**МВД России предупреждает!**

**Очень важно!!!**

**Сотрудники полиции не обзванивают граждан на предмет наличия кредитных задолженностей, это делают только мошенники!!!**

**О способах телефонных мошенничеств**

**Телефонное мошенничество** получило развитие с начала 2000-х годов, когда сотовый телефон стал массовым и доступным.
В настоящее время, когда широко используются мобильные телефоны и личный номер может быть у всех, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества растут с каждым годом. Чаще всего в сети телефонных мошенников попадаются пожилые или доверчивые люди. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

### **Обман по телефону: родственник попал в беду, требование выкупа.**

Звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.
Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку. Цена вопроса от тысячи рублей до 30 тыс. долларов США.
В организации обмана по телефону с требованием выкупа могут участвовать несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Нередко жертва сама случайно подсказывает имя того, о ком она волнуется. Если жертва преступления поддалась на обман и согласилась привезти указанную сумму, звонящий называет адрес, куда нужно приехать. Часто мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег.
После того как гражданин оставляет деньги в указанном месте или кому-то их передает, ему сообщают, где он может увидеть своего родственника или знакомого.

***Рекомендации гражданам:***

Первое и самое **главное правило – прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён – связаться с его коллегами, друзьями и родственниками для уточнения информации.** Следует задать уточняющие вопросы, ответы на которые посторонним не известны. Спросить, из какого отделения полиции звонящий. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда. Требование взятки является преступлением.

### **Телефонный номер-грабитель**

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества. Приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной - помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того, как потерпевший перезванивает, долго держат на линии. В результате оказывается, что со счёта списаны крупные суммы.
Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.
**Совет гражданам:** **не звонить по незнакомым номерам.**

### **Телефонные** **вирусы**

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: ***«Вам пришло MMS-сообщение. Для получения пройдите по ссылке...»***. **При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.**
Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер... для подтверждения операции отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Существует множество вариантов таких мошенничеств.
Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона.
**Совет гражданам:** не следует звонить по номеру, с которого отправлен SMS.

### **Простой код от оператора связи**

Потерпевшему поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки оператора мобильной связи. Обоснования этого звонка или SMS могут быть: предложение подключить новую эксклюзивную услугу; для перерегистрации во избежание отключения связи из-за технического сбоя; для улучшения качества связи; для защиты от СПАМ-рассылки; предложение принять участие в акции от вашего сотового оператора.
Предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п. на самом деле код, является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников. Как только его наберёт потерпевший, злоумышленник получает доступ к счёту.
**Для граждан:** любая упрощённая процедура изменения тарифных планов должна вызывать подозрение, необходимо перезванивать своему мобильному оператору по телефону горячей линии для уточнения условий или открыть соответствующие разделены на официальном сайте оператора (в мобильном приложении).

### **SMS-просьба о помощи**

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт. Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.
**Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.**

### Пример хищений денежных средств со счетов с использованием вредоносных программ

В сматрфон или компьютер жертвы тайно устанавливаются вредоносное программное обеспечение (ПО). Вредоносная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в СМС или ММС сообщениях. Кроме того, потерпевшие сами неосознанно могут устанавливать на мобильные устройства вредоносные программы, замаскированные под игры и другие программные продукты. Одним из признаков наличия вредоносных программы на мобильном телефоне является направление «пустых» СМС или ММС сообщений на телефоны, имеющихся в контактах устройства. При открытии адресатом такого СМС или ММС сообщения, происходит дальнейшее заражение вирусом телефонов, получившее данное сообщение.
Это могут быть троянские программы, которые не размножаются и не рассылаются сами, они ничего не уничтожают. Задача троянской программы - обеспечить злоумышленнику доступ к устройству жертвы и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений.
Если к смартфону подключена услуга «Мобильный банк», то сведения о доступе в Личный кабинет становятся известны преступнику. Тайно входя в чужие Личные кабинеты он может перечислять денежные средства сотен потерпевших на свои счета, а затем обналичивать.

**Тактика борьбы достаточно проста:**

Не допускать, чтобы вредоносные программы попадали на компьютер или смартфон (чаще всего страдают владельцы смартфонов с ОС Андроид). Если они все-таки попали, ни в коем случае не запускать их. Принять меры, чтобы, по возможности, они не причинили ущерба. Использовать специальные антивирусные программы.
Отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Они автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.
**Если деньги все-таки списались,** разработан алгоритм действий потерпевшего:
Немедленно прекратить любые действия с сотовым телефоном, принудительно отключить его, извлечь СИМ карту. Обеспечить сохранность (целостность) сотового телефона, как возможного средства совершения преступления. Не предпринимать никаких действий для самостоятельного или с привлечением посторонних ИТ-специалистов поиска и удаления вирусов, восстановления работоспособности сотового телефона, не отправлять сотовый телефон в сервисные службы ИТ для восстановления работоспособности.
Незамедлительно обратиться в свой банк по телефону горячей линии с поручением о блокировки операции с расчетным счетом и отзывом криминального перевода.
Незамедлительно обратиться в свой банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе «Мобильный банк» (приложение 2). Заявление может быть направлено в банк по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в банк в течение одного дня. Оформляется в 2-х экземплярах.
Согласно полученной в банке детализации с расчетного счета обратиться в банк получателя (используемого преступником) по телефону с заявлением о приостановке исполнения платежа и возврате средств.
В течение одного дня обратиться с заявлением в правоохранительные органы о факте хищения денежных средств. Для полиции понадобиться документальное подтверждение хищения денежных средств, в том числе выписка по банковскому счету, справка из банка, иные документы, подтверждающие списание заявленной суммы ущерба. Существует возможность получение этих данных из «личного кабинета» пользователя услуг сотовой связи, банк-онлайн с письменного согласия потерпевшего. Эта информация может быть зафиксирована протоколом осмотра места происшествия.
Оперативно обратится в банк с заполненной справкой по факту инцидента информационной безопасности в системе дистанционного банковского обслуживания (приложение 3), которое оформляется в 2-х экземплярах.
***Справочно:*** ФЗ от 27.06.2011 № 161-ФЗ «О национальной платежной системе» предусматривает процедуру обращения в банк после незаконной транзакции и дает право на возмещение незаконно списанных денежных средств со счета. Так, п. 11 ст. 9 гласит «В случаи утраты электронного средства платежа и (или) его использования без согласия клиента, клиент обязан направить соответствующее уведомление оператору по переводу денежных средств в предусмотренной договором форме незамедлительно, после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции».
В п. 15 ст. 9 указано «В случае, если оператор по переводу денежных средств исполняет обязанность по уведомлению клиента - физического лица о совершенной операции в соответствии с частью 4 настоящей статьи и клиент - физическое лицо направил оператору по переводу денежных средств уведомление в соответствии с частью 11 настоящей статьи, оператор по переводу денежных средств должен возместить клиенту сумму указанной операции, совершенной без согласия клиента до момента направления клиентом - физическим лицом уведомления. В указанном случае оператор по переводу денежных средств обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента - физического лица».

Информация с официального сайта МВД России