**Новые схемы мошенничества**

Эксперт проекта НИФИ Минфина России «Моифинансы.рф» Максим Сёмов в [интервью](https://riamo.ru/articles/shpargalki/samye-rasprostranennye-shemy-kreditnogo-moshennichestva-kak-razvodjat-rossijan-na-dengi/) PUAMO рассказал о самых распространенных схемах кредитного мошенничества.

Нельзя сказать, что мошенники начали использовать какие-то новые схемы или приемы. Даже если появляются какие-либо новые уловки – все они основаны на двух основных принципах. Схема «напугать – спасти», когда в телефонном разговоре неизвестные пугают гражданина любым неприятным известием, а затем предлагают выход из негативной ситуации – «спасение». Оно обычно заключается в переводе средств по указанным мошенниками реквизитам. Дело в том, что испуг отключает способность критически оценить ситуацию, посмотреть на нее без спешки и понять, что она нелогичная и подозрительная.

Жертве этого просто не дадут сделать,для этого используется второй базовый принцип – «претекстинг». Это алгоритм диалога с жертвой. Заранее готов сценарий разговора, предусматривающий множество вариантов развития диалога. Он содержит ответы на любые вопросы жертвы и, в зависимости от ответов, подставляет новые вопросы и тезисы, позволяющие вести беседу в нужном темпе и направлении.

Так что совсем новых схем нет. Есть только новые легенды, которые используют мошенники. И, конечно, все это основано на обмане, злоупотреблении доверием.

Давайте посмотрим, что же нового появилось в этой сфере?

* Кредитная заявка. Жертве звонит мошенник, представляясь сотрудником спецслужб или Банка России, и сообщает, что на имя жертвы в разных банках только что было оформлено несколько заявлений на выдачу кредита. Причем заявления уже одобрены, и кредитные средства вот-вот будут выданы. Для предотвращения такой выдачи жертве советуют быстрее обратиться в банк и «опередить» мошенников, самостоятельно оформив заявление на кредит. Жертва направляется в банк, где оформляет заявление и вскоре получает кредит. Как правило, речь идет о потребительских кредитах на незначительные суммы, поэтому выдача происходит быстро. Полученные деньги звонящий требует срочно перевести на «специальный счет», который курируется Банком России. Далее жертву не отпускают, а заставляют бежать в другой банк, третий, четвертый – и везде нужно заключить кредитные договоры. Все деньги переводятся на «специальный счет». Обязательное условие: нельзя говорить никому о телефонном разговоре! Особенно работникам банков. Потому что заявки, по словам звонившего, «оформляются самими банкирами». В итоге деньги исчезают, а несчастный заемщик остается один на один с банками, справедливо требующими возврата кредитов.
* Телефонные атаки на семьи военнослужащих. Мошенники пугают тем, что положенные выплаты будут удержаны из-за провинности военнослужащего (в некоторых случаях, общаясь через мессенджеры, мошенники присылают фотографии «приказов о взыскании»). Причем речь идет о списании уже ранее выплаченных средств со счета военнослужащего. Ну и дальше применяется стандартная схема обмана – мошенники говорят, что для сохранения денег нужно быстро перевести все деньги на безопасный счет. Понятно, что переведенные таким образом деньги исчезают навсегда.
* Еще одна новая схема: мошенники рассылают письма от имени налоговой службы с требованием представить налоговую декларацию. Для этого необходимо перейти по ссылке на сайт, якобы принадлежащий налоговой службе. Сайт имитирует сайт ФНС – отличие только в адресе. При переходе по ссылке жертва должна ввести реквизиты банковской карты, персональные данные. Если жертва эти данные вводит, то мошенники не только похищают деньги, но и используют персональные данные жертвы для следующих атак, в том числе для повторного мошенничества, когда с жертвой связываются лже-юристы, предлагающие вернуть похищенные средства за вознаграждение.
* Также появилась схема с обменом купюр. Под видом работников Банка России, мошенники звонят гражданам и предлагают установить мобильное приложение, позволяющее в режиме онлайн проверять подлинность денежных купюр. Якобы такое приложение разработано в рамках государственной программы поддержки и совершенно бесплатно предлагается всем гражданам страны для использования. Если установить такое приложение (а в оформлении используется символика Банка России), то мошенники получают доступ к смартфону жертвы и быстро «уводят» доступы ко всем личным кабинетам, что заканчивается не только кражей средств с личных счетов, но и оформлением новых кредитов и займов на имя жертвы.
* С купюрами связана еще одна схема мошенничества, которой уже много лет, но раз она применяется, значит актуальна и сейчас. Под видом сотрудников социальных служб мошенники обходят квартиры и дома жертв и предлагают обменять купюры номиналом 5 000 рублей на новые. В качестве причины показывают приказы и распоряжения главы Банка России о проводимом в настоящее время обмене денег. Конечно, под видом новых купюр мошенники подсовывают поддельные деньги.
* Частая схема со звонками от руководителей – так называемый «звонок босса».

Жертве поступает звонок через мессенджер от имени руководителя, который сообщает, что спецслужбами в настоящее время проводится расследование в отношении сотрудников компании, в которой работает жертва, и что в рамках такого расследования жертве необходимо выполнить некоторые задания, которые сообщит представитель спецслужб. Далее с жертвой связывается «представитель спецслужб», приказывающий срочно осуществить перевод средств на «специальный счет» (это якобы необходимо для поимки преступников). Если такой перевод будет сделан, деньги исчезнут вместе с аккаунтами «руководителя» и «сотрудника спецслужб».

* Мошенники чутко реагируют на новые услуги, продукты, появляющиеся на рынке. После появления той или иной услуги мошенники начинают перестраивать свои приемы под эти услуги. Не так давно на рынке появился сервис снятия наличных денег с помощью QR-кода. Клиент банка формирует такой код в мобильном приложении, затем использует его при снятии наличных в банкомате – это сокращает время на ввод данных в банкомате и снижает риски ошибок. Клиенту нужно лишь поднести мобильный телефон к сканеру банкомата и снять наличные средства. Незамедлительно мошенники взяли на вооружение эту услугу. Они звонят от имени банка и сообщают клиенту о том, что неизвестными от имени клиента только что был сформирован QR-код на снятие наличных. Для отмены операции необходимо прислать QR-код отмены, который, по словам мошенника, формируется точно так же, как и код снятия. Клиент в испуге формирует и посылает такой код, чем пользуются мошенники. С помощью полученного QR-кода они снимают наличные деньги со счета клиента. К сожалению, введя такой сервис, финансовые организации забыли должным образов проинформировать клиентов, о том, что банк не будет запрашивать у клиента QR-код ни под каким предлогом.
* Участились случаи повторного мошенничества – гражданину, уже пострадавшему от мошенников, звонит неизвестный, представляясь сотрудником полиции или прокуратуры. Он сообщает, что расследование преступления, где гражданин является потерпевшим, квалифицировано как крупное и будет объединено в общее с группой пострадавших. Если гражданин согласен, то для подтверждения объединения необходимо направить СМС на указанный номер. Понятно, что в случае направления любого ответа гражданин рискует остаться без доступа к личным кабинетам банков и портала госуслуг, что чревато повторным выводом средств (а также оформлением микрокредитов и займов на его имя). Кстати, еще один вариант повторного мошенничества (в основном речь идет о пострадавших от вложения в финансовые пирамиды) – оформление соглашения с внезапно появляющимися юристами о возврате похищенных средств. Конечно же, используется предоплата, ради которой все и затевается, – мошенник, получив предоплату, исчезает с ней.

Как видите, все схемы в той или иной мере используют испуг, затем следует предложение «спасения» – выхода из ситуации. И, конечно, все они основаны на обмане. Точно так же работают и старые схемы. Это и звонок из банка (на жертву оформлена кредитная заявка, и нужно срочно опередить негодяев – взять кредит самому и перевести его на безопасный счет), и звонок спецслужб («с вашего счета зафиксирован перевод средств в пользу экстремистов – вы являетесь соучастником и понесете уголовное наказание. Спасти вас может только немедленный визит в банк и перевод всех денег на безопасный счет»), и звонок близкого («мама, я попал в аварию, меня везут в тюрьму. Заплати, тогда меня отпустят до суда») и многое другое.

Повторю, все схемы основаны на конструкции «напугать – спасти».

Могут позвонить «из поликлиники» и напугать страшным диагнозом по анализам, могут позвонить ребенку и испугать сообщением, что его собака умерла. Вариантов множество, но общий признак – начать с испуга, а затем предложить что-либо сделать. Это и срочное обращение в банк, и перевод денег в мобильном приложении, и установка программы – любое действие. Единственное правильное поведение заключается в прекращении разговора.

К сожалению, значительная часть наших пожилых родственников не может прервать разговор самостоятельно. Но поможет прием, который мы назвали «Корней Чуковский». Он легко запоминается, а выполнение этих пунктов, несмотря на то, что человек не сразу прервет разговор и какое-то время будет разговаривать с мошенниками, все же поможет предотвратить преступление.

 «У меня зазвонил телефон».

1. Кто говорит?

Выясняем, кто звонит: «Представьтесь, пожалуйста»

1. Откуда?

Выясняем, от имени какой организации звонят: «Какую организацию вы представляете?»

1. Что вам надо?

Выясняем, по какому поводу звонят: «Что вас интересует?».

4. Прекращаем разговор и сообщаем о нем специально выбранному родственнику, который уже может информировать о нем ту организацию, от имени которой звонили преступники.

В заключение напомню простые правила финансовой гигиены, помогающие предотвратить финансовое мошенничество.

1. В случае телефонного звонка от неизвестного, представившегося сотрудником полиции, Банка России, прокуратуры, Росфинмониторинга, ФСБ и прочих государственных организаций, нужно немедленно прекратить разговор и сообщить о нем в ту организацию, от имени которой поступил звонок.
2. Коды и пароли от любых информационных систем, а также ПИН-код от банковских карт нужно хранить в надежном месте. Нельзя сообщать их никому! Предоставление любых цифр, направленных в СМС или продиктованных по просьбе неизвестного лица, приведет не только к потере доступа к личным кабинетам, но и к потере вами денег – мошенники переведут их с ваших счетов.
3. Если вы переводите деньги по просьбе неизвестного лица (например, по телефонному звонку от «работника прокуратуры») – вы не только потеряете эти деньги, но и можете стать участником преступления – ведь нельзя узнать, на какие цели переводятся эти деньги.

Берегите себя. Не поддавайтесь на уловки мошенников. Посещайте наши мероприятия и будьте здоровы.