

Введение

Мошенничество стало одной из самых распространённых угроз современности. Злоумышленники используют уязвимости людей - доверчивость, страх, жадность или нехватку знаний - чтобы завладеть их деньгами, личными данными или доступом к финансовым счетам. Мошенники действуют как удалённо (через звонки, сообщения, интернет), так и при личных встречах, постоянно совершенствуя свои методы.

Особую опасность представляют схемы, основанные на психологическом давлении. Жертвам не оставляют времени на размышления, вынуждая принимать поспешные решения. Понимание механизмов работы мошенников и знание базовых правил безопасности помогают избежать обмана и защитить себя и своих близких.



Мошенничество колл-центров

Мошенничество через колл-центры - это один из самых массовых способов обмана, при котором злоумышленники используют телефонные звонки для введения жертв в заблуждение. Чаще всего звонки поступают с незнакомых номеров, в том числе из других стран (например, из недружественных стран) или с поддельных российских номеров. Мошенники могут представляться сотрудниками банков, правоохранительных органов, налоговой службы, технической поддержки или даже родственниками.

Цель таких звонков - создать иллюзию срочности и заставить жертву действовать необдуманно: перевести деньги, сообщить конфиденциальные данные (например, коды из СМС или пароли от банковских счетов) или установить вредоносное программное обеспечение. Мошенники часто используют заранее подготовленные сценарии, чтобы вызвать доверие и избежать подозрений.



1. Позвонили и представились сотрудником полиции

Что это:

Мошенники представляются сотрудниками правоохранительных органов (МВД, ФСБ, Следственного комитета) и сообщают жертве о якобы возбуждённом уголовном деле, блокировке банковских счетов или необходимости содействия в расследовании. Цель - запугать жертву и вынудить её перевести деньги на "безопасный счёт****" или сообщить конфиденциальные данные.

Характерные признаки

- Звонок с незнакомого номера, часто с подменой номера (например, отображается номер МВД или другого госоргана).
- Угрозы арестом, блокировкой счетов или привлечением к уголовной ответственности.
- Требование немедленно выполнить инструкции, не сообщая об этом родственникам или знакомым.
- Просьба перевести деньги на "безопасный счёт¹" или сообщить данные банковской карты, коды из СМС, пароли.

Как защититься?

1. **Положите трубку** и перезвоните на официальный номер правоохранительного органа, чтобы уточнить информацию.
2. **Не сообщайте** никакие личные данные, реквизиты банковских карт, коды из СМС или пароли.
3. **Не переводите деньги** на указанные счета, даже если звонящий утверждает, что это необходимо для "защиты" ваших средств.
4. **Обратитесь в полицию** с заявлением, если вас пытались обмануть.



2. "Мама/Папа, я в беде!"

Что это:

Мошенники звонят жертве, представляясь её родственником (чаще всего сыном или дочерью), и сообщают о чрезвычайной ситуации: ДТП, аресте, необходимости срочно внести залог или оплатить лечение. Цель - вызвать панику и получить деньги.

Характерные признаки

- Звонок с незнакомого номера, голос может быть похож на голос родственника (используются записи или подражание).
- Сообщение о срочной необходимости перевести деньги.
- Просьба не сообщать другим родственникам о ситуации.
- Использование фраз: "Мама/папа, это я!", "Мне срочно нужны деньги!", "Я попал в беду, помоги!".

Как защититься?

1. **Не паникуйте** и положите трубку.
2. **Перезвоните родственнику**, от имени которого поступил звонок, на его привычный номер телефона.
3. **Не переводите деньги** до подтверждения личности звонящего.
4. **Предупредите родственников** о такой схеме мошенничества.



3. Фальшивые налоговые уведомления

Что это:

Мошенники представляются сотрудниками Федеральной налоговой службы (ФНС) и сообщают о задолженности по налогам, штрафам или необходимости срочно погасить долг, либо, на почту человеку приходит письмо с требованием погасить долг, максимально имитирующее реальные письма с требованием погасить имущественные или иные долги. Цель - заставить жертву перевести деньги на поддельный счёт или сообщить данные банковской карты.

Характерные признаки

- Звонок или СМС с требованием срочно погасить задолженность по налогам.
- Подозрительное письмо, пришедшее на почтовый ящик дома.
- Угрозы блокировки счетов, ареста имущества или привлечения к уголовной ответственности.
- Просьба перейти по ссылке для оплаты или сообщить данные банковской карты.
- Использование поддельных сайтов, похожих на официальный сайт ФНС.

Как защититься?

1. **Не переходите по ссылкам** из СМС или сообщений.
2. **Проверяйте получателя платежа**, который указан в письмах, не является ли он частным лицом или неизвестным ИП/ООО
3. **Проверьте информацию** о задолженности на официальном сайте ФНС (nalog.gov.ru) или в личном кабинете налогоплательщика.
4. **Не сообщайте** данные банковской карты или коды из СМС.
5. **Обратитесь в налоговую службу** по официальному телефону для уточнения информации.



4. Поддельные социологические опросы

Что это:

Мошенники звонят жертве, представляясь сотрудниками исследовательских центров или государственных организаций (ВЦИОМ, ФОМ и др.), и предлагают принять участие в социологическом опросе. В ходе разговора они выманивают личные данные, информацию о банковских картах или убеждают перевести деньги под предлогом "вознаграждения".

Характерные признаки

- Звонок с незнакомого номера с предложением принять участие в опросе.
- Вопросы о личных данных (паспортные данные, адрес проживания, место работы).
- Просьба сообщить данные банковской карты для "перечисления вознаграждения".

Как защититься?

1. **Не сообщайте личные данные** по телефону незнакомым людям.
2. **Не переводите деньги** под предлогом участия в опросе или получения вознаграждения.
3. **Уточните название организации** и проверьте её легитимность на официальных сайтах.
4. **Положите трубку**, если звонящий настаивает на срочном предоставлении данных.



5. Мошенничество с технической поддержкой

Что это:

Мошенники представляются сотрудниками технической поддержки банков, операторов связи или крупных компаний (например: служба безопасности СберБанка или Яндекс) и сообщают о проблемах с компьютером, банковским счётом или аккаунтом. Цель - получить удалённый доступ к устройству жертвы, украсть данные или деньги.

Характерные признаки

- Звонок с незнакомого номера с сообщением о "взломе аккаунта", "вирусе на компьютере" или "проблемах с банковской картой".
- Просьба установить программу для удалённого доступа¹ (например, AnyDesk, TeamViewer, RustDesk).
- Требование сообщить данные банковской карты, коды из СМС или пароли.
- Угрозы блокировки аккаунта или счёта, если жертва не выполнит инструкции.

Как защититься?

1. **Не устанавливайте** программы для удалённого доступа по просьбе незнакомых людей.
2. **Не сообщайте** данные банковской карты, коды из СМС или пароли.
3. **Положите трубку** и перезвоните в официальную службу поддержки компании, используя номер с её официального сайта, или номер с банковской карты вашего банка.
4. **Проверьте компьютер и телефон на вирусы** с помощью антивируса (Kaspersky, Dr.Web), если есть подозрения.



¹ Программа удалённого доступа - специализированное программное обеспечение, способное исполнять удалённо команды. Обычно способно выгружать файлы с устройства удалённо, и удалённо на него выгружать, что может использоваться мошенниками для получения доступа к критической информации или шантажу.

6. Ложное трудоустройство по звонку

Что это:

Мошенники предлагают жертве высокооплачиваемую работу с минимальными требованиями. Для "оформления" требуется оплатить комиссию, купить оборудование или пройти платное обучение. После получения денег мошенники исчезают.

Характерные признаки

- Звонок с незнакомого номера с предложением работы.
- Обещание высокой зарплаты за минимальные усилия.
- Требование оплатить "оформление документов", "обучение" или "оборудование".
- Использование поддельных сайтов или групп в социальных сетях для подтверждения легитимности.

Как защититься?

1. **Не переводите деньги** под предлогом оформления на работу.
2. **Проверьте информацию** о компании на официальных сайтах и в реестре юридических лиц (egrul.nalog.ru).
3. **Не сообщайте личные данные** до заключения официального трудового договора.



7. Романс-скам с переходом на звонки

Что это:

Мошенники знакомятся с жертвой на сайтах знакомств или в социальных сетях, входят в доверие и начинают просить деньги под различными предлогами (болезнь, проблемы с визой, необходимость билетов для встречи). После получения денег мошенники исчезают.

Характерные признаки

- Быстрое развитие отношений и признания в любви.
- Просьбы о финансовой помощи под различными предлогами.
- Отказ от видеосвязи или личных встреч.
- Использование фальшивых фотографий и историй (В современном мире существует технология Дипфейк², обращайте внимание на малейшие артефакты изображения на лице или странный голос)

Как защититься?

1. **Не переводите деньги** незнакомым людям, даже если они кажутся близкими.
2. **Проверьте профиль** в социальных сетях: ищите фальшивые фотографии через поиск по картинкам (например, Яндекс Картинки).
3. **Не сообщайте личные данные** и реквизиты банковских карт.
4. **Обратитесь в полицию**, если стали жертвой такого мошенничества.



² Дипфейк (англ. deepfake от deep learning «глубинное обучение» + fake «подделка») - методика синтеза изображения или голоса, основанная на искусственном интеллекте.

Иные виды мошенничества

Помимо классических схем через колл-центры, мошенники активно используют другие методы обмана, не связанные напрямую с телефонными звонками, но столь же опасные. Эти схемы часто эксплуатируют доверие, невнимательность или нехватку знаний жертв, маскируясь под легальные сервисы, государственные структуры или даже знакомых людей.

Чаще всего такие мошенничества реализуются через **интернет** (фишинговые сайты, поддельные приложения, социальные сети), **электронную почту**, **мессенджеры** (WhatsApp, Telegram, Viber) или **личные встречи**. Цель остаётся прежней: заставить жертву добровольно передать деньги, конфиденциальные данные (например, пароли, реквизиты карт) или установить вредоносное ПО. Мошенники адаптируют свои схемы под актуальные тренды - криптовалюты, онлайн-шопинг, инвестиции, благотворительность - и используют психологические приёмы, чтобы создать иллюзию легитимности и срочности.



1. Фишинг и поддельные сайты/приложения

Что это:

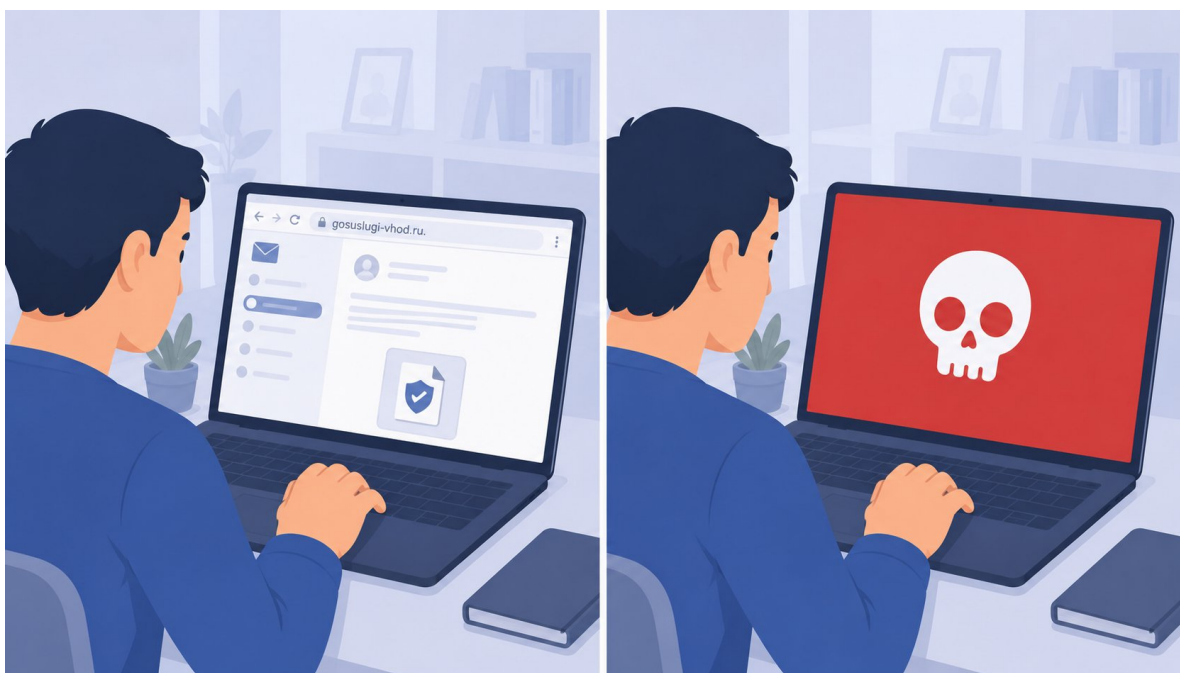
Фишинг - это метод мошенничества, при котором злоумышленники создают поддельные сайты или приложения, имитирующие официальные ресурсы банков, государственных органов, социальных сетей или интернет-магазинов. Цель - завладеть личными данными жертвы (логины, пароли, данные банковских карт) или заставить её перевести деньги.

Характерные признаки

- Письма или СМС с ссылками на поддельные сайты, похожие на официальные (например, "sberbank-login.ru" вместо "sberbank.ru").
- Требование срочно ввести данные банковской карты, пароль или код из СМС.
- Поддельные страницы входа в социальные сети или почтовые сервисы.
- Приложения для смартфонов, которые запрашивают избыточные разрешения (доступ к СМС, контактам, геолокации).

Как защититься?

1. **Не переходите по ссылкам** из писем или СМС. Вводите адреса сайтов вручную в адресной строке браузера.
2. **Проверяйте адрес сайта** в адресной строке: он должен начинаться с <https://> и содержать название официального домена (например tax.ru, а не tax.com или maks.ru).
3. **Не вводите данные банковской карты** на подозрительных сайтах.
4. **Используйте двухфакторную аутентификацию** для защиты аккаунтов.
5. **Устанавливайте приложения на телефон только из официальных магазинов** (RuStore, Google Play, App Store).



2. Мошенничество при покупке/продаже товаров

Что это:

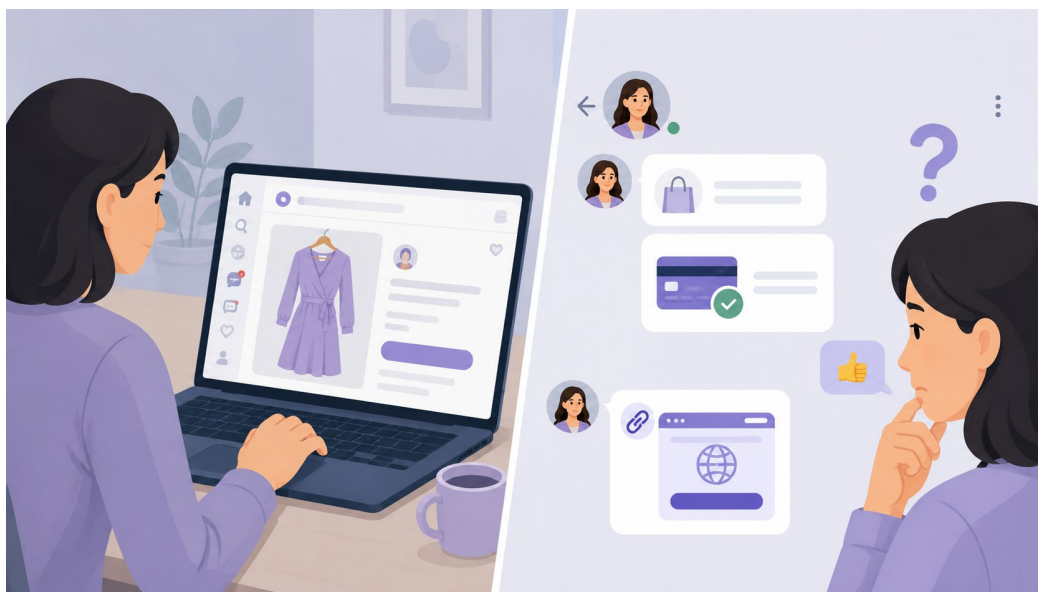
Мошенники создают объявления о продаже товаров по привлекательным ценам на популярных площадках (Avito, Юла, социальные сети). После получения предоплаты товар не отправляется, а продавец исчезает. Или же когда человек выставляет свой товар на продажу, ему пишут с предложением срочно его выкупить, что всё уже предоплачено и высылают ссылку где необходимо ввести данные карты для получения средств за товар.

Характерные признаки

- Слишком низкая цена на товар.
- Продавец отказывается от личной встречи или отправки товара через официальные службы доставки.
- Обещания заплатить больше за срочность, или что товар уже предоплачен и нужно просто ввести данные что-бы получить деньги.
- Требование полной предоплаты или перевода денег на карту.
- Поддельные отзывы или профили в социальных сетях.

Как защититься?

1. **Не переводите деньги** до получения товара.
2. **Используйте официальные службы доставки** с возможностью оплаты при получении.
3. **Проверяйте профиль продавца:** ищите отзывы, историю активности, реальные фотографии.
4. **Встречайтесь лично** в безопасных местах (например, в крупных супермаркетах в поле зрения камер или в отделении почты).
5. **Не сообщайте личные данные** продавцу или покупателю без необходимости.



3. Кripto-мошенничество

Что это:

Мошенники предлагают инвестировать в криптовалюты³, обещая высокую доходность. После перевода денег жертва теряет доступ к своим средствам, а мошенники исчезают. Также распространены схемы с поддельными криптовалютными биржами или кошельками.

Характерные признаки

- Обещания высокой доходности за короткий срок.
- Требование перевести деньги на неизвестные криптовалютные кошельки.
- Поддельные сайты криптовалютных бирж или кошельков.
- Давление на жертву с целью быстрого принятия решения.

Как защититься?

1. **Не инвестируйте в криптовалюты** без глубокого понимания рынка.
2. **Используйте только проверенные криптовалютные биржи** - биржи с высокой репутацией и работающие легально.
3. **Не переводите деньги** на неизвестные кошельки.
4. **Проверяйте информацию** о проектах на официальных сайтах и в независимых источниках.
5. **Не сообщайте данные своих криптовалютных кошельков** незнакомым людям. Не сообщайте пароли и данные от аккаунтов бирж, а особенно Seed-фразу⁴.



³ Криптовалюта - разновидность цифровой валюты, учёт внутренних расчётных единиц которой обеспечивает децентрализованная платёжная система (нет внутреннего или внешнего администратора или какого-либо его аналога), работающая в полностью автоматическом режиме.

⁴ Seed-фраза (или мнемоническая фраза) — это набор из 12, 18 или 24 слов, который предоставляет доступ к вашему криптокошельку и всем его адресам.

4. Финансовые пирамиды и ложные инвестиции

Что это:

Финансовые пирамиды - это мошеннические схемы, при которых доходы первых участников выплачиваются за счёт взносов новых участников. Рано или поздно пирамида рухнет, и большинство участников теряют свои деньги. Мошенники обещают высокую доходность, используют агрессивную рекламу и давление на жертву.

Характерные признаки

- Обещания высокой доходности (например, 50–100% в месяц).
- Отсутствие лицензии Центрального Банка РФ на осуществление инвестиционной деятельности.
- Давление на жертву с целью быстрого принятия решения.
- Требование привлекать новых участников для получения дохода.

Как защититься?

1. **Проверяйте наличие лицензии** у компании на сайте Банка России (cbr.ru).
2. **Не верьте обещаниям высокой доходности** без рисков.
3. **Не переводите деньги** на счета физических лиц или неизвестных компаний.
4. **Изучите отзывы** о компании в независимых источниках.
5. **Обратитесь в Банк России** или полицию, если подозреваете финансовую пирамиду.



5. Фальшивые благотворительные сборы

Что это:

Мошенники создают поддельные благотворительные фонды или сборы на лечение, помощь пострадавшим или другие благородные цели. Они используют социальные сети, мессенджеры и СМС для сбора денег, которые затем присваиваются.

Характерные признаки

- Сбор средств на лечение или помощь пострадавшим без подтверждающих документов.
- Использование поддельных документов или фотографий.
- Требование перевести деньги на карту физического лица.
- Отсутствие информации о фонде на официальных сайтах.

Как защититься?

1. **Проверяйте информацию** о благотворительном фонде на его официальном сайте.
2. **Не переводите деньги** на карты физических лиц.
3. **Используйте только проверенные платформы** для благотворительных сборов (например, dobro.ru).
4. **Требуйте документы**, подтверждающие необходимость сбора средств.
5. **Обратитесь в полицию**, если подозреваете мошенничество.



6. Мошенничество с займами и кредитами

Что это:

Мошенники предлагают оформить заем или кредит на выгодных условиях, но требуют предоплату за "оформление", "страховку" или "комиссию". После получения денег они исчезают, а кредит или заем не оформляется, либо оформляется, но деньги попадают в руки мошенникам.

Характерные признаки

- Предложение кредита или займа без проверки кредитной истории.
- Требование предоплаты за оформление документов.
- Использование поддельных сайтов или документов.
- Давление на жертву с целью быстрого принятия решения.

Как защититься?

1. **Не оформляйте кредиты или займы** через посредников.
2. **Не передавайте деньги «курьерам»** и не берите деньги от них.
3. **Не переводите деньги** за оформление кредита.
4. **Проверяйте информацию** о кредитной организации на сайте Банка России.
5. **Используйте только проверенные банки и МФО** для оформления кредитов.
6. **Обратитесь в полицию**, если стали жертвой мошенничества.



7. Обман с арендой жилья

Что это:

Мошенники размещают объявления об аренде жилья по привлекательным ценам, но после получения предоплаты или залога исчезают. Также распространены схемы, при которых одно и то же жильё сдаётся нескольким людям одновременно.

Характерные признаки

- Слишком низкая цена на аренду жилья.
- Отказ от личной встречи или показа жилья.
- Требование предоплаты или залога до заключения договора.
- Поддельные документы на право собственности.

Как защититься?

1. **Не переводите деньги** до заключения договора аренды.
2. **Проверяйте документы** на право собственности через Росреестр (rosreestr.gov.ru).
3. **Встречайтесь лично** с арендодателем и осматривайте жильё.
4. **Заключайте договор аренды** в письменной форме.
5. **Не сообщайте личные данные** без необходимости.



8. Мошенничество с игровыми аккаунтами и виртуальными товарами

Что это:

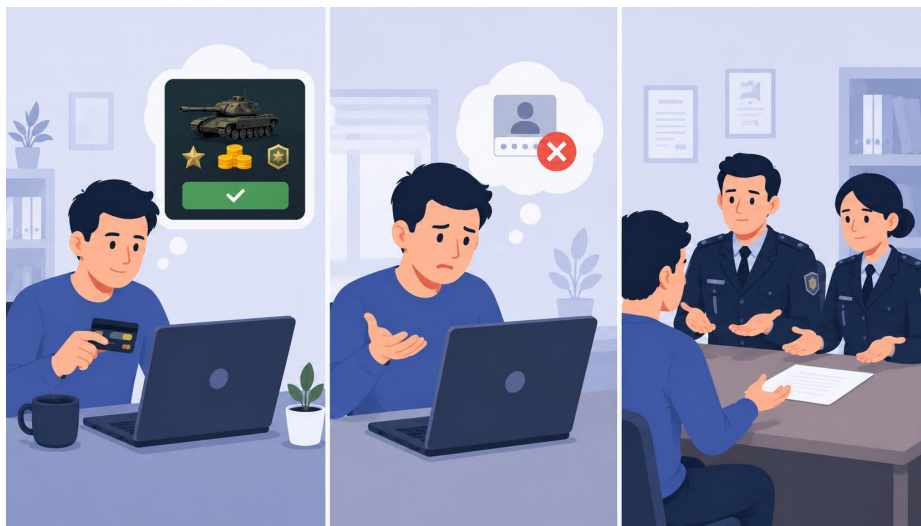
Мошенники предлагают купить или продать игровые аккаунты⁵, валюту или предметы по привлекательным ценам. После получения денег или передачи аккаунта они исчезают, а жертва остаётся без денег или аккаунта.

Характерные признаки

- Предложение купить или продать игровые аккаунты, валюту или предметы по цене ниже рыночной.
- Отказ от использования официальных платформ для сделок (например, VK Play, Steam, Epic Games).
- Требование предоплаты или передачи аккаунта до получения денег.
- Использование поддельных скриншотов или отзывов.

Как защититься?

1. **Используйте только официальные платформы** для покупки или продажи игровых аккаунтов и предметов.
2. **Не переводите деньги** до получения товара.
3. **Проверяйте репутацию продавца** на форумах и в социальных сетях.
4. **Не сообщайте данные своего аккаунта** незнакомым людям.
5. **Обратитесь в службу поддержки игры или платформы**, если стали жертвой мошенничества.



⁵ Не на всех платформах можно продавать аккаунты или предметы вне самой платформы. Большинство явно это запрещает в лицензионном соглашении. Если платформа запрещает продажу аккаунтов или предметов, такое действие может повлечь блокировку купленного или же проданного аккаунта по правилам платформы.

9. Фейковые розыгрыши и акции

Что это:

Мошенники создают поддельные розыгрыши призов или акции, предлагая жертве получить выигрыш или скидку. Для этого требуется перевести деньги за "комиссию", "доставку" или "налог". После получения денег мошенники исчезают.

Характерные признаки

- Сообщение о выигрыше в лотерее или акции, в которой жертва не участвовала.
- Требование перевести деньги за "комиссию", "доставку" или "налог".
- Использование поддельных сайтов или документов.
- Давление на жертву с целью быстрого принятия решения.

Как защититься?

1. **Не участвуйте в розыгрышах**, о которых вы не знаете.
2. **Не переводите деньги** за получение приза, если только в оффере организатора не прописана доставка за счёт участника.
3. **Проверяйте условия розыгрыша**. Даже если акция привязана к покупке, при стоимости приза свыше 4 000 рублей возникает налог 35% с суммы превышения. Организатор не всегда берёт эту оплату на себя - уточняйте это в правилах до участия.
4. **Проверяйте информацию** об акции на официальном сайте компании, а не в личных сообщениях в мессенджерах.
5. **Обратитесь в полицию**, если стали жертвой мошенничества.



10. Регистрация ИП/ООО "под ключ"

Что это:

Мошенники предлагают услуги по быстрой регистрации ИП или ООО "под ключ", но после получения денег либо не выполняют свои обязательства, либо регистрируют компанию на подставных лиц. Это может привести к серьёзным последствиям, так как ИП/ООО будут оформлены на ваше имя и действовать от вашего имени.

Характерные признаки

- Предложение зарегистрировать ИП или ООО без личного участия.
- Требование предоплаты за услуги.
- Использование поддельных документов или печатей.
- Отсутствие информации о компании в реестре юридических лиц.

Как защититься?

1. **Регистрируйте ИП или ООО самостоятельно** через официальный сайт ФНС (nalog.gov.ru).
2. **Не переводите деньги** за услуги регистрации неизвестным лицам.
3. **Проверяйте информацию** о компании в реестре юридических лиц (egrul.nalog.ru).
4. **Обратитесь в налоговую службу или полицию**, если стали жертвой мошенничества.



Общие рекомендации

1. **Будьте бдительны:** не доверяйте незнакомым людям, даже если они представились сотрудниками полиции. Требуйте от сотрудников полиции удостоверение, и не отдавайте деньги, карты или телефон без составления официального протокола и поездки в отделение.
2. **Не передавайте деньги «курьерам»:** не передавайте деньги «курьерам», «сотрудникам банка» или «следователю» который может приехать к вам домой что-бы увезти деньги или ценности в «безопасное место». Они могут показать фальшивые документы или удостоверение дабы усыпить бдительность. Это может быть попытка похитить ваши деньги!
3. **Не сообщайте личные данные:** не передавайте незнакомым лицам по телефону или в интернете данные банковских карт, пароли, коды из СМС, паспортные данные или чувствительную информацию (ваши болезни, болезни родственников или потерю близких)
4. **Проверяйте информацию:** уточняйте данные о компаниях, организациях или людях через официальные источники.
5. **Не переводите деньги** до подтверждения легитимности сделки или предложения.
6. **Используйте двухфакторную аутентификацию** для защиты аккаунтов в социальных сетях, почте и банковских приложениях.
7. **Устанавливайте приложения только из официальных магазинов** (RuStore, Google Play, App Store).
8. **Обращайтесь в полицию,** если стали жертвой мошенничества или подозреваете мошеннические действия.
9. **Информируйте родственников и друзей** о распространённых схемах мошенничества. И держите с ними регулярную связь. Вы можете обнаружить что вашего родственника пытаются обмануть до того, как это случится.