Сёти в Сетй

Дистанционное мошенничество становится все более серьезной проблемой: в минувшем году с попытками обмана по телефону или интернету столкнулись 83 процента россиян. По мере совершенствования системы кибербезопасности растут и возможности аферистов, которые придумывают все новые способы.

Варианты развода

В последнее время злоумышленники активно взялись за образовательные учреждения – сотрудникам приходят сообщения от якобы руководства вуза или специалистов Министерства науки и высшего образования. Применяются технологии подмены голоса, на аватар ставятся фото руководства. Все заканчивается тем, что необходимо заплатить серьезную денежную сумму.

Одна из старейших мошеннических схем, применяемых до сих пор, нацелена прежде всего на пожилых людей: это трюк с "попавшим в беду родственником". Скорее всего, почти все о нем слышали: звонящий в крайне эмоциональном тоне убеждает, что близкий вам человек стал виновником ДТП, попался с наркотиками или совершил какое-либо другое серьезное правонарушение. Как следует запугав собеседника и добившись желаемого психологического эффекта, преступник намекает, что "можно договориться" – и родственник избежит положенного наказания. Затем трубку передают "сотруднику силовых структур", который развивает напор и уточняет детали.

В зависимости от наглости мошенников сумма может варьироваться от 10-15 тысяч рублей до миллиона и даже больше. Деньги потребуют либо перевести сразу на карту, либо передать посреднику.

Не менее распространен звонок от "сотрудника службы безопасности банка": преступник сходу огорошивает заявлением о том, что с карты клиента прямо сейчас пытаются списать крупную сумму, и чтобы этого не случилось, надо назвать звонящему номер карты, CVV-код и код из СМС. Так аферисты получают доступ к денежным средствам клиента. Этот прием уже хорошо известен, но люди продолжают попадать в ловушку. В большинстве случаев мошенники действуют чисто интуитивно, они не знают, ни в каких банках обслуживается клиент, ни сколько денег он имеет на счете.

Еще один вид развода: человека убеждают в том, что на его мобильный телефон или на банковскую карту ошибочно перевели крупную сумму. В подтверждение этих слов приходит сообщение о зачислении средств. Расчет идет на то, что жертва почувствует себя неловко и поспешит вернуть деньги. Подвох же в том, что "ошибочный" перевод был на ничтожную сумму (например, 15 рублей, что легко принять за 1500), либо его не было вовсе, а сообщение с замаскированного телефонного номера послали сами мошенники.

Бесплатный сыр

Для прикрытия своих махинаций киберафериста часто используют рекламные акции, лотереи или розыгрыши. Звонящий может представиться радиоведущим. Вначале он поздравляет с крупным выигрышем. Затем доверчивую жертву переключают на "сотрудника призового отдела", и тот уже разводит на личные данные.

Чтобы упростить схему обмана, мошенники используют смс или мессенджеры. Текст однотипный: "У меня проблемы, срочно кинь <...> рублей на этот номер. Мне не звони, перезвоню сам". Как правило, это срабатывает на совсем юных или слишком пожилых абонентах.

Существует вариант с номером-грабителем, когда человеку приходит сообщение с просьбой от знакомого человека перезвонить на незнакомый телефонный номер, что объясняется веской причиной: срочно требуется помощь, проблемы со связью и т.д. После звонка человека долго держат на линии, и за это время с лицевого счета списываются большие суммы.

Особую угрозу таят в себе смс, отправленные мошенниками от лица финансовых организаций. Как правило, абонентам приходят сообщения об одобренном кредите или займе (при этом сам человек ни в какие банки или МФО не обращался).

Такие смс составляют по схожему шаблону: вверху – кричащая и при этом короткая фраза, способная если не заинтересовать, то точно привлечь внимание. Например, "сумма пересмотрена – получите 19500 руб.", "уважаемый клиент, вам одобрили заем на 12000 руб." и т.д. Далее находится ссылка, по которой нужно пройти для завершения процедуры получения денег. На самом деле переход по такой ссылке не сулит ничего хорошего. Цель злоумыш-ленников – заманить доверчивого и испытывающего потребность в финсредствах человека на вредоносный сайт и похитить его персональные данные, чтобы затем использовать их в других мошеннических схемах или продать коллегам по ремеслу.

Не попадись на крючок

Основной инструмент онлайн-мошенников – фишинг. Они создают поддельные сайты, заманивают на них жертв и похищают данные банковских карт. Причем мишенью жуликов становятся даже дети, для которых создают фейковые аналоги магазинов цифровой техники, а также магазинов онлайн-игр и аксессуаров для них. Их завлекают низкими ценами. Нередко киберпреступники используют образы популярных блогеров.

Подростков пытаются привлечь объявлениями о быстром и легком заработке, убеждают вложить деньги в "сверхвыгодный проект", имитируют инвестиционные онлайн-игры. Так ребенок рискует оказаться втянутым в махинации с нелегальным движением средств. Зафиксированы случаи, когда мошенники прикидывались ровесниками и выманивали у подростков данные родительских карт.

Едва ли кто-то из молодых людей не получал от своих приятелей в социальных сетях сообщения с просьбой немедленно дать взаймы или денежно помочь попавшему в беду родственнику. И эта схема до неприличия проста: после взлома страницы мошенники от имени пользователя пишут всем по списку контактов. Они могут отправлять ссылки, приводящие на фишинговые сайты с вредоносным ПО. В последнее время часто используется прием с просьбой принять участие в голосовании. Как только пользователь кликает по ссылке, мошенники получают доступ ко всем его контактам и могут рассылать сообщения от его имени.

По мере совершенствования систем безопасности растут и возможности мошенников, которые придумывают все новые схемы воровства денег с ваших банковских карт при помощи телефона и интернета. Одно из последних ноу-хау – кража финсредств через маскировку вредоносных программ под баннеры с рекламой "обновления браузера".

Наконец, еще один популярный метод – "звонок из Центробанка". Чаще звонить пытаются через мессенджеры, чтобы вместо номера определялся аккаунт, на аватаре которого – российский герб и название организации (хотя с физическими лицами Центральный банк не работает вообще. Впрочем, иногда мошенники звонят с аккаунта, подписанного "МВД России"). По телефону говорят, что кто-то пытается получить на вас кредит, и, чтобы не платить по чужим долгам, эти кредитные деньги нужно срочно забрать в отделении банка или перевести на "безопасный счет".

Только бдительность

Эксперты в области кибербезопасности констатируют, что преступники постоянно меняют тактику на фоне возросших потребностей пользователей интернета в области безопасности. Но абсолютной защиты от них не существует. При разъяснении рисков и угроз населению сотрудники банков обычно напоминают, что служба безопасности никогда не звонит клиентам сама – общение с владельцами банковских карт попросту не входит в перечень их полномочий. Поэтому все оперативные вопросы, связанные с движением денег и соблюдением норм безопасности, можно решать только при личном визите в отделение банка.

Это же касается и сотрудников Госуслуг – они не выходят на связь и уж точно не предлагают взять кредит.

В июле был принят закон, который должен усложнить жизнь мошенникам: банки смогут замораживать деньги после подозрительных операций, однако как это будет выглядеть на практике – пока неизвестно. Многие банки уже сейчас собирают базу голосов киберпреступников, которые пытаются обмануть клиентов по телефону, и способны автоматически блокировать спровоцированную ими транзакцию.

Полицейские, как правило, не дают каких-то стопроцентных рецептов защиты от жуликов, ограничиваясь общими рекомендациями, которые и так должен знать каждый россиянин. Нельзя сообщать кому-либо свои персональные данные, особенно пароли от личного кабинета, номера и PIN-коды банковских карт. Категорически нежелательно хранить такую информацию на компьютере или в смартфоне, а тем более на бумажке в кошельке. Нельзя переходить по сомнительным ссылкам, особенно присланным в СМС с подозрительного номера.

Обратите внимание: чтобы точно не нарваться на мошенников, следует игнорировать звонки с незнакомых телефонных номеров и сразу же пробивать их в любом из поисковиков в интернете. Информацию о номерах, которыми пользуются злоумышленники, собирают специальные сайты – там делятся опытом абоненты, которых пытались обмануть до вас. Если номер, с которого вам звонили, оценен отрицательно, смело заносите его в черный список. Если же вы ответили на звонок – поспешите закончить общение и ни в коем случае не следуйте указаниям по телефону от незнакомых лиц, даже если они представляются сотрудниками банка или полиции.

Крайне важно ввести в своих аккаунтах в интернете двухфакторную аутентификацию, если она еще не работает. Доступа просто по паролю недостаточно, чтобы обезопасить свои данные.

Что делать, если вы уже стали жертвой мошенников?

- Подайте заявление в полицию по ст.159 Уголовного кодекса.
- Обратитесь к кредитору с претензией, укажите в ней на факт мошеннических действий и изложите обстоятельства дела.
- Приложите к письму талон-уведомление из полиции, предоставьте справку об утрате удостоверения личности (при наличии), свидетельские показания, записи с камер в помещении, где был оформлен кредит и подтверждения вашего алиби.
- Соберите справки о состоянии счетов и об истории операций в обслуживающих банках в качестве доказательства отсутствия переводов от микрофинансовых организаций. Передайте заверенные копии кредитору.
- Если речь идет об онлайн-займе, нужно указать кредитору на то, что он оформлен не на ваш мобильный номер.
- Передайте следователю, который работает с вашим делом, все собранные документы по делу.
- Попробуйте добиться решения ситуации мирным путем. Если не получается, обратитесь к юристу.

По материалам прессы.