на русском и английском языках.

Дополнительно информируем, что функционирует Государственный информационный ресурс для потребителей https://zpp.rospotrebnadzor.ru. Каждый потребитель может ознакомиться с многочисленными памятками, обучающими видеороликами, образцами претензионных и исковых заявлений.