



РУКОВОДСТВО О ТОМ, КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Информация поможет вам распознать мошеннические схемы, защитить себя, а также обеспечить безопасность своих средств.

По данным Сбербанка, ущерб от телефонного мошенничества в 2024 году превысил 295 миллиардов рублей. **Зная методы мошенников, вы сможете защитить себя и своих близких!**

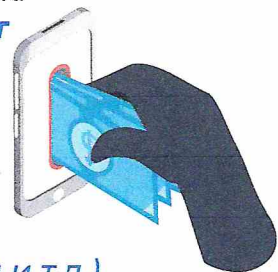
1. ОСНОВНЫЕ ВИДЫ МОШЕННИЧЕСТВА

1.1. СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА:

«Банк звонит»: Мошенники представляются сотрудниками банка и под предлогом защиты ваших средств просят назвать CVV-код (*три цифры на обратной стороне карты*), пароль из смс-сообщения или данные для входа в онлайн-банк. **Запомните: настоящие сотрудники банка никогда не запрашивают такую информацию!**

«Родственник в беде»: Вам звонят и сообщают, что ваш близкий (*сын, дочь, внук*) попал в ДТП, задержан полицией и т.д., и срочно нужны деньги. Мошенники давят на эмоции, присылают фальшивые документы (*постановлений о возбуждении дела, протоколов допроса и т.д.*). **Немедленно положите трубку и свяжитесь с родственником напрямую.**

«Вы выиграли приз!»: Вам сообщают о выигрыше ценного приза (*автомобиль, квартира, крупная сумма денег*), но для его получения необходимо оплатить "доставку", "страховку" или какой-либо другой взнос. **С вероятностью 100% с Вами связались мошенники, не общайтесь с ними и положите трубку.**





«Звонок из поликлиники\больницы»: Под видом сотрудника регистратуры или медицинского работника вам могут позвонить и, ссылаясь на запись на прием, попросить сообщить номер страхового полиса или СНИЛС. **С помощью номера вашего СНИЛС злоумышленники могут получить доступ к вашему аккаунту в системе «Госуслуги».**

«Звонок из полиции»: Мошенники представляются сотрудниками правоохранительных органов - старшими следователями, оперуполномоченными или дознавателями. Они утверждают, что в отношении вас проводится проверка или возбуждено уголовное дело из-за якобы подозрительных переводов с вашей карты на зарубежные счета. Для убедительности они могут назвать конкретный районный отдел полиции, откуда якобы звонят. Несмотря на серьезность заявлений, злоумышленники предлагают «урегулировать вопрос» дистанционно, требуя перевода денег, или предоставления конфиденциальной информации.
Помните: настоящие сотрудники полиции никогда не решают подобные вопросы по телефону и не требуют денег.

«Представитель сотового оператора»: Мошенники звонят, представляясь сотрудниками вашего сотового оператора, и сообщают об окончании срока действия договора на предоставление услуг связи. Они пытаются убедить вас сообщить код из смс-сообщения, якобы для того, чтобы продлить действие договора, но на самом деле хотят получить доступ к вашему личному кабинету в системе «Госуслуги» или платежным системам.

Положите трубку и свяжитесь с сотовым оператором по официальному номеру телефона.

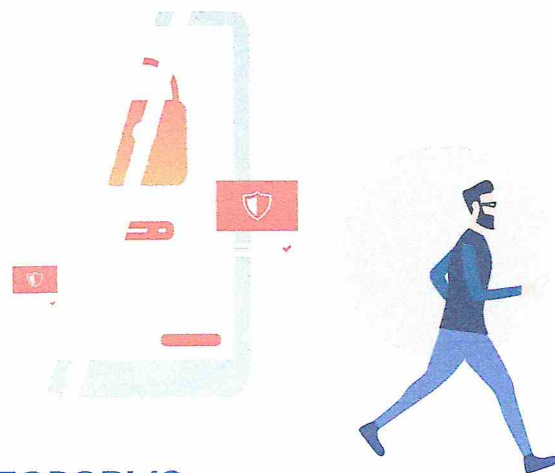




Обман на Avito/Юле (и других площадках объявлений): Обычно его используют при покупке какой-то вещи с рук. Злоумышленник находит на этих платформах объявления о продаже какой-то вещи, и обращается к продавцу по этому вопросу. Чтобы посмотреть вещь, злоумышленник просит созвониться по видеосвязи, но во время звонка у него якобы случаются какие-то технические неполадки. Чтобы обойти их, он просит собеседника включить демонстрацию экрана. В это время мошенник может, например, попытаться зайти в ваш интернет-банк или аккаунт в системе «Госуслуги», поэтому вам на телефон придёт смс-сообщение с кодом для входа или смены пароля, который злоумышленник хочет увидеть и использовать. **Не включайте демонстрацию экрана в разговорах с незнакомыми людьми.**

ПРИЗНАКИ ОБМАНА В ИНТЕРНЕТЕ:

- Адрес сайта без HTTPS (*защищенного протокола*).
- Контактная информация только через мессенджеры (*Telegram, WhatsApp*), отсутствие телефона и физического адреса.
- Слишком выгодная цена, которая значительно ниже рыночной (*например, "iPhone за 5000 руб."*).



1.3. УГРОЗЫ ЖИЗНИ И ЗДОРОВЬЮ

Мошенники запугивают жертв угрозами расправы, присылают личные данные, фото дома или работы, создают дипфейки с «захваченными» родственниками (*например, из зоны СВО*). Цель – давление и вымогательство.

Группы риска: пенсионеры, семьи военных, несовершеннолетние. Иногда жертв заставляют уйти из дома и оборвать связь с родными, чтобы создать дополнительный рычаг давления.

Важно помнить, что это блеф – чаще всего злоумышленники действуют из-за границы и не могут причинить реального вреда своим жертвам.



2. КАК ЗАЩИТИТЬСЯ?

2.1. ЗАЩИТА ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ:

Правило 1: Никогда не называйте коды из смс-сообщений, пароли и другую конфиденциальную информацию по телефону.

Правило 2: Перезванивайте только на официальные номера банков, указанные на вашей карте или официальном сайте.

Правило 3: Установите приложение для блокировки спам-номеров. *например от Яндекс*

Правило 4: По возможности не отвечайте на звонки с незнакомых номеров.



2.2. ИНТЕРНЕТ-БЕЗОПАСНОСТЬ:

Правило 1: Не переходите по подозрительным ссылкам, особенно полученным от незнакомых людей или в спам-рассылках.

Правило 2: Включите двухфакторную аутентификацию на всех важных аккаунтах (*банки, соцсети, почта*). Это обеспечит дополнительный уровень защиты.

Правило 3: Покупайте товары только на проверенных площадках и у надежных продавцов. Обращайте внимание на отзывы и рейтинг продавца. *Отсутствие отзывов — это подозрительный маркер.*



ЧТО ДЕЛАТЬ, ЕСЛИ ВАС ОБМАНУЛИ? СРОЧНЫЕ ДЕЙСТВИЯ:

Немедленно позвоните в банк и заблокируйте карту,
чтобы предотвратить дальнейшее списание средств.



Отсканируйте QR-код,
чтобы узнать, как быстро
заблокировать карту

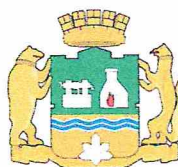
Сообщите в банк о мошеннической операции.

В некоторых случаях банк может вернуть украденные
деньги (*процедура чарджбэк*).

Подайте заявление в полицию. Это можно сделать онлайн.



Отсканируйте QR-код,
чтобы подать заявление
в МВД онлайн



Если Вы столкнулись с противоправной информацией, то Вы можете:

- Пожаловаться администрации социальной сети на контент/профиль с противоправной информацией
- Заполнить форму обращения в общественной электронной приемной Роскомнадзора (*Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций*)
- Посредством обращения через сайт Министерства внутренних дел Российской Федерации (*мвд.рф*) вы можете оставить жалобу на сайт экстремистского характера или какой-либо материал, содержащий в себе признаки экстремизма.



При переходе на сайт Министерства внутренних дел Российской Федерации перед вами появится страница со списком подразделений для приема обращений граждан. Выберите из списка и поставьте галочку напротив «Главное управление по противодействию экстремизму», прокрутите страницу вниз и нажмите кнопку «Далее».

Также Вы всегда можете обратиться в:



Управление Федеральной службы безопасности России по Свердловской области (343) 371-37-51 (телефон доверия)



Главное управление Министерства внутренних дел России по Свердловской области (343) 358-71-61, (343) 358-70-71 (телефон доверия)