

Прокуратура Прионежского района разъясняет:

«Признаки, что Вам звонит мошенник»

Даже если мошенник знает номер и срок действия Вашей банковской карты, украсть с нее деньги не так просто.

Большинство банковских карт защищены «3-D Secure» - системой, которая требует подтвердить крупные операции кодом из СМС-сообщения. А чтобы узнать этот код, злоумышленники используют разные формы фишинга: рассылают письма на электронную почту, отправляют сообщения в социальных сетях, подделывают сайты банков и звонят от их имени по телефону.

Если диалог идет по одному из сценариев, указанных ниже, завершайте разговор и звоните самостоятельно в свой банк по телефону, указанному на банковской карте.

Признак 1 Звонок поступает со скрытого номера.

Сотрудники банка всегда звонят с официальных номеров, указанных на сайте банка. Он может быть федеральным, может быть мобильным, но он никогда не будет скрытым.

Признак 2 СМС-сообщения якобы от банка приходят в новую переписку.

СМС-сообщения из банка тоже приходят с одного-двух номеров, которые Вам уже знакомы. В любом случае не переходите по ссылкам в сообщениях от неизвестных источников.

Признак 3 Собеседник не может ответить на простые вопросы.

«Мошенник»

— Здравствуйте, Вас беспокоят из банка. Мы видим по вашей карте подозрительную операцию.

— По какой карте?

— По вашей основной...

— Назовите номер карты.

—...

«Банк»

— Здравствуйте, Вас беспокоят из банка. Мы видим подозрительную операцию по Вашей карте, последние цифры 1234. Снятие наличных в другом городе, сумма 8000 рублей.

— Операцию подтверждаю. Это я снимал, спасибо!

Помните, сотрудник банка видит на экране своего компьютера всю информацию, которая имеется по Вам в базе данных этого банка. Если собеседник не готов ответить на простой вопрос, например, назвать остаток по карте, это мошенник.

Признак 4 Тревожная тема сообщения или звонка.

Чтобы напугать жертву и заставить скорее совершить нужное действие, мошенники придумывают пугающие сценарии. Говорят, что банк заблокировал счет, начислил штраф за кредит или что проведена подозрительная операция.

В такой ситуации не спешите, две минуты ничего не решат. Позвоните в банк по телефону, указанному на Вашей банковской карте и уточните необходимую информацию или позвоните родственникам.

Признак 5 Собеседник спрашивает данные банковской карты или СМС-код.

«Мошенник»

— Чтобы отменить подозрительную операцию, продиктуйте мне номер Вашей карты и код с обратной стороны.

— 1234 5678 9012 3456, код 789.

— Прекрасно, вам сейчас придет СМС-сообщение, скажите, какие там цифры?

«Банк»

— Мы заблокировали карту и заказали перевыпуск. Средства по подозрительной операции мы временно заблокировали, ситуацию изучает служба безопасности банка.

Важно помнить, что СМС-сообщение с кодом — это всё равно, что пароль от Ваших банковских счетов. Сотрудники банка никогда его не спросят, а номер карты они и так знают.

Если Вам позвонили якобы из банка, и вы хотите убедиться в надежности собеседника, спросите его ФИО. После этого перезвоните по официальному номеру банка — тому, который указан на карте и на сайте, — и попросите переключить на человека, который Вам звонил.

Признак 6 Вам обещают какую-либо выгоду без усилий.

Чтобы завлечь жертву, мошенники обещают солидный доход быстро и без усилий: суперприбыльную работу, беспроигрышные конкурсы, курсы и подписки, которые принесут прибыль без усилий. Например, мошенники возьмут предоплату за обучение и пропадут. Или пообещают приз и выманят у Вас данные карты якобы для перевода выигрыша.

Признак 7 Собеседник торопит Вас или пытается переубедить.

Помните, что сотрудник банка никогда не будет настаивать или спешить. Он же на работе.

Итак, если Вы не уверены в собеседнике, попросите его назвать номер карты или остаток на счете. Не паникуйте, если Вам пишут о блокировке счета. Позвоните в банк по номеру телефона, указанному на сайте или на самой карте. Не ведитесь на обещания легких денег или выгоды без усилий. Если собеседник торопит Вас или спрашивает СМС-код, Вы говорите с мошенником. Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков.