Схемы телефонных мошенников

Эксперт проекта НИФИ Минфина России «Моифинансы.рф», Кирилл Полещук в интервью журналу «Эксперт» рассказал о новых схемах финансовых мошенников и о мерах противодействия.

Относительно свежая схема мошенников – звонки от имени операторов сотовой связи. Они говорят потенциальной жертве, что договор с абонентом подходит к концу, его надо перезаключить, в противном случае номер перейдет в пользование другому человеку. Чтобы продлить договор предлагают продиктовать код из смс, а затем перейти по ссылке и ввести еще один код. Никакой договор, естественно, не продлевается, это уловка. Так мошенники взламывают аккаунт пользователя на госуслугах и получают доступ ко всем личным данным, которые там хранятся.

Еще один вариант схемы – мошенники предлагают сменить тарифный план, подключить какую-либо выгодную опцию или перевыпустить sim-карту. Для этого так же нужно продиктовать код из sms. В этом случае мошенники пытаются получить доступ к личному кабинету пользователя на сайте мобильного оператора. Это делается для того, чтобы настроить переадресацию сообщений и звонков с номера жертвы на номер злоумышленников. Так они смогут подтверждать операции, которые сам пользователь не совершал – например, выводить средства с банковских карт абонента или оформить на жертву кредит.

Важно! Все вопросы с оператором лучше решать с его сотрудниками в офисе или самостоятельно через официальное мобильное приложение или личный кабинет на сайте. Настоящие сотрудники оператора связи не будут просить продиктовать коды из sms по телефону и переходить по ссылкам. Если возникают сомнения, повесьте трубку и свяжитесь с оператором самостоятельно по официальному номеру, который указан на сайте.

Телефонные мошенники придумывают все более изощренные способы обмана своих жертв, но не брезгуют и старыми классическими приемами.

1. Звонок из банка.

По телефону сообщают о том, что по вашему счету якобы происходят подозрительные операции, оформлена заявка на кредит, снята крупная денежная сумма и т. д.
«Оператор» действует с нажимом, агрессивно, делает акцент именно на том, что некие мошенники уже получили доступ к счетам гражданина. Используются слова и выражения, которые заставляют сомневаться в безопасности своих денежных средств.
Обычно через украденные базы данных мошенникам становятся известны персональные данные попавшегося на крючок гражданина – ФИО, адрес, телефон и даже паспортные данные. Сам факт того, что кому-то известны ваши данные, не может не возмущать. Тем не

менее сами по себе эти данные не позволят мошенникам каким-то образом увести деньги со счета – иначе бы они и не звонили.
Им нужны ваши конкретные действия – снятие денежных средств, перечисление их на счета мошенников, сообщение данных банковских карт и кодов из смс-сообщений от банков.
Необходимо подчеркнуть – именно активные действия, которые жертва должна совершить самостоятельно, но выполняя волю «операторов».
Благодаря отточенным психологическим навыкам и методам социальной инженерии потерпевший думает, что действует самостоятельно, но является всего лишь марионеткой.
Типичным признаком человека, находящегося под психологическом воздействием, является тот факт, что он не выпускает из рук телефон ни на секунду, находясь в офисе банка или снимая деньги через банкомат.
Мошенникам важно не упускать ни на мгновение контакт с жертвой.
«Оператор» убеждает жертву, что все сотрудники банка или полиции, кто мешает жертве осуществить снятие или перевод денег, – мошенники, которые пытаются обворовать человека, и только позвонивший «оператор» может «спасти» от них.
Прозрение наступает слишком поздно.
Единственный способ защиты – не отвечать на звонки с подозрительных номеров либо же незамедлительно прекратить разговор, как только кто-то представился сотрудником банка.
Вы всегда можете самостоятельно перезвонить в свой банк и уточнить все вопросы.
Типичный звонок мошенников – через мессенджеры (вотсап, вайбер, реже вк или телеграмм).
Банки никогда не звонят через мессенджеры.

2. Звонок от родственника, попавшего в беду.

Да-да, это способ до сих пор работает и работает неплохо. Основные жертвы – старшее поколение. Благодаря украденным базам данных у мошенников, помимо номеров мобильных, есть телефонные номера городских стационарных телефонов.
Звонки обычно происходят в вечернее или ночное время, звонивший заранее знает, что будет говорить с пожилым человек, и начинает разговор с ярких эмоций («бабуля, милая, спаси меня» или «старший следователь Иванов, только что ваш внук сбил человека и т. д»).
Звонящие чередуются, передают трубку друг друг. «Сбивший человека внук», следователь, врач и т. д.
Суть сводится к необходимости передать деньги на лечение, на взятку и тому подобное.
Поэтому сразу же должно возникнуть сомнение – ну какие взятки в наше время, тем более по телефону.
Все это шоу устраивается только ради одного – побудить жертву к самостоятельным активным действиям – либо перевести деньги на счет, либо дождаться специального курьера и передать ему наличные.

При определенной доле удачи правоохранительные органы в подобных историях могут найти лишь курьеров-«бегунков», заказчики обычно находятся за границей. Роль

«бегунков» обычно выполняют наркозависимые граждане, или молодежь в поисках легких денег.
Если же деньги предавались без помощи курьеров, то шансы на раскрытие дела, наказание виновных и возврат самостоятельно отправленных мошенникам сумм стремятся к нулю.
Совет может быть прежний – сохранять холодную голову при телефонных разговорах, сразу же прерывать разговор, если вопрос стал касаться денег. Всегда можно перезвонить, связаться непосредственно с родственником, от чьего имени звонят.

3. Звонок из полиции, ФСБ и иных силовых структур

Звонящий представляется сотрудником той или иной силовой структуры, называет должность, звание и наименование органа.
Зачастую уже в этих данных можно распознать мошенника – часто называются несуществующие организации или должности.
Сообщают, что якобы ведется уголовное расследование в отношении жертвы – в настоящее время популярны «обвинения» в экстремизме, связи с иностранными агентами, переводе денег на поддержку вооруженных сил враждебных государств.
Пользуясь всеобщей истерией в данной сфере и правовой неграмотностью, мошенники часто попадают в яблочко – жертва начинается верить, что действительно сделала что-то незаконное.
Ответ в таком случае должен быть один –бросить трубку.
Если звонят действительно из правоохранительных органов, то там найдут способ с вами связаться.
Также всегда можно сказать звонящему, что на вопросы будете отвечать в присутствии адвоката, или попросить известить о предстоящем следственном действии повесткой по месту жительства. На этом закончится 99% разговоров, в том числе и с реальными сотрудниками силовых структур.

Среди иных способов телефонных мошенничеств можно выделить сообщения и звонки через мессенджеры:

- Звонок от фейкового начальника крупной организации, в которой работает жертва.
- Предложения заработка в интернете.
- Участие в голосовании за дочку/племянницу.
- Звонки от «операторов» сотовой связи о прекращении действия номера.
- Звонки от специалиста Госуслуг о взломе аккаунта.
- Победа в лотерее или сообщение о зачислении крупной денежной суммы.

В настоящее время у многих мобильных операторов популярны услуги «защитника» от телефонных мошенников.
Смысл заключается в блокировке программой подозрительных звонков. Услуга действительно защищает от телефонного спама и блокирует мошенников. При этом в блок могут попадать и полезные звонки, поэтому могут потребоваться индивидуальные настройки.

Важно!

Помните, нельзя безоговорочно верить информации, полученной из сообщений или разговоров по телефону, какой бы правдоподобной она ни казалась. Не поддавайтесь давлению со стороны звонящего. При наличии сомнений нужно самостоятельно проверить полученную информацию в официальных источниках, обратиться за советом/помощью к родственникам, друзьям или коллегам.