Телефонное мошенничество.

Актуальность темы состоит в том, что  эта тема является элементом некой сложной системной проблемы, которую невозможно решить, пока не выяснена сущность каждого из её элементов.



Очень важно, что нужно быть постоянно на чеку,  Мобильный телефон ваш друг и помощник, но мобильное мошенничество набирает обороты, и самое страшное  что все, что они вытворяют в большей степени остаётся безнаказанным. Что увеличивает прирост латентной приступности.  Причина тому, обманутые люди, их  незнание куда обратиться или маленькая сумма воровства, но поверьте,  если вы сделаете хоть шаг по защите себя,  то и защитите других людей от злостных мошенников.

Изобретательность мошенников не стоит на месте. Как только очередная схема обмана становится достоянием общественности, тут же появляется новая — более хитрая, а иногда и более продуктивная.

На сегодняшний день телефонных обманок расплодилось великое множество, правда, в основе, как правило, лежит несколько стандартных и довольно простых схем. Причём есть явно незаконные способы вытянуть из вас деньги, а есть те, к которым даже прокуратура подкопаться не сможет. Телефонные мошенники умудряются убедить доверчивых людей о необходимости тех или иных действий, секретности информации и т.п. Явным примером такого мошенничества можно посмотреть по ссылке популярной на сегодняшний день передачи «За гранью» <https://www.ntv.ru/peredacha/Za_granyu/m89640/o728098/video/> .

**Кто такие Телефонные мошенники?**

Телефонные мошенники – это новый вид мошенников, которые посредством мобильного или городского телефона выманивают деньги и практически во всех случаях остаются безнаказанными. Телефонное мошенничество весьма прибыльно и, самое главное, на данный момент практически ненаказуемо.

Оградить от мошенников в первую очередь способны лишь внимательность и здравомыслие самих граждан. Жертвами мошенников становятся все без исключения – это и бизнесмены, и чиновники, и звезды шоу-бизнеса, и обычные граждане.

**Основные виды телефонного мошенничества.**

Основные виды телефонного мошенничества:

* СМС-просьба.
* Случай с родственником.
* Розыгрыш призов.
* Кредитная карта заблокирована!
* Платный код.
* Штрафные санкции оператора.
* Ошибочный перевод средств.
* Вирусы-шантажисты.
* Интернет-баннеры, которые требуют выкуп.
* Голосовое письмо — поздравление.
* Обновление браузера.

**Звонки от «служб безопасности» банков**  
Распространены также звонки от «службы безопасности банка». Человеку звонят мошенники, которые представляются сотрудниками банка и сообщают, что по его счету неизвестные совершают подозрительные операции. Чтобы вернуть деньги, необходимо сообщить номер карты, ее трехзначный код и срок действия.  
  
**Также распространенной схемой мошенничества являются операции с «безопасным счетом».** Клиенту банка могут сообщить, что мошенники оформляют кредит на его имя. Чтобы опередить злоумышленников, человеку предлагают оформить кредит самостоятельно и перевести полученные деньги на «безопасный счет». После того как жертва переводит деньги, мошенники перестают выходить с ней на связь.  
  
**В России злоумышленники все чаще используют многошаговую схему обмана**. Жертве сначала могут позвонить сотрудники правоохранительных органов, затем перевести звонок на «Банк России» и «кредитное учреждение». У человека будут нагнетать чувство паники и сопровождать его на проводе до тех пор, пока он не переведет сбережения мошенникам или не раскусит, что говорит с мошенниками.  
  
**Жертву могут вынуждать перевести средства на «безопасный счет»,** чтобы уберечь их от мошенников. Чтобы убедить человека в правдивости информации, ему могут выслать документы с поддельной печатью Банка России или заявку на кредит якобы от лица жертвы с его персональными данными.  
  
Такой прессинг и манипуляции не позволяют человеку опомниться и обдумать ситуацию. Из-за страха жертва может оформить многочисленные кредиты, перевести деньги злоумышленникам и даже не сообщить информацию сотрудникам банка в процессе перевода денег.  
  
Отметим, Центробанк не работает напрямую с гражданами. Банк России не обслуживает и не открывает счета физлиц.  
  
Злоумышленники также могут представиться сотрудниками финучреждений или портала «Госуслуги» и уточнить, не оформлял ли человек кредит. Если человек дает отрицательный ответ, мошенники могут убедить его отменить заявку, однако для этого просят назвать код из СМС.  
  
Этого делать нельзя ни в коем случае. Вероятно, злоумышленники хотят получить доступ к личному кабинету человека на сайте банка и перевести деньги с его счета на свой.  
  
Помните, что сотрудники правоохранительных органов, кредитных учреждений, интернет-магазинов не будут просить вас назвать коды из СМС.  
  
Звонки от «сотрудников» правоохранительных органов и государственных служб  
Цель таких звонков — усыпить бдительность человека и выманить деньги клиента или узнать данные для оформления кредита.  
  
Подобную схему могут использовать также якобы сотрудники Социального фонда, налоговой, соцслужбы и так далее, которые сообщают гражданам о новых социальных выплатах. Под предлогом перевода пособий мошенники узнают у граждан данные их карт.  
  
Мошенничество с упоминанием банков и госорганов: как распознать злоумышленников  
ТЕМА ДНЯ  
Мошенничество с упоминанием банков и госорганов: как распознать злоумышленников  
13.01.2023 18:13  
Звонки с подменой номеров  
Банки часто используют специальные номера, которые легко запомнить клиентам. Однако есть специальные программы-обманки, которые маскируют настоящий номер мошенника, поэтому абонент видит знакомые ему цифры.  
  
В 2021 году приняли поправки в Федеральный закон о «О связи», благодаря которым можно блокировать СМС-сообщения и звонки с подмененных номеров. Операторы не могут менять настоящий номер телефона и должны подключиться к специальной службе Роскомнадзора.  
  
Звонки об ошибочном переводе  
Мошенник может сообщить человеку об ошибочном переводе средств на мобильный телефон и попросить вернуть деньги, которые в действительности никто не переводил.  
  
Сообщения о родственнике в беде  
Звонок о попавшем в беду родственнике обычно совершают ночью и сообщают сонному человеку о ДТП или других происшествиях, которые случились с его детьми, внуками или знакомыми. После этого у человека просят перевести сумму на электронный кошелек или банковский счет, чтобы помочь родственнику или знакомому.  
  
Сообщения о выигрыше в лотерею  
Человеку сообщают о крупном выигрыше. Но чтобы получить деньги, обычно необходимо покрыть технические издержки лотереи. Разумеется, после этого никакой выигрыш никому не переводят.  
  
Платные звонки  
Иногда мошенники совершают короткий звонок, сбрасывают вызов, а когда человек перезванивает, с его счета списывается крупная сумма денег.  
  
Телефонные вирусы  
Жертве приходит сообщение со ссылкой. При переходе по ней на компьютер или телефон внедряется вирус, который получает контроль над гаджетом.  
  
Иногда мошенники могут убедить человека установить приложение удаленного доступа к телефону. После этого мошенники получают полный контроль над смартфоном и могут перевести средства со счета жертвы посредством мобильного банка на свой счет.  
  
Особенную осторожность необходимо соблюдать владельцам смартфонов на базе Android. На iOS вирусы встречаются реже из-за особенностей программного обеспечения.  
  
Как защититься от мошенников  
Чаще всего мошенники представляются сотрудниками службы безопасности банков или правоохранительных органов. Звонящие могут сообщить о попытке взлома счета, чужом кредите, просрочках по займу или других надуманных обвинениях.  
  
Помните, сотрудники службы безопасности банка не будут звонить клиентам. При возникновении подозрений вас вызовут повесткой в отделение.  
  
Как распознать мошенника по номеру  
Не нужно брать трубку, если вам звонит незнакомый номер.  
  
Перезванивать на номера из пропущенных вызовов также не стоит, особенно если звонок был очень коротким или сразу после ответа на том конце положили трубку.  
  
Перед тем как ответить на звонок или перезвонить, стоит проверить номер в Сети. Вы можете проверить номер на специальных сайтах или воспользоваться сервисами борьбы с мошенниками. Такие есть у многих банков и поисковых систем. Кроме того, можно установить определитель номера.  
  
Обратите внимание, что сейчас в России действует «Антифрод» на подменные номера, поэтому злоумышленники постепенно отказываются от классических телефонных звонков и используют опции аудиозвонка в мессенджерах.  
  
Помните, что банки, госорганы, МФЦ, «Госуслуги», Центробанк и другие официальные организации никогда не будут звонить вам через мобильные мессенджеры.  
  
Как по разговору понять, что вы общаетесь с мошенником  
Если вам позвонили из банка и вы хотите проверить собеседника, узнайте его имя и фамилию, а затем перезвоните по официальному номеру банка — он указан на обороте карты и на сайте кредитного учреждения. Номер лучше ввести вручную, даже если с него вам звонили совсем недавно. Так вы исключите случаи подмены номеров. После этого попросите переключить на сотрудника, который якобы вам звонил.  
  
При любых подозрениях лучше прервите разговор и положите трубку.  
  
Если звонящий сообщает о краже денег со счета клиента или сомнительных операциях от его имени, стоит прервать звонок и позвонить по телефону, который указан на сайте.  
  
На мошенников также может указывать тактика сильного давления. Они всегда торопят собеседника, заставляют его совершать быстрые действия без возможности подумать. Такие разговоры также не стоит продолжать.  
  
Выдать мошенника могут и выдуманные организации и законы, незнание географии вашего региона. Если вам предлагают новое социальное пособие, уточните, на каких основаниях его выплачивают.  
  
Также мошенники могут несколько раз подряд задавать вам вопросы, на которые можно ответить «да». Избегайте таких ответов, переспрашивайте или переводите тему.  
  
Запись голоса с ответами могут использовать при оформлении кредитов на ваше имя, если банки используют биометрические данные клиентов. Особенно стоит этого избегать, если в банке вы подключены к биометрической системе.  
  
Правоохранительные органы точно не будут связываться с вами по телефону, чтобы попросить оформить кредит, сказать код из СМС, перевести деньги на электронный кошелек, угрожать и давить. При необходимости вас вызовут повесткой.  
  
Какую информацию нельзя сообщать собеседнику по телефону  
Мошенникам часто нужны данные карт, коды подтверждения из СМС, пароли для входа в интернет-банк. Сотрудники банков никогда не запрашивают такую информацию.  
  
Для переводов часто нужны только номер телефона или карты. Никаких кодов из СМС или CVV-кодов не нужно.  
  
Как обезопасить пожилых людей от телефонных мошенников  
Часто от действий злоумышленников страдают именно пожилые люди. Пенсионеры часто очень доверчивы, плохо ориентируются в цифровых технологиях и нюансах работы банков и других учреждений. Чтобы обезопасить родственников от мошенников, чаще напоминайте им основные правила безопасности. Их стоит придерживаться каждому:  
  
Не нужно сообщать код с обратной стороны карты, из СМС и для входа в интернет-банк.  
Для перевода денег используйте только официальные номера, приложения и сайты банков.  
Не перезванивайте по незнакомым номерам.  
Звоните в банки и ведомства только по официальным номерам. Узнать их можно на сайтах учреждений.  
Не переходите по подозрительным ссылкам из сообщений.  
Если вам говорят о проблемах с картой, оформлении кредитов на ваше имя, положите трубку и перезвоните в банк сами.  
Если вам предлагают какие-либо выплаты, положите трубку и позвоните в ведомство.  
Если вы потеряли карту или сообщили ее данные незнакомому человеку, немедленно ее заблокируйте.  
Для безопасности вы можете держать деньги на одной карте, а для интернет-покупок, подписок и переводов использовать вторую карту. Когда нужно что-то оплатить или где-то в интернете ввести номер карты, переводите с первой карты на вторую.  
  
Выбрать дебетовую карту  
Можно ли привлечь к ответственности телефонных мошенников  
Телефонное мошенничество подпадает под статью 159 Уголовного кодекса РФ. Злоумышленнику могут назначить штраф в 500 тысяч рублей, принудительные работы или реальный срок лишения свободы до 10 лет со штрафом или без.  
  
На практике привлечь мошенника к ответственности сложно. Злоумышленники подменяют номера, регистрируют сим-карты на чужое имя, используют сервисы для сокрытия своего местоположения.  
  
Некоторые используют средства социальной инженерии — втираются в доверие к жертве и убеждают ее оформить кредит и перевести свои сбережения и заемные деньги на чужой счет. Доказать, что вы перевели деньги в результате обмана, бывает сложно.  
  
Однако подать заявление в правоохранительные органы обязательно нужно. Чем больше пострадавших обратятся в полицию, тем выше вероятность, что злоумышленника найдут и накажут.  
  
Вам позвонили из Банки.ру: как проверить, правда ли это сотрудники компании или звонят мошенники  
Сотрудники контактного центра финансового маркетплейса Банки.ру никогда:  
  
не просят подтвердить переводы, платежи или поступление денег на вашу карту;  
не запрашивают номера карт, банковские реквизиты или кодовые слова;  
не звонят в мессенджерах, таких как WhatsApp, Telegram или Viber;  
не оповещают о комиссиях — все услуги маркетплейса бесплатны.  
Если сомневаетесь, что с вами говорит сотрудник Банки.ру, то запросите у собеседника внутренний номер. Как правило, неподготовленный мошенник бросит трубку, а подготовленный может и наврать. Чтобы проверить, с кем вы говорили, зайдите на Банки.ру, прокрутите главную страницу до самого конца и найдите вкладку «Служба поддержки». Оставьте сообщение в свободной форме и укажите номер, который вам предоставил собеседник. Мы его проверим и в ответном письме напишем, был ли звонивший нашим сотрудником или же это мошенник. В последнем случае номер лучше заблокировать.

**Куда жаловаться на телефонных мошенников.**

**Куда обратиться, если пропали деньги**

**В полицию**

**Кража денег — уголовное преступление, и им должна заниматься полиция  
Оставьте заявление о действиях мошенников**

* **по телефону горячей линии МВД 8-800-222-74-47**
* [**на сайте МВД**](https://xn--b1aew.xn--p1ai/request_main)
* **в отделении полиции по месту жительства**

**Когда дежурный в отделении полиции примет заявление, он обязан выдать вам талон-уведомление. Это означает, что заявление принято**

**В банк**

**По закону банки обязаны вернуть клиенту незаконно списанные средства, если не докажут, что клиент сам нарушил правила использования карты**[**п.15 ст. 9 закона «О национальной платёжной системе»**](https://www.consultant.ru/document/cons_doc_LAW_115625/b0062cfb1c3cae710d57f0557303e78760a31d16/) **Важно действовать быстро**

1. **Позвоните в банк, сообщите о проблеме и заблокируйте карту**
2. **Попробуйте отменить транзакцию в личном кабинете банка или в мобильном приложении**
3. **Запросите подробную выписку со счёта, где будет указано, куда переведены деньги**

**Если вы лично раскрыли мошеннику конфиденциальную информацию — например, дали пин-код от карты или сказали CVV-код — банк не обязан возвращать деньги. Этот платёж считается добровольным, банк не имеет права отменять его и списывать деньги со счёта получателя  
  
Банки не вмешиваются в договорные отношения клиентов, все претензии между плательщиком и получателям решаются без участия банка**[**п. 1.25 гл. 1 Правил перевода денежных средств**](http://www.consultant.ru/document/cons_doc_LAW_131829/373ee330758c2c5369484b83fa46aaf50f72efd9/)

**Если банк отказывается решать ваш вопрос, попросите письменный отказ с указанием причин. Напишите жалобу**[**на сайте Банка России**](https://cbr.ru/Reception/Message/Register?messageType=Complaint)



**Будьте в курсе!**

Кто предупрежден — тот вооружен! Ознакомьтесь с наиболее распространенными видами мошенничества.

2.При получении звонка с незнакомого номера проанализируйте ситуацию и принимайте взвешенные решения.

3. Чтобы разблокировать компьютер от вирусов, используйте антивирусное ПО известных разработчиков, в том числе бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям, гарантирующим избавление от вируса или исчезновение Интернет-баннера при отправке SMS на короткий номер.

4. Отдавайте предпочтение проверенным сервисам.

5. Опасайтесь кражи телефона при нахождении в роуминге. Кражи мобильных телефонов совершаются с целью осуществления вызовов в роуминге, что приводит к образованию задолженности. В связи с этим, отдыхая заграницей, будьте внимательны и не оставляйте мобильные телефоны без присмотра! В случае кражи мобильного телефона незамедлительно заблокируйте номер, чтобы предотвратить использование мошенниками средств, находящихся на Вашем лицевом счете. По возвращении в Россию Вы сможете восстановить свой номер.

6.НИКОГДА не вводите номер своего телефона на сайтах, требующих "ПОДТВЕРДИТЕ, ЧТО ВЫ ЧЕЛОВЕК". Поиск данных о фамилии, создание видеоролика с Вашим фото, астрологический прогноз и т.п. - источники последующей рассылки спама и заразы.

7.Отключите в телефоне автоматический переход по ссылкам в СМС и ММС, если таковой вдруг у вас где-то включен.

8. Скопируйте или спишите  содержание SMS и номер пакостного отправителя   и отправьте их  по электронной почте, не по SMS (!!) своему оператору. У всех операторов есть на сайте ссылка на жалобы по мошенничеству.

9.Задача SMS - спровоцировать ответный звонок, SMS или переход по ссылке. Экспериментировать с ними не стоит под угрозой потери денег, поэтому на адрес отправителя  никогда НЕ  звоните для разборок,  не отвечайте эсэмэской "вы достали, не сохраняйте СМС, не копируйте ссылку.

10.Никогда не открывайте ссылки "для проверки" на компе. Есть риск, что вы активируете платную подписку контент-гомосеков даже таким образом. Ничего нового, кроме факта заразности вы не узнаете.

11. Проверяйте периодически баланс и через всякие интернет-помощники отсутствие платных подписок на всех своих номерах

12. Если деньги  все-таки  списали и  действительно необоснованно, незамедлительно пишите оператору письменную претензию, получайте экземпляр с печатью о приеме и ТРЕБУЙТЕ как возврата  денег, так и письменного ответа оператора о причине неправомерного списания

13.Не поленитесь написать заявление в отделение полиции, если денег все же списали. Это статья "Мошенничество".

14.Не поленитесь написать заявление в полицию, если смс приходят в ночи и ЧАСТО. Это статья "Хулиганство".

**Люди, не будьте наивными!**



Интернет ресурсы

1. <https://www.gosuslugi.ru/situation/financial_fraud/when_deceiving>

2. <https://stopmoshennik.com/russia/>

3. Banki.ru <https://www.banki.ru/news/daytheme/?id=10985509>

4. <https://ru.wikipedia.org/>

5. <https://cbr.ru/>

6. <https://openbudget.irkobl.ru/sodeystvie/federalnyy-uroven/>

Информацию подготовил:

ведущий специалист ФУА МО Куйтунский район А.А. Кошкарева